

CENTRO NACIONAL DE DESARROLLO  
E INVESTIGACIÓN EN TECNOLOGÍAS LIBRES (CENDITEL)



# SEGURIDAD INFORMÁTICA Y LA IDENTIDAD DIGITAL

## Fundamentos y Aportes



Gobierno Bolivariano  
de Venezuela

Ministerio del Poder Popular  
para la Educación Universitaria, Ciencia y Tecnología

Centro Nacional de Desarrollo e  
Investigación en Tecnologías Libres (Cenditel)



---

# SEGURIDAD INFORMÁTICA Y LA IDENTIDAD DIGITAL

## Fundamentos y Aportes

---

**Endira Mora, Antonio Araujo, Víctor Bravo  
Rodolfo Sumoza, José Contreras, Daniel Quintero**

**Maquetación y Dibujos: Gabriela Villasana**

**Portada: Cipriano Alvarado**

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres - CENDITEL

Ministerio para el Poder Popular para la Educación Universitaria, Ciencia y Tecnología



**Publicación de la Fundación CENDITEL**



Derecho de Autor © 2014 de: Endira Mora, Antonio Araujo, Víctor Bravo, Rodolfo Sumoza, José Contreras, Daniel Quintero.  
Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres (CENDITEL).  
Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología.  
República Bolivariana de Venezuela.

Los contenidos de esta publicación expresan el punto de vista personal de los autores y son divulgados con el propósito de generar el debate de torno a temas de interés nacional y regional. De ningún modo debe entenderse que los mismos representan necesariamente la política oficial del Centro Nacional de Desarrollo e Investigación en Tecnologías Libres ni del Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología.

Algunos Derechos Reservados – Copyleft.

La presente obra está liberada bajo una Licencia Creative Commons Venezuela 3.0: Reconocimiento, No comercial, Compartir Igual 3.0, que permite compartir, exhibir, modificar y ampliar la obra para fines no comerciales, siempre y cuando se de crédito a su (s) autor (es) y la licencia de las nuevas obras creadas a partir de la original posean iguales términos y condiciones a la licencia de la obra original.

Más información sobre la licencia en: <https://creativecommons.org/licenses/by-sa/3.0/ve/>

Código fuente de la obra disponible en: <https://tibusay.cenditel.gob.ve/publicaciones>

Noviembre 2014, Primera Edición

HECHO EL DEPÓSITO DE LEY  
Depósito Legal: lf70120146003465  
ISBN: 978-980-7154-18-5

Maquetación y Dibujos: Gabriela Villasana  
Portada: Cipriano Alvarado  
Corrección de textos: Luis Perales  
Impresión: JC Impresores

Edición colaborativa usando la herramienta de control de versiones Git.  
Maquetado usando  $\text{\LaTeX}$ , Bib $\text{\TeX}$  y pdf $\text{\TeX}$ .

*A la creatividad*

## COLABORADORES

---

Alexis Dávila  
Dhionel Díaz  
Johanna Álvarez  
Luis Perales  
Maryorie Varela  
Solazver Solé

# LISTA BREVE DE CONTENIDOS

---

## PARTE I FUNDAMENTOS: SEGURIDAD E IDENTIDAD DIGITAL

|   |           |
|---|-----------|
| <b>1 Bases de la identidad digital</b>        | <b>2</b>  |
| Antonio Araujo, Víctor Bravo y Rodolfo Sumoza |           |
| <b>2 Políticas de Seguridad</b>               | <b>35</b> |
| Víctor Bravo y Antonio Araujo                 |           |
| <b>3 Sistemas Anónimos</b>                    | <b>64</b> |
| Rodolfo Sumoza                                |           |
| <b>4 Fundamentos jurídicos</b>                | <b>78</b> |
| Endira Mora                                   |           |

## PARTE II APORTES EN CERTIFICACIÓN ELECTRÓNICA Y ANONIMATO

|   |            |
|---|------------|
| <b>5 Desarrollo de una aplicación para Gestión de una AC Raíz utilizando Software Libre</b> | <b>114</b> |
| Víctor Bravo y Antonio Araujo   |            |
| <b>6 Propuesta de acoplamiento de la firma electrónica avanzada en procesos de negocio</b>  | <b>129</b> |
| Víctor Bravo y Antonio Araujo   |            |
| <b>7 Modelo de protocolo para un sistema anónimo basado en estrategias bio-inspiradas</b>   | <b>142</b> |
| Rodolfo Sumoza  |            |
| <b>8 Sistema de medición de anonimato</b>   | <b>146</b> |
| Rodolfo Sumoza  |            |

## PARTE III APORTES ESTRATÉGICO-POLÍTICOS EN IDENTIDAD DIGITAL

|   |            |
|---|------------|
| <b>9 Explorando el sentido de la Identidad Digital para la Venezuela del Siglo XXI</b>  | <b>152</b> |
| José J. Contreras   |            |
| <b>10 La ciberguerra, la ciberdefensa y la Identidad Digital Suramericana en UNASUR</b> | <b>171</b> |
| Daniel Quintero   |            |
| <b>Apéndices</b>  | <b>187</b> |

# Índice general

---

|                                     |       |
|-------------------------------------|-------|
| Lista de Figuras                    | XIII  |
| Lista de Tablas                     | XVI   |
| Agradecimientos                     | XVII  |
| Acrónimos                           | XVIII |
| Introducción                        | XXII  |
| <i>Victor Bravo, Rodolfo Sumoza</i> |       |

## PARTE I FUNDAMENTOS: SEGURIDAD E IDENTIDAD DIGITAL

|   |          |
|---|----------|
| <b>1 Bases de la identidad digital</b>        | <b>2</b> |
| Antonio Araujo, Víctor Bravo y Rodolfo Sumoza |          |
| 1.1. Identidad Digital ID                     | 2        |
| 1.1.1. Identidad Parcial                      | 3        |
| 1.1.2. Rol                                    | 3        |
| 1.1.3. Manejo de la ID                        | 3        |
| 1.2. Protección de la ID                      | 4        |
| 1.2.1. Certificación Electrónica              | 4        |
| 1.2.2. Firma Electrónica                      | 4        |
| 1.2.3. Registro del comportamiento            | 4        |
| 1.2.4. Privacidad vinculada a la ID           | 5        |
| 1.3. Técnicas de verificación de identidad    | 10       |
| 1.3.1. Contraseñas                            | 10       |
| 1.3.2. Certificados electrónicos              | 11       |
|   | VII      |

|                               |   |           |
|-------------------------------|---|-----------|
| 1.3.3.                        | Firmas electrónicas   | 17        |
| 1.3.4.                        | Dispositivos de usuario   | 18        |
| 1.3.5.                        | Usos comunes de dispositivos de usuario                                 | 28        |
| Referencias                   |   | 34        |
| <b>2</b>                      | <b>Políticas de Seguridad</b>   | <b>35</b> |
| Víctor Bravo y Antonio Araujo |   |           |
| 2.1.                          | Introducción  | 35        |
| 2.2.                          | Políticas de seguridad de las tecnologías de información y comunicación | 36        |
| 2.3.                          | Importancia de la seguridad de la información                           | 37        |
| 2.4.                          | Seguridad de la Información para Tecnologías Libres                     | 38        |
| 2.5.                          | Principio de defensa en profundidad                                     | 38        |
| 2.5.1.                        | Los principios generales de la defensa en profundidad                   | 39        |
| 2.6.                          | Responsabilidad   | 40        |
| 2.7.                          | Procesos para aumentar la adopción de seguridad de la información       | 40        |
| 2.7.1.                        | Identificación de los riesgos   | 41        |
| 2.7.2.                        | Evaluación de los riesgos de seguridad                                  | 42        |
| 2.7.3.                        | Selección de los controles  | 43        |
| 2.7.4.                        | Implementar los controles seleccionados                                 | 43        |
| 2.7.5.                        | Supervisar y mejorar los controles de seguridad                         | 43        |
| 2.8.                          | Grupo de seguridad de la información                                    | 44        |
| 2.9.                          | Gestión de contraseñas  | 44        |
| 2.9.1.                        | Tamaños de contraseñas  | 45        |
| 2.10.                         | Entornos de la Seguridad de la Información                              | 46        |
| 2.10.1.                       | Puesto de trabajo   | 46        |
| 2.10.2.                       | Centro de datos   | 46        |
| 2.11.                         | Tipos de Seguridad de la Información                                    | 46        |
| 2.11.1.                       | Seguridad Lógica  | 46        |
| 2.11.2.                       | Seguridad Física  | 47        |
| 2.12.                         | Cuenta de usuario   | 47        |
| 2.12.1.                       | Cuenta de usuario crítica   | 47        |
| 2.13.                         | Vulnerabilidades de los sistemas de información                         | 47        |
| 2.13.1.                       | Causas de las vulnerabilidades de los sistemas informáticos             | 47        |
| 2.14.                         | Herramientas para la seguridad de la información                        | 48        |
| 2.14.1.                       | Cortafuegos   | 48        |
| 2.14.2.                       | Utilidad de un cortafuegos  | 50        |
| 2.14.3.                       | Consideraciones para la instalación y configuración de cortafuegos      | 50        |
| 2.14.4.                       | Sistemas de detección de intrusiones (IDS)                              | 51        |
| 2.15.                         | Identificación de los riesgos a terceros                                | 52        |
| 2.16.                         | Seguridad lógica en los puestos de trabajo                              | 52        |
| 2.17.                         | Seguridad lógica en los centros de datos                                | 53        |
| 2.18.                         | Seguridad física en los puestos de trabajo                              | 54        |
| 2.19.                         | Seguridad física en los centros de datos                                | 54        |
| 2.19.1.                       | Servicios que prestan o prestarán los centros de datos                  | 54        |



|                |  |           |
|----------------|--|-----------|
| 2.19.2.        | Ubicación y condición física de los centros de datos                                   | 55        |
| 2.19.3.        | Especificaciones técnicas de los centros de datos                                      | 55        |
| 2.19.4.        | Control de acceso físico a los centros de datos  | 56        |
| 2.19.5.        | Sistema de aire acondicionado  | 57        |
| 2.19.6.        | Protección, detección y extinción de incendios   | 57        |
| 2.20.          | Especificación de las Políticas de seguridad de la información en los centros de datos | 58        |
| 2.21.          | Políticas de respaldo y recuperación   | 59        |
| 2.21.1.        | Normas para las políticas de respaldo y recuperación                                   | 59        |
| 2.22.          | Gestión de incidentes de seguridad   | 59        |
| 2.22.1.        | Antes del incidente de seguridad:  | 60        |
| 2.22.2.        | Durante el incidente de seguridad:   | 60        |
| 2.22.3.        | Después del incidente de seguridad:  | 61        |
| 2.23.          | Plan de recuperación ante desastres  | 61        |
| Referencias    |  | 63        |
| <b>3</b>       | <b>Sistemas Anónimos</b>   | <b>64</b> |
| Rodolfo Sumoza |  |           |
| 3.1.           | Técnicas para proporcionar privacidad  | 65        |
| 3.1.1.         | Bases del Anonimato  | 66        |
| 3.1.2.         | Técnicas de Anonimato  | 68        |
| Referencias    |  | 76        |
| <b>4</b>       | <b>Fundamentos jurídicos</b>   | <b>78</b> |
| Endira Mora    |  |           |
| 4.1.           | El ordenamiento jurídico venezolano y las nuevas tecnologías de la información         | 78        |
| 4.2.           | Derecho de <i>Habeas Data</i>  | 80        |
| 4.2.1.         | Derechos que otorga el <i>Habeas Data</i>  | 81        |
| 4.2.2.         | Procedimiento de <i>Habeas Data</i>  | 82        |
| 4.3.           | Ley Especial Contra Delitos Informáticos (LECDI)                                       | 84        |
| 4.3.1.         | Definición de Delito Informático   | 84        |
| 4.3.2.         | Clasificación de los Delitos Informáticos  | 85        |
| 4.3.3.         | Características de los Delitos Informáticos  | 86        |
| 4.3.4.         | Tipificaciones de la Ley Especial contra Delitos Informáticos                          | 87        |
| 4.4.           | Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas                | 89        |
| 4.4.1.         | Los Mensajes de datos en la LDMFE  | 92        |
| 4.4.2.         | Eficacia probatoria  | 92        |
| 4.4.3.         | Requisitos del Mensaje   | 93        |
| 4.4.4.         | La emisión y recepción de mensajes de datos  | 94        |
| 4.4.5.         | Confidencialidad de los mensajes de datos  | 95        |
| 4.5.           | La firma electrónica en la LMDFE   | 95        |
| 4.5.1.         | Diferencias entre la firma electrónica y la firma autógrafa                            | 96        |
| 4.5.2.         | Eficacia probatoria de la firma electrónica  | 96        |
| 4.5.3.         | Obligaciones del signatario  | 96        |
| 4.5.4.         | Ventajas de la firma electrónica   | 97        |

|         |   |     |
|---------|---|-----|
| 4.5.5.  | De SUSCERTE y los PSC   | 97  |
| 4.5.6.  | Consideraciones finales   | 99  |
| 4.6.    | Ley de Infogobierno   | 99  |
| 4.6.1.  | Derechos que se otorgan en la Ley de Infogobierno   | 100 |
| 4.6.2.  | Uso del software libre en la Administración Pública Nacional                                      | 101 |
| 4.6.3.  | Derecho y Garantía sobre el acceso a la información   | 101 |
| 4.6.4.  | Sanciones que contempla Ley de Infogobierno   | 102 |
| 4.7.    | Otras normas aplicables   | 103 |
| 4.7.1.  | Decreto 825 del 10 de mayo de 2000  | 103 |
| 4.7.2.  | Ley Orgánica para la Ciencia, Tecnología y Innovación   | 103 |
| 4.7.3.  | Ley Orgánica de la Administración Pública   | 103 |
| 4.7.4.  | Ley de Registro Público y del Notariado   | 104 |
| 4.7.5.  | Ley de Instituciones del Sector Bancario  | 104 |
| 4.7.6.  | Ley de Contrataciones Publicas  | 105 |
| 4.7.7.  | Código Orgánico Tributario  | 105 |
| 4.8.    | Legislación Internacional en el Marco de las tecnologías de la información                        | 106 |
| 4.8.1.  | Convenio Europeo para la protección de los Derechos Humanos y de las Libertades fundamentales     | 106 |
| 4.8.2.  | Iniciativa Internacional para la protección del consumidor en el marco del Comercio Electrónico   | 106 |
| 4.8.3.  | Ley Modelo de la CNUDMI sobre Comercio Electrónico (Law on electronic commerce UNCITRAL)          | 106 |
| 4.8.4.  | Ley Modelo de la CNUDMI sobre Firmas Electrónicas (Law on electronic signature UNCITRAL) del 2001 | 107 |
| 4.8.5.  | España  | 107 |
| 4.8.6.  | Alemania  | 108 |
| 4.8.7.  | México  | 108 |
| 4.8.8.  | Colombia  | 108 |
| 4.8.9.  | Brasil  | 108 |
| 4.8.10. | Argentina   | 108 |
| 4.8.11. | Cuba  | 109 |
| 4.8.12. | Consideraciones Finales   | 109 |
| 4.9.    | Conclusiones  | 109 |
|         | Referencias   | 111 |

## PARTE II APORTES EN CERTIFICACIÓN ELECTRÓNICA Y ANONIMATO

|          |   |            |
|----------|---|------------|
| <b>5</b> | <b>Desarrollo de una aplicación para Gestión de una AC Raíz utilizando Software Libre</b> | <b>114</b> |
|          | Víctor Bravo y Antonio Araujo   |            |
| 5.1.     | Introducción  | 115        |
| 5.2.     | Marco Teórico   | 115        |
| 5.2.1.   | Seguridad Informática   | 115        |
| 5.2.2.   | Criptografía  | 116        |
| 5.2.3.   | Certificados electrónicos   | 116        |

|                               |  |            |
|-------------------------------|--|------------|
| 5.2.4.                        | Estándar X.509   | 117        |
| 5.2.5.                        | Lenguaje Unificado de Modelado   | 118        |
| 5.2.6.                        | Software Libre   | 119        |
| 5.3.                          | Infraestructura de Clave Pública   | 119        |
| 5.3.1.                        | Componentes de la Infraestructura de Clave Pública (ICP)                                 | 119        |
| 5.4.                          | Desarrollo de la aplicación  | 120        |
| 5.4.1.                        | Conceptualización  | 120        |
| 5.4.2.                        | Diseño   | 121        |
| 5.4.3.                        | Implementación   | 123        |
| 5.4.4.                        | Pruebas  | 125        |
| 5.4.5.                        | Despliegue y configuración   | 125        |
| 5.5.                          | Conclusiones   | 125        |
| 5.6.                          | Glosario   | 127        |
| Referencias                   |  | 128        |
| <b>6</b>                      | <b>Propuesta de acoplamiento de la firma electrónica avanzada en procesos de negocio</b> | <b>129</b> |
| Víctor Bravo y Antonio Araujo |  |            |
| 6.1.                          | Introducción   | 129        |
| 6.2.                          | El modelo actual de firma electrónica  | 130        |
| 6.3.                          | Antecedentes   | 131        |
| 6.4.                          | Acoplamiento de la firma electrónica avanzada  | 132        |
| 6.4.1.                        | Componente de firma electrónica avanzada   | 132        |
| 6.4.2.                        | Método de conexión   | 134        |
| 6.5.                          | Casos de estudio   | 135        |
| 6.5.1.                        | Caso OpenERP   | 136        |
| 6.5.2.                        | Caso SAID  | 136        |
| 6.5.3.                        | Caso Flujos de Trabajo   | 138        |
| 6.6.                          | Conclusiones   | 138        |
| Referencias                   |  | 140        |
| <b>7</b>                      | <b>Modelo de protocolo para un sistema anónimo basado en estrategias bio-inspiradas</b>  | <b>142</b> |
| Rodolfo Sumoza                |  |            |
| 7.1.                          | Introducción   | 142        |
| 7.2.                          | Colonias Artificiales de Hormigas en Anonimato   | 143        |
| 7.3.                          | Conclusión   | 144        |
| Referencias                   |  | 145        |
| <b>8</b>                      | <b>Sistema de medición de anonimato</b>  | <b>146</b> |
| Rodolfo Sumoza                |  |            |
| 8.1.                          | Introducción   | 147        |
| 8.2.                          | Trabajos Relacionado   | 147        |
| 8.3.                          | Propuesta  | 148        |
| 8.3.1.                        | Raíz del Error Cuadrático Medio - RSME   | 148        |
| 8.3.2.                        | Divergencia de Jennesen-Shannon  | 148        |

|                   |     |
|-------------------|-----|
| 8.3.3. Resultados | 149 |
| Referencias       | 150 |

### **PARTE III APORTES ESTRATÉGICO-POLÍTICOS EN IDENTIDAD DIGITAL**

|   |            |
|---|------------|
| <b>9 Explorando el sentido de la Identidad Digital para la Venezuela del Siglo XXI</b>  | <b>152</b> |
| José J. Contreras   |            |
| 9.1. ¿Identidad? ¿Identidad Digital?  | 152        |
| 9.2. El surgimiento de la Identidad   | 154        |
| 9.3. “Vida” y “Mundo”; “Labor” y “Trabajo”  | 156        |
| 9.4. El trastoque de la modernidad  | 156        |
| 9.5. La Identidad en la sociedad digital  | 158        |
| 9.6. La identidad digital y la diferencia entre el “contar con” y la “confianza”        | 160        |
| 9.7. La resignificación de los dominios público y privado                               | 161        |
| 9.8. La Identidad preciosa  | 162        |
| 9.9. Identidad Digital a tiempo de revolución bolivariana                               | 165        |
| 9.10. Palabras finales: el recuento   | 168        |
| Referencias   | 170        |
| <b>10 La ciberguerra, la ciberdefensa y la Identidad Digital Suramericana en UNASUR</b> | <b>171</b> |
| Daniel Quintero   |            |
| 10.1. Introducción  | 171        |
| 10.2. La Cibernética y el Ciberespacio, contextualización de las definiciones           | 172        |
| 10.3. La ciberguerra y sus repercusiones estratégicas                                   | 173        |
| 10.4. Elementos Normativos y Principios de la Ciberguerra                               | 175        |
| 10.5. La Identidad Digital Suramericana, contribuyente a la ciberdefensa de la UNASUR   | 177        |
| 10.6. Algunas Ideas Finales   | 184        |
| Referencias   | 185        |
| <b>Apéndices</b>  | <b>187</b> |
| <b>A Certificado electrónico X.509 Versión 3 en texto plano</b>                         | <b>189</b> |

## LISTA DE FIGURAS

---

|      |   |    |
|------|---|----|
| 1.1  | Seudonimato   | 7  |
| 1.2  | Seudonimato con respecto al Anonimato                             | 8  |
| 1.3  | Conjuntos No Observables  | 9  |
| 1.4  | Cédula de identidad de la República Bolivariana de Venezuela.     | 12 |
| 1.5  | Infraestructura Nacional de Certificación Electrónica.            | 13 |
| 1.6  | Sistema de banca en línea que utiliza un certificado electrónico. | 15 |
| 1.7  | Detalles de los campos de un certificado electrónico.             | 16 |
| 1.8  | Tarjeta de débito magnética.                                      | 18 |
| 1.9  | Tarjeta magnética de telefonía pública.                           | 19 |
| 1.10 | Tarjeta con chip de memoria para telefonía pública.               | 20 |
| 1.11 | Tarjetas con microprocesador.                                     | 21 |
| 1.12 | Tarjeta sin contacto.   | 22 |
| 1.13 | Tarjeta dual o híbrida.   | 23 |
| 1.14 | Lectores de tarjetas inteligentes de contacto.                    | 23 |
| 1.15 | Lectores de tarjetas inteligentes sin contacto.                   | 24 |
| 1.16 | Lector de tarjetas inteligentes de interfaz dual.                 | 24 |
| 1.17 | Token criptográficos.   | 25 |

|      |   |     |
|------|---|-----|
| 1.18 | Token criptográfico en formato MicroSD y SD.                          | 25  |
| 1.19 | Dispositivos de contraseña de un solo uso.                            | 26  |
| 1.20 | Chip SIM de telefonía celular.  | 27  |
| 1.21 | Lectores biométricos.   | 28  |
| 1.22 | Tarjeta electrónica de alimentación.                                  | 29  |
| 1.23 | Tarjeta inteligente para certificado electrónico.                     | 30  |
| 1.24 | Token USB para certificado electrónico.                               | 30  |
| 1.25 | Tarjeta inteligente de pasaje estudiantil.                            | 31  |
| 1.26 | Tarjeta y lector de control de acceso físico.                         | 31  |
| 1.27 | Muestra de pasaporte electrónico.                                     | 32  |
| 1.28 | Símbolo de pasaporte electrónico según ICAO.                          | 33  |
| 2.1  | Ciclo de la Seguridad de la Información                               | 36  |
| 2.2  | Enfoque tradicional de Seguridad.                                     | 39  |
| 2.3  | Enfoque de defensa en profundidad.                                    | 40  |
| 2.4  | Proceso de percepción de la Seguridad.                                | 41  |
| 2.5  | Cortafuegos por Hardware.   | 48  |
| 2.6  | Cortafuegos por Software.   | 49  |
| 2.7  | Cortafuegos personal.   | 49  |
| 2.8  | Cortafuegos personal combinado.                                       | 50  |
| 2.9  | Estructura funcional básica del IDS.                                  | 51  |
| 3.1  | Configuración del Sistema General                                     | 67  |
| 3.2  | Conjuntos Anónimos  | 67  |
| 3.3  | Redes de Mezcla   | 73  |
| 3.4  | Topología Mix   | 74  |
| 5.1  | Especificación del estandar X.509                                     | 117 |
| 5.2  | Modelo jerárquico de una ICP  | 120 |
| 5.3  | Caso de uso principal   | 121 |
| 5.4  | Caso de uso para el actor Administrador Autoridad de Certificación    | 122 |
| 5.5  | Diagrama de clases  | 122 |
| 5.6  | Diagrama de actividades para el caso de uso “Emisión de Certificados” | 123 |
| 5.7  | Sistema de registro de acciones                                       | 124 |
| 5.8  | Configuración de los componentes del nodo raíz de una ICP             | 126 |

|      |  |     |
|------|--|-----|
| 6.1  | Diagrama UML de acoplamiento                             | 133 |
| 6.2  | Diagrama de flujo para el acoplamiento del ComponenteFEA | 134 |
| 6.3  | Interfaz de usuario OpenERP para el ComponenteFEA        | 137 |
| 10.1 | Ciberdefensa - Ciberguerra: Planos                       | 183 |
| 10.2 | Ciberdefensa y la IDS                                    | 184 |

## LISTA DE TABLAS

---

|     |  |    |
|-----|--|----|
| 1.1 | Fabricantes de Tarjetas JavaCard y sus Sistemas Operativos | 21 |
| 1.2 | Proporción de suscriptores por tipo de tecnología móvil.   | 29 |



## AGRADECIMIENTOS

---

Le agradecemos a todos: ¡GRACIAS!

E. A. V. R. J. D.

## ACRÓNIMOS

---

|          |   |
|----------|---|
| AFIS     | Automated Fingerprint Identification System                             |
| AC       | Autoridad de Certificación  |
| API      | Application Programming Interface                                       |
| AR       | Autoridad de Registro   |
| BPEL     | Business Process Execution Language                                     |
| CAN      | Comunidad Andina de Naciones  |
| CANTV    | Compañía Anónima Nacional Teléfonos de Venezuela                        |
| CDMA     | Code division multiple access   |
| CDS      | Consejo de Defensa Suramericano   |
| CEED     | Centro de Estudios Estratégicos de Defensa de la UNASUR                 |
| CGR      | Contraloría General de la República                                     |
| CICPC    | Cuerpo de Investigaciones Científicas, Penales y Criminalísticas        |
| CNA      | Computer Network Attack   |
| CND      | Computer Network Defense  |
| CNE      | Consejo Nacional Electoral  |
| CNE*     | Computer Network Exploitation   |
| CNO      | Computer Network Operations   |
| CNUDMI   | Comisión de las Naciones Unidas para el Derecho Mercantil Internacional |
| CONATEL  | Comisión Nacional de Telecomunicaciones                                 |
| COSIPLAN | Consejo Suramericano de Infraestructura y Planeamiento                  |

|          |  |
|----------|--|
| CRL      | Certificate Revocation List  |
| CSAN     | Comunidad Sudamericana de Naciones                                 |
| FIDO     | Fast IDentity Online   |
| GCHQ     | Government Communications Headquarters                             |
| GSM      | Global System for Mobile Communications                            |
| HMI      | Human-machine Interface  |
| HSM      | Hardware Security Module   |
| ICAO     | International Civil Aviation Organization                          |
| IEC      | International Electrotechnical Commission                          |
| IETF     | Internet Engineering Task Force                                    |
| INE      | Instituto Nacional de Estadísticas                                 |
| IO       | Information Operations   |
| IP       | Internet Protocol  |
| ISDN     | Integrated Services for Digital Network                            |
| HTML     | HyperText Markup Language  |
| ICP      | Infraestructura de Clave Pública                                   |
| ISO      | International Organization for Standardization                     |
| MERCOSUR | Mercado Común del Sur  |
| MIME     | Multi-Purpose Internet Mail Extensions                             |
| MUSCLE   | Movement For The Use Of Smart Cards In a Linux Enviroment          |
| NSA      | National Security Agency   |
| OCSP     | Online Certificate Status Protocol                                 |
| PADES    | PDF Advanced Electronic Signatures                                 |
| PDF      | Portable Document Format   |
| PET      | Privacy Enhancing Technologies                                     |
| PIN      | Personal Identification Number                                     |
| PKCS     | Public Key Cryptographic Standards                                 |
| PKI      | Public Key Infrastructure  |
| PUK      | PIN UnlocK Code  |
| PSC      | Proveedor de Servicios de Certificación                            |
| SAIME    | Servicio Administrativo de Identificación, Migración y Extranjería |
| SHA      | Secure Hash Algorithm  |
| SSH      | Secure SHell   |
| SSL      | Secure Sockets Layer   |
| SUDEBAN  | Superintendencia de las Instituciones Bancarias                    |
| SUSCERTE | Superintendencia de Servicios de Certificación Electrónica         |
| TCP      | Transmission Control Protocol                                      |
| TIC      | Tecnología de Información y Comunicación                           |
| TLS      | Transport Layer Security   |

|          |  |
|----------|--|
| XML      | Extensible Markup Language                           |
| ONU      | Organización de Naciones Unidas                      |
| OTAN     | Organización del Tratado del Atlántico Norte         |
| OTP      | One-time Password                                    |
| UML      | Unified Modeling Language                            |
| UNASUR   | Unión de Naciones Suramericanas                      |
| UNCITRAL | United Nations Commission on International Trade Law |
| USB      | Universal Serial Bus                                 |
| VPN      | Virtual Private Network                              |
| XMLDSig  | XML Signature  |

*“Todos debemos reflexionar y los que tenemos que tomar decisiones con más razón, por eso yo les ruego a ustedes, los investigadores, (...) que me hagan llegar reflexiones, esas reflexiones de ustedes, que no se queden engavetadas, ¡no!. Necesitamos conocerlas, todos los que tenemos poder de decisión, para enrumbar la nave, ¡para ponerle rumbo a la brújula!”*

*Comandante Hugo Rafael Chávez Frías  
Presidente de la República Bolivariana de Venezuela  
10 de Noviembre de 2006*

***“La Sociedad del Talento”**  
Discurso pronunciado en el acto de Inauguración del  
Centro Nacional de Desarrollo e Investigación en Tecnologías Libres.*

# INTRODUCCIÓN

---

VICTOR BRAVO, RODOLFO SUMOZA

Fundación CENDITEL

La era digital ha implicado incontables cambios en las vidas de muchas personas en todo el mundo. Ya sea indirecta o directamente, buena parte de nosotros posee vínculos con el entorno digital. Utilizamos las Tecnologías de Información y Comunicación (TIC) para desarrollar un sinnúmero de actividades que contribuyen con la estructuración social y cultural. Esto ha involucrado la necesidad de adaptarnos a nuevas formas de percibir y entender la vida, incluyendo la propia forma que nos conocemos o nos damos a conocer, es decir, nuestra forma de hacer sociedad y la manera cómo evolucionan nuestras culturas. Uno de los temas que requiere particular atención en relación con estas ideas es el de la identidad en la Internet, idea de amplio uso en la informática actual y que se ha delimitado y enmarcado bajo el concepto de **Identidad Digital (ID)**.

Esta noción toma elementos del término tradicional de identidad, que en su definición más básica implica el reconocimiento de las personas mediante el uso de características apreciables de forma física, que generalmente son elementos propios y únicos de cada ser humano, como lo son la apariencia, la forma geométrica de la mano o las huellas dactilares. En este sentido, cada país en particular ha adoptado esquemas de identificación para sus ciudadanos que utilizan técnicas estándares más o menos sofisticadas que permiten la interacción social y cultural dentro de una sociedad formada para y en la contemporaneidad. La Identidad Digital promete traer nuevas posibilidades al mundo, pero también se plantea como una nueva dimensión social y personal que se construye con la práctica informática del día a día involucrando nuevos y diversos aspectos técnicos, jurídicos y sociales. Es por ello, que en este nuevo ámbito llamado ciberespacio, no es obligatorio el uso de elementos biométricos para construir la identidad de un individuo, ya que entre otras consideraciones estos elementos ameritan un andamiaje tecnológico que actualmente puede resultar costoso, excesivo o engorroso. Hoy en día, la Identidad Digital no sólo se acota a un documento de identificación, sino que se amplía a todas las características que definen a un individuo y a través de las cuales se puede dar cuenta de su propia existencia en el ciberespacio.

En los últimos 6 años, en la Fundación CENDITEL (Nodo Mérida) se han estado realizando proyectos de investigación y desarrollo en el área de la Identidad Digital. Particularmente se ha trabajado en los temas de Certificación Electrónica, Firma Electrónica, Privacidad y Anonimato, produciendo en este recorrido publicaciones, software y hardware, todo ello bajo las pautas del software libre.

Este libro surge como una iniciativa para dar a conocer los aportes hechos desde la Fundación y con la intención de que los lectores que no estén cercanos a estos temas de estudio los conozcan. Se presentan aspectos importantes de la seguridad informática, de manera que el lector tenga las bases teóricas necesarias para la apropiación de las propuestas hechas en CENDITEL.

El libro se divide en tres partes, la primera de ellas orientada a fundamentar el tema en estudio desde diferentes perspectivas. Así, en el primer capítulo se describen conceptos estrechamente vinculados a la identidad digital, utilizando una estrategia de revisión de términos y tecnologías que se consideran claves dentro del contexto venezolano y latinoamericano. Seguidamente, en el segundo capítulo se desarrolla una propuesta de “Políticas de seguridad de la información en software libre” aplicables directamente a pequeñas y medianas organizaciones, pudiendo ser útiles también para usuarios particulares que trabajen en ambientes informáticos. En el tercer capítulo se introduce el tema de Anonimato, concepto que abre el espectro del estudio sobre la seguridad y protección de la identidad, ya que incluye aspectos sobre el comportamiento y accionar humano, cuyo registro y perfilamiento hacen vulnerables a las personas. Para finalizar la primera parte, se discuten las principales ideas relacionadas con este tema en el área jurídica actual venezolana y sus repercusiones en los ámbitos técnicos y sociales del país.

La segunda parte contiene cuatro artículos que fueron publicados en espacios de divulgación tales como congresos o revistas científicas, que se han compilado en este libro con la finalidad que tuvieran mayor difusión. Bajo este esquema, se presenta un artículo sobre el desarrollo de una aplicación de gestión para Autoridades de Certificación Raíz de una PKI. Un segundo artículo muestra un método para integrar firmas electrónicas en procesos de negocio. Sobre anonimato se presentan dos artículos: el primero de ellos muestra una propuesta que implica utilizar estrategias bioinspiradas para la optimización en un sistema para proveer anonimato y el segundo propone una nueva forma de medir los niveles de anonimato para este tipo de sistema.

Finalmente, en la tercera parte se realiza una discusión desde los puntos de vista políticos y sociales sobre el tema de la identidad digital, ofreciendo reflexiones y apreciaciones signadas por los acontecimientos recientes en este ámbito.



# FUNDAMENTOS: SEGURIDAD E IDENTIDAD DIGITAL

---



## CAPÍTULO 1



# BASES DE LA IDENTIDAD DIGITAL

---

ANTONIO ARAUJO, VÍCTOR BRAVO Y RODOLFO SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

En este capítulo se pretende explicar el tema de la identidad digital (ID) y en ese sentido se presentan varias definiciones para colocar en contexto al lector. Inicialmente se muestran conceptos sobre la propia *Identidad Digital*, luego se explican términos relevantes como el de *rol*, *identidad parcial*, *manejo de la identidad*, y la *protección de la identidad*, que involucran el área de la *privacidad*, *anonimato*, *seudonimato*, *certificación* y *firma electrónica*.

### 1.1. Identidad Digital ID

A continuación se presentan de manera resumida varios conceptos de Identidad Digital utilizados como base del trabajo [1]:

1. Es el conjunto de datos que describen y representan a un sujeto: persona, grupo de personas o cosas de manera única. Puede contener información sobre gustos, creencias, relaciones, tendencias, ideologías, y cualquier otro descriptor vinculado al sujeto.

2. Es la suma de toda la información disponible en formato digital de un sujeto (persona, grupo de personas, cosas).
3. Puede ser explicada como una percepción única o exclusiva de vida, con su integración a un grupo social, y con continuidad, la cual está acotada y formada por una sociedad. La identidad puede estar ligada a cualquier sujeto, ya sean seres humanos, personas jurídicas, y dispositivos electrónicos.
4. La identidad es un conjunto de atributos pertenecientes a un individuo que permiten diferenciarlo del resto de individuos que forman parte de un conjunto determinado. Por esta razón no existe una identidad única y universal, sino que pueden existir varias para un mismo individuo, según el conjunto y contexto al que se haga referencia. Incluso los valores de los atributos y los atributos mismos pueden cambiar en el tiempo.
5. La identidad digital denota la atribución de propiedades a una persona, las cuales son, desde el punto de vista técnico, operacionalmente accesibles de forma inmediata, por su característica digital. El identificador de una identidad parcial digital puede ser una dirección de correo electrónico en un grupo de noticias o en una lista de correos.

### **1.1.1. Identidad Parcial**

Una identidad parcial es un subconjunto de atributos del conjunto que compone la identidad completa, formada por la unión de todos los atributos de esta persona. Desde un punto de vista técnico, estos atributos constituyen datos. Como se mencionó anteriormente estos atributos y valores pueden variar en el tiempo. Un seudónimo puede considerarse como una identidad parcial. La identidad de cada persona está compuesta por muchas identidades parciales, las cuales representan a la persona en un contexto o rol específico.

### **1.1.2. Rol**

Desde el punto de vista de la Sociología un rol o rol social constituye un conjunto de acciones conectadas o relacionadas, conceptualizadas por los actores en una situación social. Es frecuente definirlo como un comportamiento esperado en un contexto individual social dado.

El Rol en Informática es un término vinculado a la Seguridad de las Tecnologías de Información y Comunicación (TIC) y su significado es el de la función que un usuario tiene al utilizar un sistema. Las funciones les dan acceso a diferentes niveles de seguridad.

### **1.1.3. Manejo de la ID**

En Identidad Digital se logran distinguir dos instancias de los sujetos (personas, grupos de personas o cosas): la primera es la definición de sí mismo (autodefinición interior y personal), y la segunda es la que los define en un contexto social con sus respectivos atributos, que se mantienen para dar la posibilidad de acceso a la comunicación y que los ata de cierta manera a un control y un grado de consistencia con respecto al resto.

El manejo de la ID implica la gestión de varias identidades parciales (usualmente denotadas por seudónimos) de un individuo. Establecer la reputación es posible cuando un individuo reutiliza las identidades parciales. Un prerequisite para la selección de una identidad parcial es el de conocer el contexto en el que la persona está actuando.

#### **1.1.3.1. Sistema de manejo de la identidad**

Se refiere a la administración y diseño de los atributos de las identidades. Se puede distinguir entre un sistema de manejo de identidad y una aplicación para el manejo de la identidad: La primera puede ser entendida como una infraestructura, y la segunda como un conjunto de componentes coordinados entre sí. Las aplicaciones para el manejo de la identidad son herramientas para manejar individualmente sus comunicaciones relevantes, las cuales pueden ser configuradas y operadas en el lado de los usuarios o en el lado de los servidores. El manejo de la identidad, soportado técnicamente, tiene que autorizar a los usuarios para reconocer diferentes

tipos de comunicaciones o situaciones sociales, y acceder a ellas con respecto a su relevancia, funcionalidad y al nivel de riesgo de la privacidad y seguridad en función de hacer y asumir roles de forma adecuada.

En general, las aplicaciones para el manejo de la identidad, específicamente en cuanto al manejo de las identidades parciales, representan los diferentes seudónimos con sus respectivos datos de acuerdo a los diferentes roles que el usuario ha asumido y de acuerdo a los diferentes patrones de comunicación. En los casos donde se hace explícito el flujo de los datos personales, donde se le permite al usuario tener un mayor grado de control, la guía principal es la de “reconocer y escoger” su propia identidad, y se procura minimizar la cantidad de los datos utilizados. En una situación y contexto específico, tal sistema le da soporte al usuario en la selección de seudónimos que representen a sus identidades parciales.

## **1.2. Protección de la ID**

Ya establecido el contexto terminológico, es importante mencionar que la gestión o manejo de la ID depende de las tecnologías de información y comunicación, las cuales involucran niveles de riesgos, vulnerabilidades, etc. que aumentan el uso y desarrollo de técnicas, protocolos, mecanismos y demás elementos enfocados en su protección.

### **1.2.1. Certificación Electrónica**

Uno de los mecanismos comunes para establecer identidades digitales es a través de la certificación electrónica, ésta comprende la gestión de procesos en los que se emplean elementos como software, dispositivos y documentación de políticas que permiten establecer identidades digitales a individuos o dispositivos. La certificación electrónica se usa en organizaciones privadas o públicas, dentro de los países y a nivel mundial.

Los elementos que se gestionan en los procesos de la certificación electrónica se describen con mayor detalle en la sección 1.3. En los capítulos 5 y 6 de la segunda parte de este libro, se presentan aportes concretos de la Fundación CENDITEL sobre certificación electrónica.

### **1.2.2. Firma Electrónica**

Similar a la firma autógrafa de un ser humano, la firma electrónica es un mecanismo para establecer la voluntad de aceptación del contenido de un documento en formato electrónico y por lo tanto establece una herramienta muy útil para la gestión de la ID. Se apoya en los procesos y elementos empleados en la certificación electrónica para permitir que un individuo o dispositivo pueda firmar electrónicamente cualquier documento, archivo o cadena de bytes.

En la sección 1.3 se presenta con mayor detalle la noción de firma electrónica. En el capítulo 6 de la segunda parte de este libro, se presenta un aporte de la Fundación CENDITEL sobre el uso de firmas electrónicas avanzadas en la gestión de procesos organizacionales.

### **1.2.3. Registro del comportamiento**

#### **1.2.3.1. Análisis de Tráfico**

Tal como se menciona en [2] el Análisis de Tráfico tuvo sus orígenes durante la Segunda Guerra Mundial, incluyendo su relación con el ataque que se hizo sobre Pearl Harbour. Actualmente Google utiliza los enlaces

de incidencia para evaluar la importancia de las páginas web, las compañías de tarjetas de crédito examinan las transacciones para descubrir patrones de gastos fraudulentos. La idea de fondo de esta técnica radica en que durante el tráfico de datos se pueden registrar el tiempo y la duración de la comunicación, y se examina esta información para determinar la forma detallada del flujo de datos, las identidades de las partes que se comunican, y lo que puede ser establecido sobre su ubicación. Incluso los datos pueden ser poco precisos o estar incompletos, y simplemente a través del conocimiento de patrones típicos de comunicación se podría inferir sobre una comunicación en particular que se esté observando.

Esta técnica a pesar de que obtiene información de menor calidad en comparación a la obtenida con las técnicas del criptoanálisis, es mucho más fácil, barata y viable en cuanto a la extracción y procesamiento del tráfico de datos. El Análisis de Tráfico ha inspirado a otras técnicas utilizadas para la protección de sistemas, y para la construcción de sistemas de confianza. En cuanto al Análisis de Tráfico del protocolo de seguridad SSH (cónsola de comandos segura, o SSH por sus siglas en inglés), a pesar de que ofrece comunicaciones seguras para acceder a terminales remotos a través de un proceso de autenticación que utiliza mecanismos de clave pública, y que luego de este proceso toda la información viaja cifrada garantizando su confidencialidad e integridad, en [3] se muestra que aun existe gran cantidad de información que se deja pasar sin ocultarse. En su modo interactivo, el protocolo SSH transmite cada pulsación de tecla como un paquete distinto y de esta forma la longitud de la clave puede ser trivialmente descubierta. Además, dado que la distribución de los teclados no es aleatoria, y que las claves con frecuencia están basadas en palabras reales, el tiempo exacto de las pulsaciones de teclas está relacionado a qué tan rápido un carácter particular puede ser tipeado después de otro. Esto implica que al haber una suficiente variabilidad entre los patrones de tipeo de las personas entonces existe la posibilidad de identificarlos, particularmente después de observar una secuencia larga.

El Análisis de Tráfico de los protocolos introducidos para proveer accesos web privados (Secure Sockets Layer o SSL y el Transport Layer Security o TLS), se basa en estudiar la información que aún deja escapar este protocolo cuando se establece una comunicación web hacia un servidor. Los navegadores solicitan recursos, que son normalmente páginas HTML, y éstas a su vez están asociadas a otros recursos adicionales como imágenes, tablas, etc., los cuales pueden ser descargados a través de enlaces cifrados, pero su tamaño aún puede ser determinado por el observador, quien puede inferir cuáles páginas están siendo accedidas (por ejemplo podrá inferir cuáles reportes de una compañía están siendo descargados). Incluso, estudiando el comportamiento de los sistemas de almacenamiento local de las páginas visitadas en la web (web cache) puede inferirse cuáles sitios web se han accedido con sólo reconocer el patrón de almacenamiento en los cache de cada uno.

También se puede determinar la identificación de los dispositivos en la red sólo con estudiar el comportamiento y las características particulares de los cambios del reloj en cada dispositivo.

#### **1.2.4. Privacidad vinculada a la ID**

La privacidad está vinculada a la información proveniente de cualquier fuente que se relacione a un individuo y que éste desea que no se divulgue públicamente. Esta información puede estar contenida en los perfiles que se tienen del individuo, los cuales son conjuntos de atributos que se consideran identidades parciales de las personas. Cuando terceros (atacantes) crean estos perfiles de las personas para realizar hechos negativos (no deseados) contra ellas, a través de ataques como el Análisis de Tráfico sin autorización, se considera que existe una vulnerabilidad que debe ser protegida. Es por eso que en el contexto de la Identidad Digital, y su protección, están involucradas las técnicas y procedimientos para proteger la Privacidad, y puntualmente se puede hablar de Anonimato al procurar evitar la creación de dichos perfiles sin autorización.

##### **1.2.4.1. Anonimato**

Se vincula a los usuarios (sujetos) que utilizan un sistema de comunicación, y que en general puede decirse que un sujeto es anónimo cuando no puede ser identificado dentro de un conjunto de sujetos, denominado el conjunto anónimo. Este conjunto está conformado por todos los posibles sujetos que pueden causar (o estar relacionados con) una acción. "No ser identificado" significa que ese sujeto no puede ser caracterizado de forma única o particular dentro de ese conjunto. Un sujeto actúa anónimamente cuando, desde el punto de vista del adversario, su acción no puede relacionarse con su identidad, dado que hay un conjunto de sujetos

que podrían ser los causantes potenciales de la acción (y el adversario no puede distinguir a su verdadero causante). El anonimato debe permitirle a un sujeto utilizar un recurso o servicio sin revelar su identidad, esto implica que el anonimato por sí mismo no procura proteger la identidad de un usuario en un ámbito general, lo que pretende es evitar que otros usuarios o sujetos puedan determinar la identidad de un usuario cuando éste genera una acción u operación en particular.

#### 1.2.4.2. Seudonimato

La palabra seudónimo proviene del griego *pseudonumon* la cual significa “nombre falso”, es decir, un nombre distinto al “nombre real”. Sin embargo, como el “nombre real” tiene también un origen arbitrario, el nombre de seudónimo puede ser extendido a todos los identificadores o cualquier otra cadena de bits que identifique a un sujeto. Tal como se expresa en [1], los seudónimos son identificadores (nombres u otras cadenas de bits) de sujetos. Para el caso que se está tratando, son los identificadores de los emisores y receptores de mensajes. Es posible que en algunos casos convenga agrupar los nombres reales en un conjunto distinto al de los “nombres falsos” (no considerados reales), pero en otros casos un “nombre real” puede ser considerado como un seudónimo que resulta de una selección inicial, para la identificación de un sujeto. Incluso, en gran parte de la literatura excluyen la fracción que le da el nombre de “falso” (“pseudo”), y sólo utilizan, para referirse a nombres de seudónimos, la palabra *nym*s. Desde un punto de vista más básico (fundamental), un seudónimo puede ser considerado como un tipo de atributo del sujeto, que puede ser controlado por el diseñador de sistemas o por el mismo usuario.

Se pueden generalizar los seudónimos como identificadores de sujetos particulares o conjuntos de sujetos que son sus contenedores. En las configuraciones tradicionales se asume que cada seudónimo se refiere a un solo contenedor, invariante sobre el tiempo, el cual no puede ser transferido a otros contenedores. Algunos tipos especiales de seudónimos pueden ser solamente extendidos y transferidos a otros contenedores, por ejemplo, un seudónimo de grupo se refiere a un conjunto de contenedores, y un seudónimo transferible puede ser transferido de un contenedor a otro. Utilizando la noción de seudónimo de grupo, se podría inducir el conjunto anónimo: Utilizando la información provista por el seudónimo solamente, un atacante no podría decidir si una acción fue ejecutada por una persona específica dentro del conjunto.

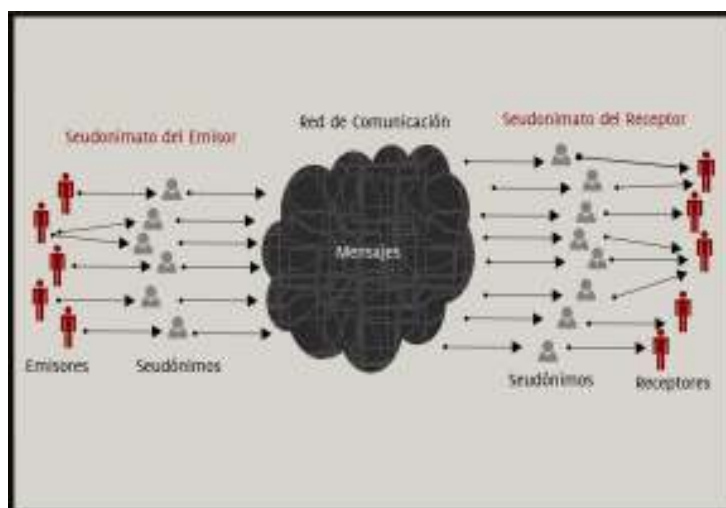
En resumen, utilizando un criterio formal, un seudónimo se puede considerar como el estado de utilizar un “nombre falso” como identificación (ID), y seudonimato se puede definir como el proceso donde se utilizan los seudónimos como identificadores. El seudonimato tiene como uno de sus principales objetivos el permitirle a un usuario utilizar un recurso o servicio sin tener que revelar su verdadera identidad, y sin quitarle la responsabilidad sobre el uso del mismo.

Es evidente, por definición, que el anonimato y la responsabilidad son extremos opuestos con respecto a la relacionabilidad de los sujetos, sin embargo, a través del uso del seudonimato se procura establecer un punto intermedio para cumplir con ambas partes: Responsabilizar a los usuarios (sujetos) de sus acciones y evitar que se revele su identidad. Incluso utilizando el mismo seudónimo, le puede permitir al sujeto tener cierto nivel de reputación (esto suponiendo que existen los mecanismos adecuados para poder autenticar los mensajes enviados por el contenedor del seudónimo). Además, existen configuraciones de sistemas anónimos que permiten evitar el abuso en su utilización, pudiendo revelarse, en ciertos casos, la identidad del usuario que haya incurrido en cualquier tipo de acciones no permitidas (esto en el supuesto que sólo determinadas autoridades certificadas pueden revelar esta identidad).

El seudonimato del emisor se define como el uso de seudónimos por parte del emisor, y el seudonimato del receptor se define como el uso de seudónimos del receptor. En la figura 1.1 se representa esta noción de seudonimato (extraída de [1]).

Cuando se utilizan “nombres falsos” como etiquetas que identifican a un sujeto, es conveniente considerar cómo se trata o maneja la responsabilidad y la autorización. Es decir, los seudónimos digitales pueden ser utilizados para autenticar los mensajes, ya que un seudónimo digital es una cadena de bits que dentro de este contexto es un ID único del sujeto, el cual puede ser utilizado para autenticar el ítem de interés o IDI del contenedor relativo a su seudónimo, esto implica que la responsabilidad puede ser manejada a través del uso de seudónimos. Sin embargo, ello puede no ser suficiente para alcanzar este tipo de gestión de la responsabilidad, por tal motivo en algunos casos prácticos, es necesario acompañar al seudónimo con otro tipo de pruebas de

validez (tales como firmas digitales), y/o utilizar terceras partes (autoridades de certificación digital) que le den validez a los seudónimos.



**Figura 1.1** Seudonimato

Se pueden considerar las siguientes definiciones del seudonimato con respecto al anonimato:

**Seudónimo público:** La relación entre un seudónimo y su contenedor puede ser de conocimiento público, por ejemplo podría estar en una lista o directorio público.

**Seudónimo no público:** La relación inicial del seudónimo y su contenedor puede ser conocida por ciertas partes (entidades de control o administración centralizada o descentralizada), pero no son del conocimiento público.

También se pueden considerar otros tipos de seudónimos:

**Seudónimo personal:** Es un subtítulo para el nombre del contenedor el cual está relacionado con su identidad civil por ejemplo el número de la cédula de identidad o pasaporte.

**Seudónimo por rol:** Está limitado a roles específicos, es decir, su asignación está relacionada a los roles que desempeña el contenedor. Por ejemplo, los seudónimos que comúnmente se utilizan bajo el rol de “usuario de Internet” son denominados “nombre de usuarios”.

**Seudónimo por transacción:** Un mismo contenedor podría tener un seudónimo por cada transacción que realice.

El nivel de anonimato en relación al tipo de estrategia de utilización de seudónimos se representa en la figura 1.2.

En general, el anonimato del seudónimo por rol, y del seudónimo por relación es más fuerte que el anonimato debido al uso de seudónimos personales. La fortaleza del anonimato se incrementa con la aplicación de seudónimos por rol y relación. El último nivel de fortaleza se consigue utilizando los seudónimos por transacción dado que no existe información sobre la relación entre cada una de las transacciones. En ocasiones, se utiliza el nombre de seudónimo de un solo uso para denotar los seudónimos por transacción. La fortaleza del anonimato antes mencionada se refiere a que desde un punto de partida se define que el mayor nivel (fortaleza) de anonimato se logra cuando no se proporciona información sobre la identidad en absoluto. En otras palabras, el anonimato es más fuerte mientras menos datos personales del contenedor puedan ser relacionados



**Figura 1.2** Seudonimato con respecto al Anonimato

al seudónimo, y mientras los seudónimos sean utilizados con menor frecuencia (estos es cuando un mismo contenedor utiliza un mayor número de seudónimos).

Un seudónimo digital se puede conformar con el uso de algún mecanismo de clave pública utilizado para probar las firmas digitales, donde los contenedores del seudónimo pueden probar que son los verdaderos “dueños” del seudónimo solamente construyendo una firma digital creada con su clave privada. En la mayoría de los casos los seudónimos digitales son las mismas claves públicas generadas por los propios usuarios.

Un certificado de clave pública contiene una firma digital de una determinada autoridad de certificación que provee algún tipo de seguridad cuando un mismo sujeto utiliza la clave pública para otro de sus seudónimos. En el caso de que el seudónimo provenga del nombre real de un sujeto, se le llama certificado de identidad. Un certificado de atributo es un certificado digital que contiene más cantidad de información (atributos) y claramente se refiere a un certificado específico de clave pública. Independientemente de los certificados, los atributos también pueden ser utilizados como identificadores de conjuntos de sujetos, no sólo de sujetos particulares.

#### 1.2.4.3. No relacionabilidad

La no relacionabilidad sólo tiene sentido práctico si previamente se han definido las propiedades del anonimato, seudonimato y no-observabilidad de dichos sistemas, y se han caracterizado las entidades o ítems de interés que se desean relacionar (por parte del atacante). En [1] se menciona que las entidades o ítems de interés (IDI) son sujetos, mensajes, eventos, acciones, etc. La relacionabilidad se considera a la información que se tiene sobre la relación real que existe entre los IDIs, es decir, que en todos los casos reales existirá cierta relación entre ellos y la relacionabilidad es la información respecto a ésta. Por ende, la no relacionabilidad, desde la perspectiva del adversario, significa que la información obtenida después de un ataque es la misma información que se tenía antes del mismo, es decir, los IDIs no están ni más ni menos relacionados comparando el periodo anterior y posterior al ataque. Desde la perspectiva probabilística, la no relacionabilidad significa que la probabilidad de que dos o más ítems de interés están relacionados (desde la perspectiva del atacante) es la misma antes y después del ataque.

La no relacionabilidad debe implicar que el usuario puede hacer múltiples usos de un recurso o servicio sin que esto conlleve a que el adversario pueda establecer una relación entre estos usos, es decir, requiere que los usuarios y/o los sujetos no tengan la disponibilidad de determinar que cierto usuario fue el causante de cierta acción en el sistema.

Si se considera que el envío y recepción de mensajes son los IDIs, el anonimato puede ser definido como la no relacionabilidad de uno de ellos con cualquier identificador de un sujeto (en este caso un emisor o un

receptor). Específicamente, el anonimato de un IDI es la no relación con cualquier sujeto y el anonimato de un sujeto es su no relación con cualquiera de ellos. De esta manera se puede considerar anonimato del emisor como las propiedades que hacen que un emisor no pueda ser relacionado con ningún mensaje, y que un mensaje no pueda ser relacionado con ningún emisor.

De igual forma, el anonimato del receptor significa que un mensaje no puede ser relacionado con ningún receptor, y un receptor no puede ser relacionado con ningún mensaje. La relación de anonimato es la imposibilidad de determinar quién se comunica con quién, es decir, el emisor y el receptor son no relacionables.

La no relacionabilidad es una condición suficiente para el anonimato, pero no es una condición necesaria. Incluso en algunos casos se puede considerar que aun fallando la propiedad de la no relacionabilidad se puede conseguir un nivel de anonimato alto. Esto si se hace referencia a la definición estricta del anonimato: no poder ser identificado dentro de un conjunto de sujetos.

#### 1.2.4.4. No observabilidad

En contraste con la definición de anonimato, y la de no relacionabilidad, donde se considera la protección de la relación del IDIs con respecto a los sujetos o a otros IDIs, la no observabilidad considera la protección de los IDIs en sí mismos, ya que se define como el estado de que un IDI sea indistinguible entre un conjunto de IDIs del mismo tipo (el “tipo” lo definen las características de interés en cada caso, por ejemplo, considerar la emisión de mensajes como un IDI, tiene su características propias, que hacen que se pueda diferenciar de otro tipo de IDI). Por ejemplo, se podría decir que al ser no observable, no es posible distinguir entre un mensaje y el ruido aleatorio.

Semejante al caso del anonimato, también se tienen conjuntos de sujetos no observables con respecto a esta propiedad. Es decir, el conjunto de emisores no observables tiene la propiedad de que cada emisor no puede ser distinguido del resto y el conjunto de receptores no observables tiene la propiedad de no poderse distinguir, desde el punto de vista del atacante, de un receptor en el resto de los receptores de ese conjunto. La relación de no observabilidad de esta forma significa que no es posible distinguir entre un emisor y un receptor que intercambian un mensaje, es decir, si se considera un mensaje en particular entonces el conjunto de la relación de no observabilidad está compuesto por todos los posibles pares emisor-receptor, entre los cuales no se podría diferenciar o determinar que existe una relación de envío-recepción. En la figura 1.3 se puede observar gráficamente la configuración de dichos conjuntos.

Desde una perspectiva de usuario, la no observabilidad se podría definir como la propiedad de que un usuario pueda utilizar un recurso o servicio sin que otros (terceras partes) tenga la posibilidad de determinar que el recurso o servicio está siendo utilizado.

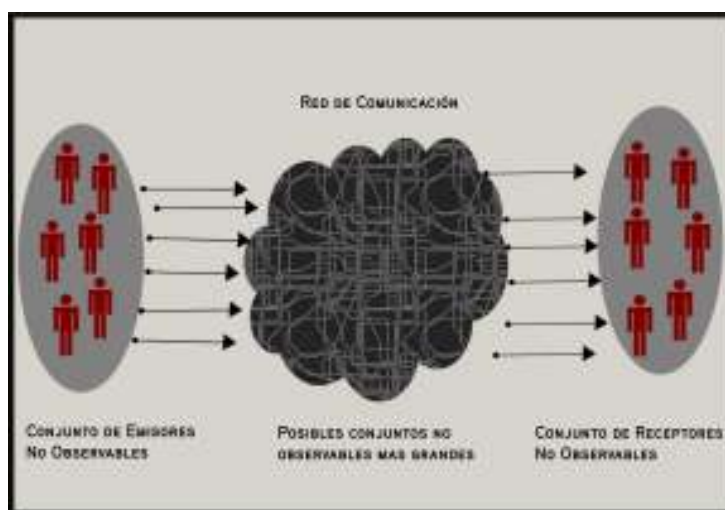


Figura 1.3 Conjuntos No Observables



### 1.3. Técnicas de verificación de identidad

Hasta ahora se han descrito conceptos básicos sobre la Identidad Digital. También se ha visto que es posible asignarla a seres humanos, personas jurídicas y hasta dispositivos electrónicos para realizar acciones en distintos entornos. En general, las acciones que se pueden realizar están supeditadas a su verificación, ya sea al momento de su ejecución o después de ejecutada.

Al momento de realizar una acción se verifica la Identidad Digital de un usuario (individuo o dispositivo electrónico) para garantizar que ésta sea reconocida como válida dentro del universo de usuarios existentes. Por ejemplo, un usuario puede enviar un correo electrónico en una red de computadores si tiene su identificador de correo y su respectiva contraseña. Existe toda un área de investigación sobre mecanismos para establecer lo que una entidad puede hacer luego de demostrar su identidad digital en sistemas informáticos, esta corresponde con los sistemas de autorización.

La verificación de la Identidad Digital de un usuario luego de ejecutada una acción, puede ser utilizada para establecer responsabilidades legales de un individuo ante acciones realizadas en sistemas informáticos o en comunicaciones electrónicas. La Identidad Digital apoyada en el uso de distintas técnicas y mecanismos permite que un ser humano pueda interactuar con el amplio abanico de servicios que existen en la actualidad.

Así como en el mundo físico una persona utiliza algún mecanismo para demostrar su identidad, ya sea por un documento, una tarjeta de afiliación u otro mecanismo, en los entornos digitales se utilizan distintos mecanismos para demostrar y verificar la Identidad Digital de las personas o dispositivos electrónicos. En las siguientes secciones se describen algunas técnicas empleadas para tales fines y se muestran ejemplos de aplicaciones comunes.

#### 1.3.1. Contraseñas

Las contraseñas son quizás, el método más utilizado para asociar una identidad a personas en el mundo digital. Una contraseña en este ámbito se refiere a una secuencia de caracteres secreta que se utiliza generalmente en combinación con un nombre de usuario o correo electrónico para obtener acceso a determinados recursos de un sistema informático. El sistema informático puede estar en la web, funcionar en un computador sin acceso a red, o ser un sistema dedicado tal como un cajero automático de banco, o un mecanismo de control para el acceso a un lugar físico. El acceso al correo electrónico, a una sesión en una computadora, al sitio de un banco en la Internet, la acción para desbloquear un teléfono móvil, así como actividades que se hacen a diario con los dispositivos lo utilizan como sistema primigenio y en muchas ocasiones como único procedimiento disponible para este fin.

En primer lugar, para construir un sistema de contraseñas se necesita un almacén de datos, en el cual se guarden los datos vinculados con la clave que pueden representar el ámbito de operación de un usuario dentro de un sistema informático, lo cual incluye esquemas de autorización para operar sobre objetos o generar acciones.

Muchas veces los almacenes de datos para los esquemas de contraseñas se construyen usando archivos de texto (por ejemplo, los sistemas Linux o Unix que utilizan el archivo */etc/shadow*), o también es muy frecuente utilizar un conjunto de relaciones u objetos en una base de datos.

Algunas de las reglas básicas para almacenar contraseñas se muestran a continuación:

- Utilizar esquemas de seguridad para el resguardo de la base de datos acorde con las reglas generales de administración de servidores, sistemas de cómputo embebido o cualquier otro tipo de sistema donde resida el almacén de datos.
- No guardar las contraseñas en texto plano, en su lugar utilizar algoritmos (con la suficiente fortaleza contra ataques) de una sola vía para transformar las claves que ingrese el usuario.
- Implementar políticas y protocolos de creación y asignación de claves tales como: vinculación a dos o más correos electrónicos; prueba de fortaleza de contraseñas; monitorear los accesos de los usuarios por lugar, frecuencia; operaciones entre otras.

- Realizar auditorías periódicas a todo el proceso de gestión de claves.

Uno de los objetivos que debe tener cualquier sistema de protección es proveer al usuario de instrumentos para mejorar su interacción con los sistemas informáticos, evitándole hacer tareas engorrosas o difíciles, sin que esta prerrogativa desmejore significativamente los niveles de seguridad. En este sentido, actualmente están disponibles varias tecnologías vinculadas con la gestión de contraseñas, que generalmente son implementadas por todos los navegadores para la Internet, entre ellas están:

- **Cookies:** también denominadas galletas informáticas, son pequeñas porciones de información sobre los datos de acceso a una aplicación (sesión) .
- **Listas de claves:** Es una lista donde se encuentran asociadas las claves y nombres de usuarios con los sitios que se visitan en la Internet. Cuando el usuario visita un sitio web que se encuentra en la lista, el navegador ingresa automáticamente el nombre de usuario y su clave en el formulario.
- **Sistemas centralizados o locales de gestión de claves:** son aplicaciones en la web o de uso local (computadora, tableta o teléfono móvil) para gestionar las claves de todos los sistemas al que los usuarios acceden desde sus dispositivos electrónicos.

Por otra parte, para que una contraseña sea resistente a ataques de fuerza bruta, debe contar con varias propiedades como las descritas más adelante. Muchos sistemas verifican las claves antes de que sean asignadas, pero no pueden asegurar de forma completa que la contraseña es inviolable dado que mucho de la responsabilidad de uso reside en el propietario de la clave: el usuario.

Generalmente para que una contraseña sea considerada fuerte, debe tener por lo menos las siguientes propiedades:

- Ser lo suficiente larga. Hoy en día, se considera ocho (8) caracteres la extensión mínima de una contraseña para la mayoría de los sistemas informáticos, este número puede disminuir si se acompaña con el uso de una tarjeta o elemento físico seguro (*token*).
- No ser una palabra contenida en diccionarios.
- Estar compuesta por letras minúsculas, mayúsculas y caracteres especiales.

Muchos sistemas informáticos cuentan entre sus políticas el cambio periódico de claves por parte de los usuarios, con respecto a ello Schneier en [3] considera que la política citada puede ser contraproducente y no se recomienda, debido a que si ya se cuenta con una contraseña fuerte no existe la necesidad de cambiarla.

Se estima que las contraseñas como método de control de acceso seguirán siendo el método más popular varios años más, por lo tanto se hace necesario prestar atención en los aspectos de gestión organizacional y técnica de este tipo de herramienta, para lograr conectar de manera eficiente las políticas con las aplicaciones y con las personas, tomando en cuenta que no se debe disminuir demasiado la ergonomía en pro de la seguridad.

### 1.3.2. Certificados electrónicos

A una persona que desea realizar un trámite o solicitar un servicio en una institución pública o privada generalmente se le exige que demuestre su identidad para ser atendida. La manera común en la que se demuestra la identidad de un individuo es a través de su documento de identidad o cédula de identidad. Por ejemplo, un pensionado del seguro social debe presentar su cédula de identidad para retirar dinero de su cuenta de banco, así como un solicitante de un préstamo para adquisición de vivienda principal debe presentar, entre otros requisitos, su cédula de identidad. En general todas las personas utilizan la cédula de identidad como un documento físico que garantiza su identidad ante otras personas, instituciones, empresas e inclusive ante otros países. En la figura 1.4 se muestra una cédula de identidad de un ciudadano de la República Bolivariana de Venezuela.

En la sociedad digital en la que se desenvuelven muchos individuos en la actualidad, es necesario utilizar algún mecanismo que permita establecer su identidad digital. Una alternativa es el certificado electrónico.



**Figura 1.4** Cédula de identidad de la República Bolivariana de Venezuela.

Éste es un documento electrónico que asocia un conjunto de datos digitales a un usuario para establecer su identidad. Así como la cédula de identidad incluye datos de una persona como nombres, apellidos, fecha de nacimiento y estado civil, los certificados electrónicos también incluyen datos que permiten establecer la identidad digital de su titular y tienen un periodo de validez.

La cédula de identidad es emitida por una institución pública en la que los ciudadanos confían por cuanto cumple estándares que la hacen difícil de falsificar. En el caso de los certificados electrónicos se busca mantener estas mismas características al ser emitidos por una entidad con la que tanto individuos como sistemas informáticos tengan una relación de confianza.

Los certificados electrónicos son un elemento fundamental en el modelo de confianza denominado *Infraestructura de Clave Pública* (PKI por sus siglas en inglés). Este modelo describe una tecnología utilizada para establecer identidades a través de certificados electrónicos y permitir el intercambio de información segura entre partes que se comunican. La PKI agrupa programas o software, piezas de hardware y documentación de políticas para establecer lo que se puede hacer o no con un certificado electrónico.

Los certificados electrónicos están basados en la criptografía de clave pública. Este tipo de criptografía aprovecha el uso de un par de claves con características muy particulares para transmitir información.

Al usarse criptografía de clave pública en una comunicación entre dos personas cada una genera un par de claves. El par de claves tiene la propiedad de complementarse entre sí, de forma que los datos cifrados usando una de ellas se pueden descifrar usando la otra. Una de las claves va a ser conocida por la persona con quien se desea establecer la comunicación y es denominada *clave pública*, la otra clave va a ser secreta y protegida por su titular y es denominada *clave privada*. El objetivo de un certificado electrónico es asociar la clave pública de un usuario con su identidad. De esta manera, una persona presenta su certificado electrónico ante un sistema informático para demostrar su identidad digital.

En la República Bolivariana de Venezuela existe una ICP jerárquica denominada *Infraestructura Nacional de Certificación Electrónica*. Constitucionalmente se fundamenta en la Providencia Administrativa Número 016 del 05 de Febrero de 2007 de la Gaceta Oficial Número 38.636<sup>1</sup>. Esta jerarquía es supervisada y controlada por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE)<sup>2</sup>, organismo adscrito al Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología.

La *Infraestructura Nacional de Certificación Electrónica* incluye los siguientes elementos:

<sup>1</sup><http://www.tsj.gov.ve/gaceta/marzo/020307/020307-38636-27.html>

<sup>2</sup><http://suscerte.gob.ve/>

- Autoridad de Certificación (AC) Raíz del Estado Venezolano<sup>3</sup>. Es la base sobre la cual se inicia la relación de confianza de la *Infraestructura Nacional de Certificación Electrónica*. Se encarga de emitir, renovar, revocar y suspender los certificados electrónicos de los Proveedores de Servicios de Certificación.
- Autoridades de Certificación de los Proveedores de Servicios de Certificación (PSC). Entidades subordinadas a la Autoridad de Certificación Raíz del Estado Venezolano y se encargan de emitir, renovar, revocar y suspender los certificados electrónicos a los signatarios y a sus Autoridades de Certificación subordinadas, en caso de tenerlas.
- Autoridades de Registro de los Proveedores de Servicios de Certificación. Entidades encargadas de controlar la generación de los certificados electrónicos de sus Autoridades de Certificación y comprobar la veracidad y exactitud de los datos suministrados por los signatarios. Generalmente las Autoridades de Registro y las Autoridades de Certificación de los PSC son vistos como una sola entidad de la PKI.
- Signatarios o titulares de certificados electrónicos emitidos por los PSC.

En la figura 1.5 se muestra un bosquejo de la Infraestructura Nacional de Certificación Electrónica.



**Figura 1.5** Infraestructura Nacional de Certificación Electrónica.

Cuando una persona necesita una Identidad Digital en la Internet, puede recurrir a un PSC para que le venda o asigne un certificado electrónico de acuerdo a sus respectivos documentos de políticas de certificados y declaración de prácticas de certificación. Estos documentos establecen las normas y usos de los certificados electrónicos emitidos por cada Autoridad de Certificación. En el capítulo 4 se presentan los fundamentos jurídicos de los certificados electrónicos.

Hasta el momento de publicación de este libro, en Venezuela los PSC acreditados ante la SUSCERTE son los siguientes:

- Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico<sup>4</sup>, organismo adscrito al Ministerio del Poder Popular para la Educación Universitaria, Ciencia y Tecnología.
- Proveedor de Certificados (PROCERT<sup>5</sup>), C.A., primera entidad privada dentro de la República Bolivariana de Venezuela en ser acreditada ante el Estado Venezolano.

<sup>3</sup><http://acraiz.suscerte.gob.ve/>

<sup>4</sup><https://ar.fii.gob.ve>

<sup>5</sup><https://www.procort.net.ve/acprocert.asp>

Los certificados electrónicos se utilizan principalmente para:

- Autenticación de usuarios. Los certificados electrónicos permiten demostrar la identidad de usuarios.
- Enviar y recibir información cifrada hacia y desde terceros. Con los certificados electrónicos se puede enviar información cifrada que sólo podrá ser vista por destinatarios específicos a través de algoritmos criptográficos. Esto proporciona confidencialidad entre las partes que se comunican.
- Firmar electrónicamente documentos. La clave privada asociada a un certificado electrónico se utiliza para firmar electrónicamente cualquier documento electrónico. Esto proporciona una verificación de la autoría de un documento y que su contenido permanezca sin modificaciones, es decir que se mantenga su integridad.

En el caso de la República Bolivariana de Venezuela, el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas electrónicas promulgado en el año 2001 y publicado en la Gaceta Oficial número 37.148 del 28 de febrero de ese año<sup>6</sup>, crea mecanismos para que la firma electrónica tenga la misma eficacia y valor probatorio de la firma autógrafa mediante el uso de certificados electrónicos de la Infraestructura Nacional de Certificación Electrónica. El concepto de firma electrónica se tratará con mayor detalle en la siguiente sección.

Una característica de los certificados electrónicos es que pueden ser emitidos tanto para individuos como para dispositivos de red. Uno de los usos más populares de los certificados es la validación de nombres de dominio en la Internet, por ejemplo: *www.gobiernoenlinea.gob.ve*. Esto es considerado como una defensa contra acciones de falsificación que buscan tomar datos de los usuarios de estos sitios de manera masiva y que generalmente se coordinan como parte de ataques tales como el denominado *phishing*. En este tipo de ataque se suplanta la identidad de servidores en la Internet y se obtiene información como datos personales, números de tarjetas de crédito, contraseñas de acceso y otros tipos de información sin el consentimiento del usuario.

Una de las herramientas comunes para acceder a los sistemas publicados en la Internet son los navegadores web. Tanto en computadores de escritorio como en dispositivos móviles, los navegadores están preparados para identificar los servidores que alojan una página web particular en el caso que se esté usando un certificado electrónico. Con el uso del certificado se intercambia información de manera segura con sus visitantes y además se garantiza que se están comunicando con el servidor correcto y no uno fraudulento.

El proceso de intercambio de información entre un usuario y un servidor a través de las páginas web sigue un conjunto de reglas y formatos que se especifican en protocolos de transferencia. El protocolo de transferencia de hipertexto (HTTP por sus siglas en inglés) se puede utilizar junto a los protocolos para capa de conexión segura o seguridad para capa de transporte, conocidos como SSL/TLS por sus siglas en inglés, para formar el protocolo HTTPS que permite realizar comunicación cifrada entre un usuario y un servidor. Las direcciones de sitios web de la Internet que utilizan el protocolo HTTP con certificados electrónicos tienen como prefijo *https://*.

En la figura 1.6 se muestra una captura de pantalla del sistema de banca en línea de un banco de la República Bolivariana de Venezuela que utiliza un certificado electrónico.

Los navegadores web mantienen un almacén de certificados de autoridades de certificación en las que confían para la emisión de certificados electrónicos. En el caso de la figura 1.6, el navegador muestra un indicador de color verde sobre la barra de dirección para mostrar al usuario que el certificado electrónico presentado es reconocido como válido por estas autoridades. En el caso de que un usuario esté conectado a una página web con un certificado electrónico que el navegador no reconoce, éste último mostrará un mensaje que alerta al usuario de una posible comunicación con un sitio no confiable. El indicador puede variar de un navegador a otro pero mantiene su función de alertar al usuario.

Un certificado electrónico está compuesto por un conjunto de campos de datos definidos por el estándar de Internet X.509 versión 3<sup>7</sup>, algunos campos son obligatorios y otros son extensiones que pueden o no aparecer en un certificado particular. A continuación se listan los campos comunes de un certificado electrónico X.509.

- Versión: Describe la versión del certificado codificado. La versión actual es la 3.

<sup>6</sup><http://www.tsj.gov.ve/gaceta/febrero/280201/280201-37148-07.html>

<sup>7</sup><http://www.ietf.org/rfc/rfc3280.txt>

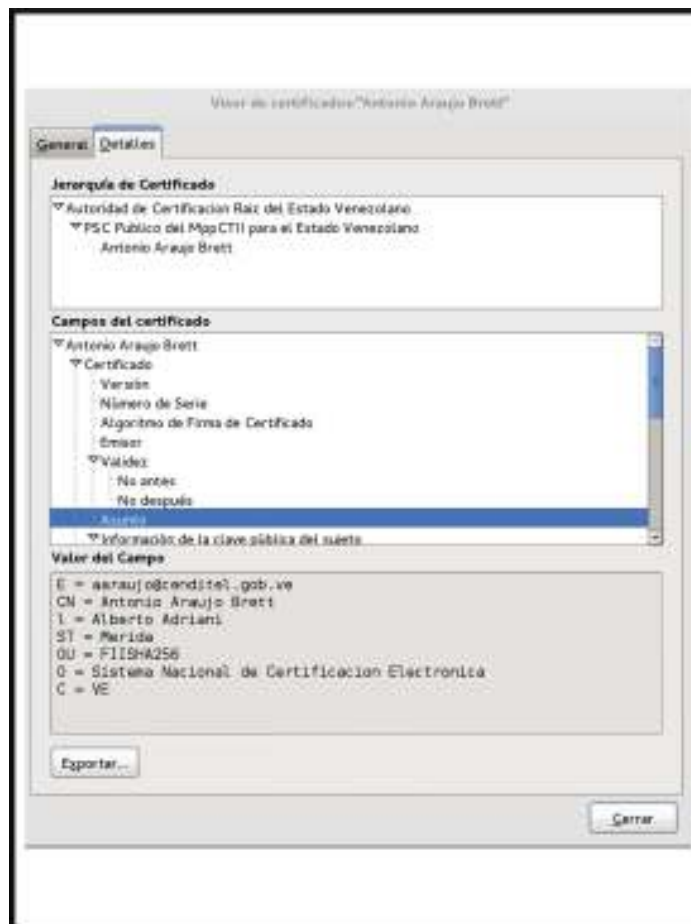


**Figura 1.6** Sistema de banca en línea que utiliza un certificado electrónico.

- **Número de serie:** Es un identificador único para el certificado electrónico emitido por una autoridad de certificación.
- **Algoritmo de firma:** Identificación del algoritmo criptográfico utilizado por la autoridad de certificación para firmar el certificado.
- **Emisor:** Identificación de la autoridad de certificación que emitió el certificado electrónico.
- **Validez:** Intervalo de tiempo durante el cual la autoridad de certificación mantiene información sobre el estado del certificado. El período de validez está representado por dos fechas: una fecha a partir de la cual la validez del certificado comienza y otra en la que termina. La validez de un certificado electrónico está definida en la documentación de políticas de certificado de una autoridad de certificación.
- **Sujeto:** Nombre del titular del certificado electrónico. Los campos sujeto y emisor de un certificado electrónico están definidos utilizando convenciones que se definen en el estándar X.500. Esto permite establecer un nombre único mediante la definición de un concepto conocido como *nombre distinguido* [3]. En general un nombre distinguido incluye los siguientes valores:
  - **CN:** Nombre Común del titular. Normalmente se utiliza el nombre y apellido de la persona titular del certificado o nombre de dominio asociado al sistema informático en caso de ser un certificado electrónico para dispositivos.
  - **E:** Correo electrónico del titular.
  - **L:** Localidad donde reside el titular.
  - **ST:** Estado donde reside el titular.
  - **OU:** Unidad organizacional de la que depende el titular.
  - **O:** Organización a la que pertenece el titular.

- C: País en el que reside el titular.
- Información de clave pública del sujeto: tiene la clave pública del sujeto e identifica el algoritmo con el cual se utiliza la clave.
- Extensiones: Secuencia de una o más extensiones que sirven para asociar atributos adicionales del sujeto.
- Firma electrónica del certificado: Representación de la firma electrónica de la autoridad de certificación sobre el certificado que utiliza una codificación particular.

En la figura 1.7 se muestran los detalles de los campos de un certificado electrónico de la Infraestructura Nacional de Certificación Electrónica visto en un navegador web.



**Figura 1.7** Detalles de los campos de un certificado electrónico.

Una forma de distribuir los certificados electrónicos es a través de dispositivos de usuario, como por ejemplo tarjetas inteligentes, que permiten proteger los elementos del certificado; en particular la clave privada. En la sección 1.3.4 se presentan algunos dispositivos como tarjetas inteligentes y token criptográficos utilizados con certificados electrónicos.

En el capítulo 5 se describe el proceso de desarrollo de una aplicación para gestionar una autoridad de certificación raíz en una ICP utilizando tecnologías libres.

En el apéndice A se muestra el contenido de un certificado electrónico X.509 Versión 3 en formato de texto plano.

### 1.3.3. Firmas electrónicas

La firma electrónica otorga a un documento digital la propiedad de integridad vinculada con la voluntad de aceptación de una entidad jurídicamente hábil. Se puede decir que la firma electrónica pretende obtener en cada comunidad o país las mismas propiedades legales y culturales que tiene la firma autógrafa, por lo tanto, se puede decir que es un concepto que se trasladó del ámbito físico (papel) al ámbito digital o ciberespacio.

La realización de la firma electrónica se apoya en los algoritmos de una sola vía, tales como SHA256, SHA224, o MD5, y en la criptografía de Clave Pública. El algoritmo más básico tiene dos pasos: 1) la generación de una reseña (texto que representa una suma única y fija) de un documento (a firmar) utilizando un algoritmo de una sola vía que asegure la integridad del documento digital y 2) el cifrado de la reseña generada en el paso 1 utilizando la clave privada del firmante. Para la verificación de la firma solo se necesita obtener la Clave Pública del firmante, cuyo certificado generalmente es validado por una Autoridad de Certificación confiable, para posteriormente descifrar el contenido de la firma y comparar la reseña resultante con una nueva generada en el momento de validación, si son iguales el documento no ha sufrido ninguna alteración.

De la definición de firma electrónica se han propuesto diversos estándares (con sus respectivas implementaciones). Entre los estándares más importantes están:

- Estándar Criptográfico de Clave Pública 7 (**PKCS#7** [7]): es uno de los formatos más básicos de firma electrónica, es un pequeño archivo anexo a un documento firmado que contiene la reseña cifrada con la clave privada del firmante. Este formato se encuentra disponible en los motores criptográficos más usados tales como OpenSSL, Microsoft CryptoAPI <sup>TM</sup> o Java Cryptography Architecture (JCA).
- Firma PDF (**PADES o A/1**): formato para firma de documentos para impresión Adobe <sup>TM</sup> PDF:
- Firma XML **XMLSig**: forma en lenguaje XML para firmas electrónicas.
- Firma Electrónica Avanzada (con sufijo proveniente de su nombre en inglés **AdES**): formato de firma que cumple ciertos criterios de seguridad para que pueda ser validado como documento probatorio en trámites dentro de la Unión Europea.

Aunque la firma electrónica no está ligada de forma unívoca con el modelo PKI (Basado en autoridades de certificación), la mayor cantidad de aplicaciones funcionan bajo este modelo de confianza. Un modelo de confianza alternativo, ampliamente utilizado en comunidades de desarrollo de software libre tales como el proyecto Debian<sup>8</sup>, consiste en la creación de *anillos de confianza*, los cuales son conjuntos de personas que han verificado sus identidades entre sí mediante el protocolo acordado por la comunidad para tales efectos, en donde muchas veces se incluye la revisión minuciosa de documentos de identidad físicos reconocidos internacionalmente. Una característica de este modelo es que su correcto funcionamiento sólo depende de la capacidad de organización y cooperación de la comunidad que lo utilice, y su factibilidad de emplearse en grandes conjuntos de personas requiere la aceptación de diversas formas de transitividad<sup>9</sup> en la confianza.

El uso de la firma electrónica para muchas implementaciones está asociada con el uso de una tarjeta inteligente o *token* criptográfico, lo que implica que si una persona desea firmar debe insertar una tarjeta inteligente que le ha sido asignada con anterioridad, en la cual se encuentre almacenado el certificado de firma vinculado al firmante, en un dispositivo lector conectado a su vez a una computadora o dispositivo móvil, luego debe escribir una contraseña o número de identificación personal (PIN por sus siglas en inglés) que ejecuta finalmente la acción de firma.

La firma electrónica actualmente se utiliza en organizaciones y en administraciones públicas de muchas partes del mundo para mejorar la ejecución de sus procesos, el lector puede ver algunos ejemplos de ello en la segunda parte del presente libro.

<sup>8</sup><https://www.debian.org/>

<sup>9</sup>Existe transitividad en la confianza cuando ocurre que si una persona A confía en una persona B, y esa persona B confía en una persona C, ello implica que la persona A confía en la persona C.



### 1.3.4. Dispositivos de usuario

Una de las formas en que las personas demuestran su identidad en distintos entornos es a través de dispositivos tecnológicos. Los certificados de nacimiento, los documentos de identidad, las actas de matrimonio, los contratos y hasta los pasaportes utilizan algún tipo de tecnología; en este caso la palabra impresa sobre un papel o un soporte análogo.

Con el devenir de nuevas tecnologías, las personas han tenido que emplear mecanismos distintos para demostrar su identidad. Ahora es común tratar con sistemas informáticos en los cuales se realizan tareas tan cotidianas como comprar comida en un abasto o supermercado, pagar el servicio de agua, teléfono o energía eléctrica y hasta pagar los impuestos. El cambio en la forma de realizar las actividades cotidianas ha exigido que las personas empleen otros tipos de dispositivos tecnológicos para demostrar su identidad. En esta sección se describen algunos dispositivos de usuario que se emplean en la actualidad.

#### 1.3.4.1. Tarjetas como medio de almacenamiento seguro

Uno de los medios más comunes para demostrar la identidad de las personas es a través de tarjetas plásticas de policloruro de vinilo (PVC). Con un bajo costo, características de ergonomía y con mayor durabilidad que el papel, las tarjetas de plástico PVC son las más empleadas en la actualidad. Generalmente, la información asociada a la identidad de las personas está impresa en la tarjeta, y en algunos casos se agrega una fotografía. Esta tarjeta es emitida por la entidad que desea establecer la identidad de la persona y es intransferible.

Existen distintos tipos de tarjetas empleadas para demostrar la identidad de las personas. A continuación se describen las más comunes.

#### 1. Tarjetas con cintas magnéticas.

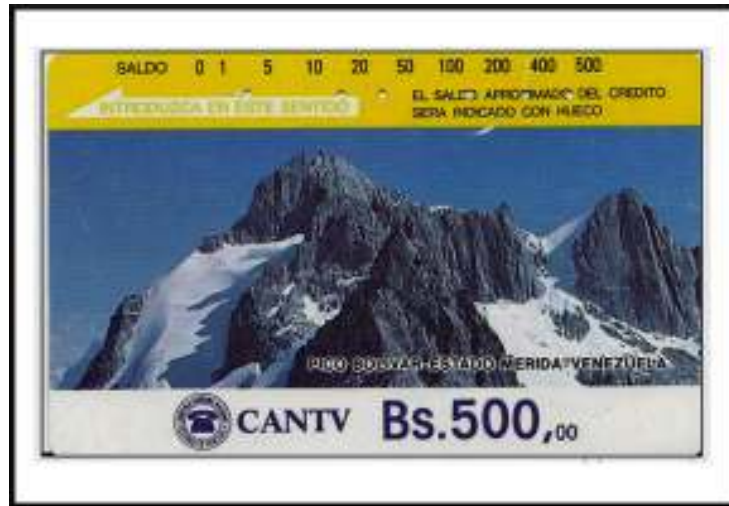
Este tipo de tarjetas emplea una banda o cinta magnética en la cual se codifican datos digitales. El estándar ISO 7811<sup>10</sup> en sus partes 2, 4 y 5 especifican las propiedades de la cinta magnética, las técnicas de codificación y la ubicación de las pistas magnéticas. Desde sus inicios las tarjetas débito y crédito, tanto de instituciones financieras públicas como privadas eran de este tipo. En la figura 1.8 se muestra una tarjeta de débito con cinta magnética.



**Figura 1.8** Tarjeta de débito magnética.

<sup>10</sup>[http://www.iso.org/iso/home/store/catalogue.tcl/catalogue\\_detail.htm?csnumber=31440](http://www.iso.org/iso/home/store/catalogue.tcl/catalogue_detail.htm?csnumber=31440)

Otro uso de las tarjetas con cintas magnéticas se pudo ver en la telefonía pública. En Venezuela, durante los años 80 y 90 la Compañía Anónima Nacional Teléfonos de Venezuela, CANTV, emitía tarjetas magnéticas de distintas denominaciones para teléfonos públicos. En la figura 1.9 se muestra una de las tarjetas emitidas por la CANTV.



**Figura 1.9** Tarjeta magnética de telefonía pública.

A pesar de su uso masivo, las tarjetas con cinta magnética presentaron serias debilidades que permitían leer los datos almacenados, borrarlos e inclusive modificarlos si un atacante poseía el equipo necesario. Uno de los ataques más comunes en estas tarjetas es la llamada “clonación de tarjeta”, en la que el atacante podía copiar los datos de la cinta magnética con un dispositivo especializado para luego insertarlos en una nueva tarjeta usurpando la identidad del titular. Ante esta situación, este tipo de tarjetas ha sido sustituido por otras con nuevos mecanismos de seguridad que se describen más adelante.

## 2. Tarjetas inteligentes o tarjetas con chip

A diferencia de las tarjetas con cintas magnéticas, las denominadas tarjetas inteligentes tienen como característica principal el uso de un circuito integrado o chip insertado en la tarjeta que tiene componentes para transmitir, almacenar y procesar datos [8]. Las tarjetas inteligentes ofrecen varias ventajas con respecto a las tarjetas con cintas magnéticas, principalmente la capacidad de almacenamiento, la protección de datos contra acceso no autorizado y la eventual ejecución de aplicaciones o programas en el chip.

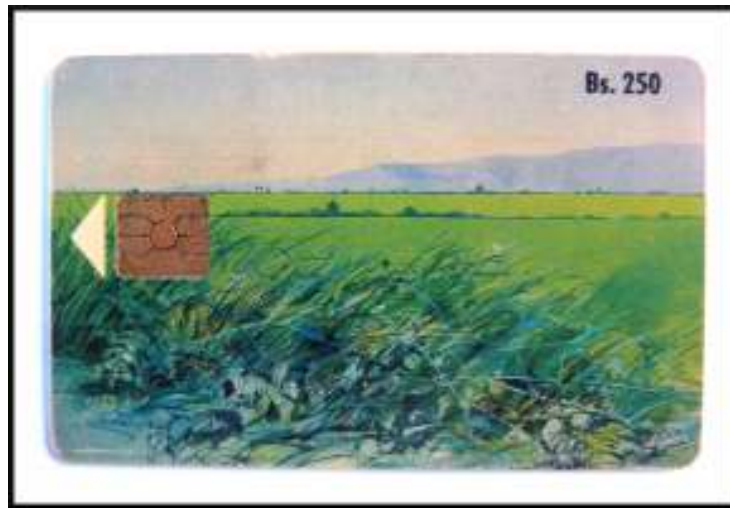
De acuerdo al tipo de chip que utilizan las tarjetas inteligentes se pueden dividir en dos grupos: tarjetas con chip de memoria y tarjetas con chip microprocesador.

### ■ Tarjetas con chip de memoria.

Permiten almacenar datos protegidos en un chip o circuito integrado y son útiles en aplicaciones donde el costo es una consideración principal. Fueron las primeras tarjetas inteligentes utilizadas de forma masiva para aplicaciones de telefonía. En el chip se almacenaba electrónicamente la cantidad de dinero de la que disponía el usuario para hacer llamadas.

En Venezuela, la CANTV distribuía tarjetas de memoria prepagadas de distintas denominaciones para la telefonía pública. En la figura 1.10 se muestra una tarjeta con chip de memoria.

Las tarjetas de memoria también pueden ser reutilizadas en algunas aplicaciones, por ejemplo para recargar el saldo de un usuario sin necesidad de obtener una nueva tarjeta plástica. Otros usos de estas tarjetas se describen en secciones posteriores de este capítulo.



**Figura 1.10** Tarjeta con chip de memoria para telefonía pública.

■ Tarjetas con chip microprocesador.

A diferencia de las tarjetas de memoria, permiten almacenar claves y ejecutar algoritmos criptográficos en el microprocesador. Las tarjetas con microprocesador utilizan un sistema operativo, similar al de los computadores, para realizar las operaciones internas. Son utilizadas en telefonía celular, sistemas de pagos electrónicos, cifrado de datos y para realizar firmas electrónicas (ver sección 1.3.3).

Entre las principales ventajas de este tipo de tarjetas están: una mayor capacidad de almacenamiento, la posibilidad de mantener datos confidenciales y la habilidad de ejecutar algoritmos criptográficos.

Estas tarjetas tienen mecanismos de seguridad para mitigar los ataques como la mencionada “clonación de tarjetas”. En general, el acceso a datos protegidos en el chip está restringido por dos características importantes: el Número de Identificación Personal (PIN por sus siglas en inglés) y la Clave de Desbloqueo Personal (PUK por sus siglas en inglés).

- El PIN, es un código de seguridad que le permite bloquear y desbloquear la tarjeta para evitar que otro usuarios pueda tener acceso a su contenido.
- El PUK, es un código que sirva para desbloquear la tarjeta y definir un nuevo PIN. Se emplea como mecanismo de seguridad cuando se introduce erróneamente el PIN más de un número establecido de veces.

En la figura 1.11 se muestran varias tarjetas con microprocesador.

**Tabla 1.1** Fabricantes de Tarjetas JavaCard y sus Sistemas Operativos

| Fabricante                        | Sistema Operativo |
|-----------------------------------|-------------------|
| Gemalto <sup>13</sup>             | JavaCard          |
| NXP <sup>14</sup>                 | JCOP              |
| Giesecke & Devrient <sup>15</sup> | Sm@rtCafé Expert  |
| Atos <sup>16</sup>                | CardOS            |
| Consortio MULTOS <sup>17</sup>    | MULTOS            |

**Figura 1.11** Tarjetas con microprocesador.

Las características fundamentales y funciones de las tarjetas inteligentes o de microprocesador están especificados en la familia de estándares ISO/IEC 7816<sup>11</sup> de la Organización Internacional para Estandarización (ISO por sus siglas en inglés) y la Comisión Electrotécnica Internacional (IEC por sus siglas en inglés).

### 3. Tarjetas Java Card

Un tipo de tarjetas inteligentes que se encuentra en muchas aplicaciones son las Java Card. Estas tarjetas utilizan la tecnología Java<sup>12</sup> sobre un chip para ejecutar múltiples aplicaciones. Los fabricantes de tarjetas inteligentes generalmente desarrollan su propia versión del sistema operativo Java o siguen especificaciones abiertas. Algunos fabricantes de tarjetas inteligentes y sistemas operativos conocidos se muestran en la tabla 1.1.

<sup>11</sup>[http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=54089](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54089)

<sup>12</sup><http://www.java.com>

<sup>13</sup><https://www.gemalto.com/>

<sup>14</sup><http://www.nxp.com/>

<sup>15</sup><http://www.gi-de.com>

<sup>16</sup><http://atos.net/en-us/home.html>

<sup>17</sup><http://www.multos.com/>

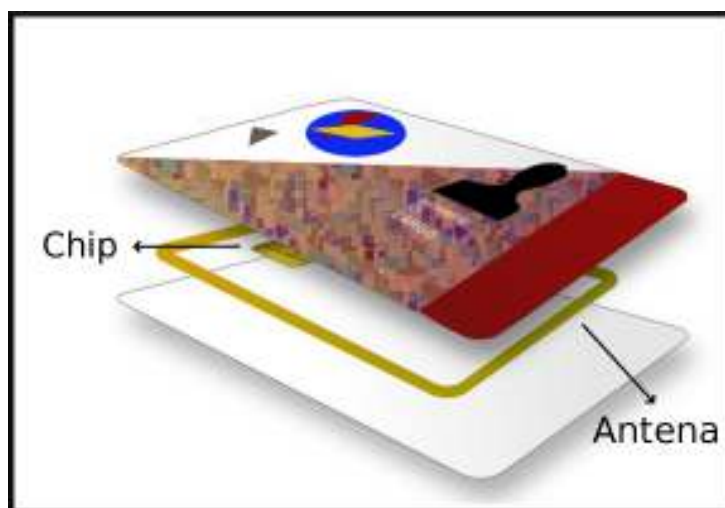
También es posible encontrar proyectos de software libre que permiten interactuar con tarjetas Java Card. El movimiento para el uso de tarjetas inteligentes en ambientes Linux<sup>18</sup> (MUSCLE por sus siglas en inglés), es un proyecto que define un marco de trabajo para el desarrollo de aplicaciones con tarjetas inteligentes en entornos Linux.

#### *Método de transmisión de datos en tarjetas inteligentes*

Las tarjetas inteligentes pueden utilizar distintos métodos para comunicarse con los terminales o lectores para el acceso a la información protegida. De acuerdo al método de transmisión de datos las tarjetas inteligentes pueden dividirse en tarjetas de contacto, tarjetas sin contacto y tarjetas duales o híbridas.

En las tarjetas de contacto el chip de la tarjeta entra en contacto físico con el terminal o lector. En la figura 1.11 se muestran algunas tarjetas de contacto.

En las tarjetas sin contactos el chip no entra en contacto físico con el terminal o lector ya que se utiliza una comunicación inalámbrica entre ellos. Este tipo de tarjetas son utilizadas en entornos y aplicaciones donde las personas deben ser identificadas rápidamente. Algunos ejemplos de uso incluyen controles de acceso, transporte público, identificación de equipajes, entre otros. Las tarjetas sin contacto además de un chip poseen una antena incrustada que le permite establecer la comunicación con los lectores. En la figura 1.12 se muestra una tarjeta sin contacto.



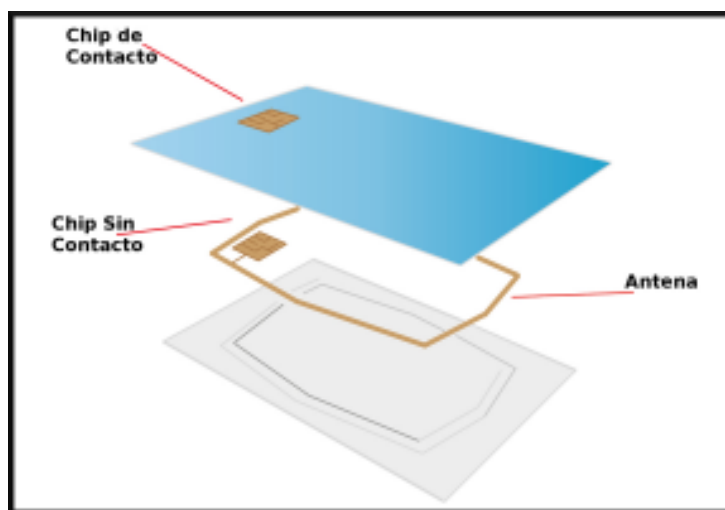
**Figura 1.12** Tarjeta sin contacto.

El estándar principal de comunicaciones en tarjetas sin contacto es el ISO/IEC 14443<sup>19</sup>.

En las tarjetas duales o híbridas se utiliza un chip con contacto y sin contacto en la misma tarjeta. En la figura 1.13 se muestra una tarjeta con chip de contacto y sin contacto.

<sup>18</sup><http://www.musclecard.com>

<sup>19</sup>[http://www.iso.org/iso/iso\\_catalogue/catalogue\\_ics/catalogue\\_detail\\_ics.htm?csnumber=39693](http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39693)



**Figura 1.13** Tarjeta dual o híbrida.

#### **1.3.4.2. Lectores de tarjetas**

Los lectores son dispositivos electrónicos de entrada que leen datos de medios de almacenamiento en forma de tarjetas. Existen lectores para tarjetas de memoria, tarjetas magnéticas y tarjetas inteligentes con interfaces con contacto, sin contacto o de interfaz dual (ambas interfaces en un mismo lector).

Los lectores de tarjetas pueden conectarse a los computadores a través de distintos puertos como por ejemplo USB o serial. En las figuras 1.14, 1.15 y 1.16 se muestran algunos lectores de contacto, sin contacto y dual respectivamente.



**Figura 1.14** Lectores de tarjetas inteligentes de contacto.



**Figura 1.15** Lectores de tarjetas inteligentes sin contacto.



**Figura 1.16** Lector de tarjetas inteligentes de interfaz dual.

Al igual que las tarjetas inteligentes, para los lectores también existen estándares que especifican su operación. Entre estos estándares se encuentran: PC/SC (Personal Computer / Smart Card) con especificaciones para la integración de tarjetas inteligentes en computadores personales definidas por el PC/SC Workgroup<sup>20</sup> y el USB-CCID (Integrated Circuit(s) Cards Interface Device) con especificaciones para dispositivos USB que se comunican con tarjetas de circuitos integrados como tarjetas inteligentes definidas por el Grupo de Trabajo de Dispositivos (DWG por sus siglas en inglés) del Foro de Implementadores de USB<sup>21</sup> (USB-IF por sus siglas en inglés).

#### **1.3.4.3. Token Criptográfico**

También llamado token de seguridad, token de autenticación o simplemente token USB, es un dispositivo similar a las tarjetas inteligentes en su arquitectura. Posee un microprocesador criptográfico que permite reali-

<sup>20</sup><http://www.pcscworkgroup.com>

<sup>21</sup><http://www.usb.org/about/>

zar las mismas operaciones criptográficas y de autenticación que las tarjetas inteligentes a través de un puerto USB.

A diferencia de las tarjetas inteligentes no utilizan un lector pero sí requieren la instalación de un controlador de *hardware* en el computador para que sea reconocido. En la figura 1.17 se muestran algunos token criptográficos utilizados en aplicaciones como certificación electrónica y firmas electrónicas.



**Figura 1.17** Token criptográficos.

También es posible encontrar tokens criptográficos en formato de tarjetas MicroSD o SD como se muestra en la figura 1.18. Las tarjetas MicroSD con certificados electrónicos almacenados se pueden utilizar en teléfonos celulares para propósitos de autenticación o firma electrónica.



**Figura 1.18** Token criptográfico en formato MicroSD y SD.

#### **1.3.4.4. Dispositivos de autenticación con contraseñas de un solo uso**

Los dispositivos de autenticación con contraseñas de un solo uso (OTP por sus siglas en inglés), generan un código único y aleatorio que permite a un usuario autenticarse y tener acceso a sistemas informáticos. Estos dispositivos representan una variación del mecanismo de autenticación común de usuario y contraseña ya que



esta última es válida para una sola sesión. La generación de los códigos se realiza, principalmente, de acuerdo a varios enfoques existentes:

- Mediante algoritmos matemáticos para que un servidor de autenticación verifique el dispositivo.
- Mediante la sincronización de tiempo entre el servidor de autenticación y el dispositivo.

En la figura 1.19 se muestran algunos de estos dispositivos.



**Figura 1.19** Dispositivos de contraseña de un solo uso.

#### **1.3.4.5. Chip SIM**

Es una tarjeta o chip que posee información relacionada al cliente o suscriptor de cada empresa prestadora de servicio de telefonía en el Sistema Global para las Comunicaciones Móviles (GSM por sus siglas en inglés). El chip o módulo de identificación de suscriptor (SIM por sus siglas en inglés) almacena datos como la clave del cliente usada para identificarse en la red.

En general, el chip SIM está diseñado para proveer las siguientes funciones básicas:

- Seguridad (identificación del cliente, autenticación de SIM y criptado de datos).
- Almacenamiento de datos (números de contactos, mensajes cortos, configuración del teléfono celular e información del suscriptor).
- Administración del cliente.

En la figura 1.20 se muestra un chip SIM.

#### **1.3.4.6. Autenticación de dos factores**

El proceso de autenticación de una persona permite que ésta tenga acceso a un computador, a un sitio web de la Internet o a sistemas informáticos. Generalmente, el proceso de autenticación ocurre en una sola etapa en la cual la persona presenta algún tipo de credencial para demostrar su identidad, por ejemplo un nombre de usuario y contraseña. Este tipo de autenticación es conocida como autenticación de un solo factor. Para mejorar los niveles de seguridad en el proceso de autenticación se agrega una segunda etapa en la que la persona debe presentar una credencial adicional y de distinto tipo a la primera para demostrar su identidad. Este tipo de autenticación es conocida como autenticación de dos factores.

En la actualidad existen organizaciones y empresas que proveen servicios en línea como correo electrónico, redes sociales, mensajería instantánea y banca electrónica entre otras, que emplean alguna o varias formas de



**Figura 1.20** Chip SIM de telefonía celular.

autenticación de dos factores con la intención de que sus usuarios tengan acceso a sus recursos y se disminuya la suplantación de identidad.

Aunque no es exactamente un dispositivo físico, la autenticación de dos factores utiliza distintos mecanismos para validar la identidad de un usuario al solicitarle alguna prueba adicional. Entre los mecanismos utilizados están el Servicio de Mensajes Cortos (SMS por sus siglas en inglés), una llamada telefónica, un correo electrónico, un token o dispositivo de hardware o una implementación de software<sup>22</sup>. Cuando una persona desea autenticarse en un sistema informático presenta un identificador y contraseña como primer factor de autenticación. Luego el sistema envía un código, a través de uno de los mecanismos mencionados, que el usuario debe introducir como segundo factor de la autenticación. Si el código introducido es el correcto, el sistema permite el acceso al usuario a sus recursos.

La autenticación de dos factores puede ser utilizada en entornos como:

- Integración de sistemas.
- Acceso remoto y redes privadas virtuales (VPN por sus siglas en inglés).
- Administración de contraseñas.
- Cifrado de discos.
- Protección de servidores.

Desde Febrero de 2013 la Alianza de Identidad Rápida en Línea (FIDO Alliance<sup>23</sup> por sus siglas en inglés) agrupa a un conjunto de organizaciones y empresas que tienen como objetivo establecer estándares de interoperabilidad entre dispositivos de autenticación así como enfrentar el problema de crear y recordar múltiples nombres de usuarios y contraseñas para sistemas informáticos.

#### **1.3.4.7. Lectores biométricos**

Son dispositivos electrónicos capaces de leer características inherentes a los seres humanos para identificar y autenticar usuarios en un entorno particular. Con éstos es posible dar acceso a un espacio físico o recursos informáticos.

Entre las características humanas empleadas por los lectores biométricos están:

- Huella digital
- Geometría de la mano
- Patrones de líneas del Iris
- Patrones de las venas encontradas en la parte trasera del ojo

<sup>22</sup><http://twofactorauth.org/>

<sup>23</sup><https://fidoalliance.org/>

- Forma de la oreja
- Rasgos faciales
- Escritura

Es común encontrar lectores biométricos de huellas digitales en aeropuertos, computadores portátiles e inclusive en registros electorales. En la figura 1.21 se muestran algunos lectores biométricos.



**Figura 1.21** Lectores biométricos.

Uno de los registros biométricos más conocidos es el que mantienen algunos países al momento de emitir los documentos de identidad a sus ciudadanos. En la República Bolivariana de Venezuela, se solicitan las huellas digitales a todos los ciudadanos al momento de emitirle la Cédula de Identidad y el Pasaporte. Estas son registradas en un sistema de identificación de huellas automatizado (AFIS por sus siglas en inglés). La información puede ser consultada por las instituciones de gobierno para verificar la identidad de los ciudadanos venezolanos.

### 1.3.5. Usos comunes de dispositivos de usuario

En esta sección se presentan algunos usos y aplicaciones los dispositivos de usuario como elementos que apoyan el proceso de verificación de identidad.

#### 1.3.5.1. Telefonía móvil

Entre las tecnologías predominantes de telefonía móvil en Venezuela se encuentran el Acceso Múltiple por División de Código (CDMA por sus siglas en inglés) y GSM que emplea un chip en el teléfono para el acceso a la red. De estas, GSM tiene mayor despliegue en la República Bolivariana de Venezuela. En la tabla 1.2 se muestra la proporción de suscriptores por tipo de tecnología de acuerdo a las estadísticas preliminares del Sector Telecomunicaciones realizadas por la Comisión Nacional de Telecomunicaciones de la República Bolivariana de Venezuela (CONATEL), para el segundo trimestre de 2014<sup>24</sup> con base en 31.731.715 suscriptores totales de telefonía móvil.

De acuerdo a los indicadores del servicio de telefonía móvil a nivel nacional generados por la CONATEL, correspondientes al cuarto trimestre del 2013, el porcentaje de usuarios activos había sido de 102,59 %. Se estimaron 103 líneas en uso del sistema de telefonía móvil por cada 100 habitantes.

<sup>24</sup><http://conatel.gob.ve/files/indicadores/cifras-2do-2014.pdf>

**Tabla 1.2** Proporción de suscriptores por tipo de tecnología móvil.

| Tecnología | Proporción de suscriptores ( % ) |
|------------|----------------------------------|
| GSM        | 70,28                            |
| CDMA       | 29,37                            |

El despliegue masivo de la telefonía móvil con la tecnología GSM en la República Bolivariana de Venezuela y el impulso de iniciativas de gobierno electrónico se pueden aprovechar para formular y ejecutar proyectos en los que los teléfonos móviles sirvan como dispositivos de verificación de identidad.

#### 1.3.5.2. Banca electrónica

En el año 2010, la Superintendencia de las Instituciones Bancarias (SUDEBAN) inició el proyecto de la incorporación del chip electrónico en las tarjetas de débito, crédito y demás tarjetas de financiamiento de pago electrónico. En marzo del año 2012 la SUDEBAN exhortó a los usuarios de la banca a canjear sus tarjetas de débito y crédito por aquellas con el sistema de chip electrónico antes del 01 de Julio de ese año<sup>25</sup>. Este requerimiento de la SUDEBAN exigió la adaptación de cajeros automáticos y puntos de ventas para el soporte de las nuevas tarjetas en búsqueda de una reducción de los índices por fraude de clonación.

Para el año 2014 todos los bancos de la República Bolivariana de Venezuela migraron su plataforma de tarjetas de débito, crédito y demás tarjetas de financiamiento de pago electrónico a tecnología de tarjetas con chip.

Instituciones públicas que dependen del Gobierno Bolivariano y empresas privadas utilizan tarjetas inteligentes para brindar a sus empleados el beneficio del bono de alimentación. A través de estas tarjetas los empleados pueden adquirir productos en abastos y supermercados con un mayor nivel de seguridad comparado con la emisión de tiquetes en papel. La figura 1.22 muestra una de las tarjetas emitidas por uno de las entidades bancarias del Estado Venezolano.

**Figura 1.22** Tarjeta electrónica de alimentación.

#### 1.3.5.3. Certificación electrónica

Con el despliegue de la Infraestructura Nacional de Certificación Electrónica la República Bolivariana de Venezuela cuenta con los Proveedores de Servicios de Certificación (PSC) que emiten certificados electrónicos

<sup>25</sup><http://sudeban.gob.ve/webgui/root/documentos/notas-de-prensa/np-chip.pdf>

a los ciudadanos. Como medida de seguridad la emisión de estos certificados se realiza en algún dispositivo de usuario como tarjetas inteligentes o token USB (ver sección 1.3.2). En las figuras 1.23 y 1.24 se muestra una tarjeta inteligente y un token USB utilizado por un PSC acreditado de la República Bolivariana de Venezuela.



**Figura 1.23** Tarjeta inteligente para certificado electrónico.



**Figura 1.24** Token USB para certificado electrónico.

#### **1.3.5.4. Tarjeta inteligente de pasaje estudiantil**

El Gobierno Bolivariano a través del Ministerio del Poder Popular para Transporte Terrestre gestiona el Proyecto Pasaje Preferencial Estudiantil como instrumento social para garantizar el acceso de los estudiantes al sistema de transporte público. El proyecto entrega a los estudiantes una tarjeta inteligente como sistema de pago electrónico a través del débito del pasaje, en sustitución del ticket o boleto de papel. La figura 1.25 muestra una tarjeta inteligente de un estudiante.

Cada tarjeta inteligente cuenta con los datos que identifican al alumno, cédula de identidad y nombre de la institución donde cursa estudios. Es intransferible y tiene una vigencia de 4 años. Además es renovable y también recargable.



**Figura 1.25** Tarjeta inteligente de pasaje estudiantil.

#### **1.3.5.5. Tarjetas para control de acceso físico**

Otro de los principales usos de las tarjetas inteligentes es el control de acceso físico. Se utiliza en oficinas, salones, bancos e instituciones públicas o privadas en las cuales se desea controlar el acceso a espacios físicos. Generalmente estas tarjetas tienen una interfaz sin contacto que utiliza la tecnología RFID. En la figura 1.26 se muestra una tarjeta de control de acceso físico y su respectivo lector.



**Figura 1.26** Tarjeta y lector de control de acceso físico.

#### **1.3.5.6. Pasaporte Electrónico**

Cada país emplea un documento con validez internacional para establecer la identidad de sus ciudadanos: el pasaporte. En la República Bolivariana de Venezuela la emisión del pasaporte para los ciudadanos está a cargo del Servicio Administrativo de Identificación, Migración y Extranjería (SAIME), organismo adscrito al Ministerio del Poder Popular para Relaciones Interiores y Justicia.

Como resultado de un proceso de transformación iniciado en el año 2005, el Ejecutivo Nacional aprobó la ejecución del Proyecto de Transformación y Modernización de la Oficina Nacional de Identificación y Extranjería (ONIDEX) que se convirtió en el actual SAIME. Así mismo se inició la emisión del Pasaporte Electrónico para los ciudadanos en el año 2007.

El Pasaporte Electrónico de la República Bolivariana de Venezuela es un documento similar a cualquier pasaporte de papel pero con un conjunto de medidas de seguridad adicionales. Se utiliza una lámina de polí-carbonato con un circuito electrónico incrustado en ella. En la figura 1.27 se muestra un pasaporte electrónico.



**Figura 1.27** Muestra de pasaporte electrónico.

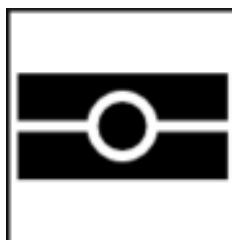
A diferencia del pasaporte impreso en papel, en el electrónico todos los datos del ciudadano se encuentran también almacenados en formato electrónico en un chip criptográfico sin contacto. Para garantizar la integridad de los datos así como el origen de los mismos se emplea la tecnología de firma electrónica (ver sección 1.3.3). SAIME firma electrónicamente toda la información asociada a un ciudadano y esta puede ser leída en cualquier oficina o punto de inmigración de un país para verificar su identidad.

Todas las especificaciones que deben cumplir los pasaportes electrónicos están definidas por la Organización de Aviación Civil Internacional<sup>26</sup> (ICAO por sus siglas en inglés).

El Pasaporte Electrónico de la República Bolivariana de Venezuela posee en su anverso el símbolo que se muestra en la figura 1.28. Este es un indicador visual de que el pasaporte es electrónico y que contiene un circuito integrado sin contacto, con capacidad de almacenamiento de datos de al menos 32kB.

Los esfuerzos de la República Bolivariana de Venezuela en el proceso de actualización del pasaporte electrónico, permiten a los ciudadanos venezolanos entrar en algunos países del mundo sin necesidad de tramitar visas.

<sup>26</sup><http://www.icao.int/>



**Figura 1.28** Símbolo de pasaporte electrónico según ICAO.



## REFERENCIAS

---

1. Rodolfo Sumoza. Sistemas anónimos en escenarios globales. Master's thesis, Universidad Complutense de Madrid, 2008.
2. J. F. Raymond. Traffic analysis: Protocols, attacks, design issues, and open problems. In H. Federrath, editor, *Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability* - Springer-Verlag, LNCS, 2000.
3. Dawn Xiaodong Song; David Wagner; Xuqing Tian. Timing analysis of keystrokes and timing attacks on ssh. In USENIX Association, editor, *Proceedings of the 10th USENIX Security Symposium*, 2001.
4. A. Pfitzmann and M. Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. [http://dud.inf.tu-dresden.de/Anon\\_Terminology.shtml](http://dud.inf.tu-dresden.de/Anon_Terminology.shtml), 2000.
5. Bruce Schneier. Choosing secure passwords. <http://boingboing.net/2014/02/25/choosing-a-secure-password.html>, 2014.
6. Andrew Nash, William Duane, Celia Joseph, and Joseph Brink. *PKI: Infraestructura de clave pública*. McGraw-Hill, Mexico, 2002.
7. PKCS#7. Cryptographic Message Syntax. <https://tools.ietf.org/html/rfc2315>, 2013.
8. Wolfgang Effing Wolfgang Rankl. *Smart Card Handbook*. Wiley, Mexico, 3 edition, 2004.

## CAPÍTULO 2



# POLÍTICAS DE SEGURIDAD

---

VÍCTOR BRAVO Y ANTONIO ARAUJO

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

### 2.1. Introducción

Las políticas de seguridad de la información deben seguir un proceso de actualización periódica sujeta a cambios en la organización y relacionados con actividades tales como: la gestión de talento humano, la realización de cambios en la infraestructura, la diversificación de las actividades, el desarrollo de nuevos servicios, la detección de vulnerabilidades y el incremento o decremento de los niveles de confianza. Ya que los empleados son los que llevan a cabo las tareas dentro de las organizaciones, es importante que las políticas de seguridad no se conviertan en una forma de restricción o carga para ellos.

Hay que tener en cuenta que todas las herramientas tecnológicas implementadas por una organización tales como cortafuegos, sistemas de detección de intrusos, dispositivos biométricos, entre otros, pueden resultar inútiles si existen elementos recurrentes en los procesos como la falta de información, el mal uso de los controles de seguridad de la información, el no cumplimiento de las políticas de seguridad o el desinterés o ánimo de causar daño de algún miembro desleal de la organización.

En este sentido se debe disponer de documentación sobre las reglas y normas vinculadas a la seguridad de la información. El objetivo de un documento de políticas de seguridad es proponer lineamientos generales a considerar desde el momento de definir las directrices de seguridad de la información de una organización de acuerdo a las necesidades o limitaciones que existan en ella, con el fin de concretar las ideas en documentos que orienten las acciones de la organización.

Todo proceso de la organización debe documentarse y clasificarse para su rápido y fácil acceso, de tal manera que no existan vacíos que se susciten en la práctica y que den pie a la improvisación o la aparición de una o más vulnerabilidades asociadas a sistemas informáticos. El establecimiento de un archivo físico o virtual con una normativa estricta es recomendable para la documentación de las políticas de seguridad.

El seguimiento de las políticas de seguridad y su documentación son elementos claves cuando una organización desea obtener una certificación, por lo tanto corresponde a uno de los pasos básicos en el proceso de maduración (mejora constante) de las políticas de seguridad.

En este capítulo se describen los elementos asociados a las políticas de seguridad de la información basados en el ciclo de los activos de información que está conformado por los siguientes conceptos: **amenaza**, **riesgo**, **vulnerabilidad**, **activos**, **valor activo**, **controles** y **Requisito de seguridad** (Ver fig. 2.1). También se ofrece un conjunto de consejos sobre la gestión de la seguridad en una organización considerando aspectos tales como el uso de las tecnologías libres, la gestión de contraseñas y el funcionamiento de un grupo dedicado a la seguridad de la información adaptado a una visión dinámica de la organización.



**Figura 2.1** Ciclo de la Seguridad de la Información

## 2.2. Políticas de seguridad de las tecnologías de información y comunicación

Las políticas de seguridad de la información en una organización representan una herramienta para mostrar a sus miembros la importancia y sensibilidad que se debe tener sobre este tema. Estas políticas deben describir las características clásicas de la seguridad de la información que se expresan a través de los siguientes conceptos:

- **Confidencialidad:** condición en la que sólo los usuarios autorizados tienen acceso al contenido de los datos.
- **Disponibilidad:** condición en la que se puede acceder a información o utilizar un servicio siempre que se necesite.
- **Integridad,** condición en la que se garantiza que la información o mensaje no han sido alterados.
- **No repudio:** condición en la que se previene que una entidad involucrada en una comunicación niegue luego su participación en la misma.

- **Control de acceso:** se controla el acceso a recursos de usuarios autorizados.

Las personas representan el eslabón más débil de la seguridad de la información, Ellas pueden seguir o no las políticas de seguridad que fueron definidas y aprobadas por la directiva, pueden realizar acciones que provoquen un agujero de seguridad en la red a través de instalación de software malicioso en las computadoras, revelación de información sensible a terceros entre otros. Según especialistas de la materia, el mayor porcentaje de fraudes, sabotajes, accidentes relacionados con los sistemas informáticos son causados desde lo interno [4], ya que las personas que pertenecen a la institución pueden conocer perfectamente los sistemas, sus barreras y sus puntos débiles.

El objetivo entonces, es proponer lineamientos generales a considerar desde el momento de definir las directrices de seguridad de la información de una institución de acuerdo a las necesidades y limitaciones que existen en ella, de manera de concretar las ideas en documentos que orienten las acciones de la organización.

### 2.3. Importancia de la seguridad de la información

Las organizaciones deben entender que la seguridad de la información es un proceso que debe desarrollarse en ciclos iterativos y no como una receta. Dicho en otras palabras se entiende como el hecho de generar una relación vivencial con la tecnología y sus actores, a través de la construcción de una experiencia que modifique la visión de equipo y que sigue un objetivo en común.

Basado en ello se pueden definir los objetivos más importantes a seguir en el área de la seguridad de la información:

- Minimizar y gestionar los riesgos detectando los posibles problemas y amenazas a la seguridad de la información.
- Garantizar la utilización adecuada de los recursos y de las aplicaciones en los sistemas.
- Limitar la pérdida de información y recuperar sistemas en caso de un incidente de seguridad de la información.

Para cumplir con estos objetivos las instituciones deben contemplar tres planos de actuación: Técnico, Humano e Institucional.

#### **Dentro del plano *técnico* se tienen las siguientes actividades:**

- Evaluación de los activos físicos y de información de la organización.
- Selección, instalación, configuración y actualización de las soluciones de hardware y software.
- Incorporación de elementos criptográficos a los procesos y aplicaciones.
- Desarrollo seguro de aplicaciones.

#### **Dentro del plano *humano* se tienen las siguientes actividades:**

- Promoción de buenas prácticas de actuación vinculadas con la seguridad de la información.
- Sensibilización y formación del personal y directivos de la institución.
- Funciones, obligaciones, responsabilidades del personal.

Y dentro del plano *institucional* se deben definir e implementar políticas, normas, procedimientos de seguridad de la información y planes de contingencias en casos de desastres en el contexto de los activos de información.

## 2.4. Seguridad de la Información para Tecnologías Libres

En el ámbito de las tecnologías libres y específicamente en el software libre, la noción de seguridad ha sido objeto de controversia. Entusiastas del software libre promueven las potencialidades de este tipo de software en contraste con el software propietario. Asimismo, los partidarios del software propietario y que están detrás de los desarrollos de este tipo, promueven sus aplicaciones y herramientas tomando como un especial elemento de protección el uso de actualizaciones.

Las potencialidades intrínsecas del software libre permiten incorporar elementos de seguridad en sistemas informáticos de instituciones, organizaciones y hasta usuarios finales. Entre estas potencialidades se incluyen:

- La capacidad de analizar y estudiar las tecnologías subyacentes a las aplicaciones.
- La posibilidad de auditar los programas fuentes (código escrito en un lenguaje de programación)
- La frecuente corrección de errores y publicación de software gracias al apoyo de comunidades de usuarios y desarrolladores alrededor de las aplicaciones y herramientas.
- El rompimiento del paradigma de la seguridad por obscuridad el cual determina que el funcionamiento de procedimientos de seguridad (criptográficos) deben ser secretos y por lo tanto la seguridad solo reside en la capacidad de ocultar su funcionamiento y no las claves.

La seguridad de la información en software libre sigue un modelo de desarrollo de software basado en la cooperación, así como en la creación de comunidades en torno a una tecnología. En el mundo del software libre existen aplicaciones y herramientas con características y funcionalidades similares a las existentes en el software propietario. Inclusive en algunos casos se reconocen herramientas de software libre como mejores opciones tal como el caso del servidor web *Apache*<sup>1</sup>. La adopción de software libre como alternativa para mejorar la seguridad de la información en organizaciones implica un cambio de pensamiento, un cambio del modelo imperante basado en la gestión de compras de soluciones, por un modelo que incorpora tecnologías libres en búsqueda de la mejora continua de los procesos.

## 2.5. Principio de defensa en profundidad

Se refiere a una estrategia de origen militar que tiene por objetivo hacer que el atacante pierda el empuje inicial y se vea detenido en sus intentos al requerir superar varias barreras en lugar de una [1]. En informática consiste en el diseño e implementación de varias líneas de seguridad independientes dentro del mismo sistema informático. De este modo, si una de las líneas de seguridad logra ser traspasada por los atacantes, conviene disponer de líneas de seguridad adicionales que dificulten, debiliten y retrasen el ataque en desarrollo, evitando el acceso o control no autorizado de los activos de información de la organización.

El enfoque tradicional de seguridad que se presenta en la figura 2.2, establece una sola línea de seguridad alrededor de los activos de manera que cubra la mayor área posible. Un problema que presenta este enfoque es que la línea de seguridad es susceptible a tener vulnerabilidades dadas por una mala configuración del sistema de protección o la ocurrencia de fallas en los sistemas. Es necesario subrayar que una vez que un ataque supera esta línea de seguridad, las formas de detenerlo son mínimas.

Por otro lado el enfoque de defensa en profundidad, como muestra la figura 2.3, establece múltiples líneas de seguridad, donde las vulnerabilidades de una línea de seguridad son cubiertas por las fortalezas de las otras.

Cada vez que un atacante atraviesa una de las líneas de seguridad existe la posibilidad que se generen alertas y el ataque pueda ser detectado. Se pudiese obtener información sobre su origen, naturaleza, anomalías y con esto se puede reforzar las otras líneas de seguridad, que podrían detener el ataque o que el mismo no genere pérdidas mayores a la organización, además permite, corregir en cierta medida la o las vulnerabilidades de las líneas de seguridad que fueron traspasadas.

<sup>1</sup>El sitio web de este software se encuentra en la dirección web <http://www.apache.org>



**Figura 2.2** Enfoque tradicional de Seguridad.

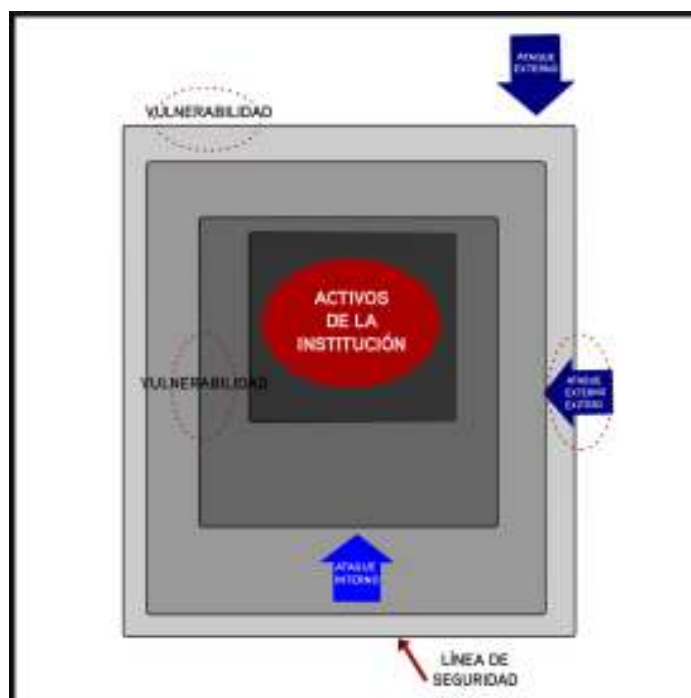
Este enfoque permite cubrir varios de los puntos de riesgos de un sistema y dependiendo de la estructuración de las líneas de seguridad, también funciona para proteger a los activos de información de los ataques internos.

Dentro de una organización existen múltiples grupos de usuarios con diferentes actividades y responsabilidades, por lo que se requiere estructurar las líneas de seguridad de manera que para cada grupo de usuario le corresponda una línea logrando de forma efectiva incrementar la protección contra atacantes internos.

### 2.5.1. Los principios generales de la defensa en profundidad

Este enfoque está basado en una visión en cascada que puede describirse en base a las siguientes consideraciones:

- Engloba todos los aspectos de gestión técnica y de ejecución.
- Los medios implementados actúan gracias a una capacidad de alerta y difusión que proviene de una correlación de los incidentes.
- Las acciones a tomar deben ser dinámicas: deben tener una evaluación constante del contexto.
- Las políticas de seguridad contemplan la capacidad de reacción y planificación de acción ante incidentes.
- Las acciones a tomar deben ser suficientes. Cada medio de protección (humano o técnico) debe contar con protección propia, medios de detección y procedimientos de reacción.
- Los activos deben protegerse en función a su sensibilidad y nivel de importancia de manera de contar con al menos tres líneas de seguridad.



**Figura 2.3** Enfoque de defensa en profundidad.

## 2.6. Responsabilidad

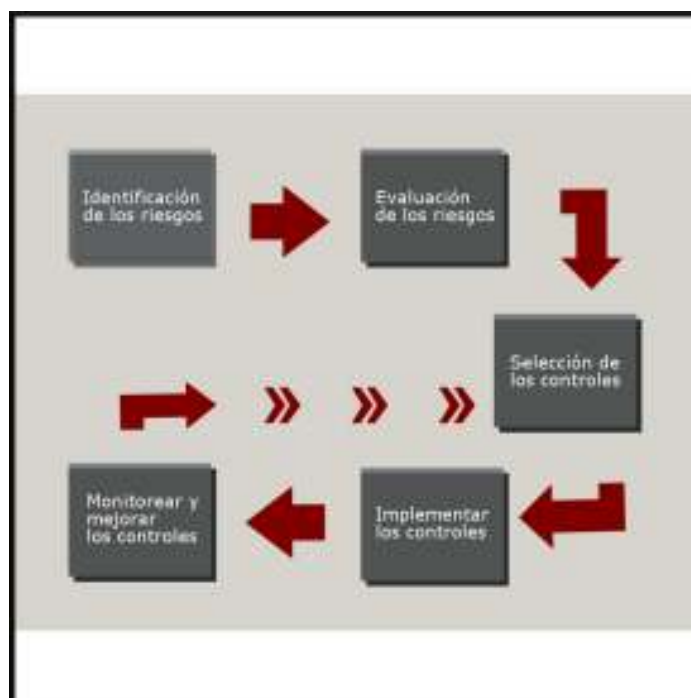
Antes de que se apliquen las políticas de seguridad en una organización deben ser aprobadas, publicadas, documentadas, y comunicadas a todos sus miembros, ya que estos son los responsables de la aplicación y cumplimiento de dichas políticas en cada una de sus áreas.

Todos los roles y responsabilidades de la seguridad de la información deberían estar claramente definidas y documentadas. Su asignación debería realizarse en concordancia con las políticas de seguridad. Las personas con responsabilidades en la seguridad de la información pueden delegar las tareas de seguridad a otros. No obstante, ellos siguen siendo responsables y deberán determinar si cualquier tarea delegada ha sido realizada correctamente.

No se recomienda que todas o la mayoría de las responsabilidades de la seguridad de la información y el manejo de las actividades críticas de la organización estén sobre un grupo pequeño de personas. Esta situación generaría una debilidad en la seguridad de la información, que por ejemplo podría afectar al normal funcionamiento de la organización si este grupo pequeño de personas por alguna razón no pueden atender sus compromisos.

## 2.7. Procesos para aumentar la adopción de seguridad de la información

Es esencial que las organizaciones identifiquen claramente sus requisitos de seguridad. La figura 2.4 muestra la relación entre los procesos a incluir para lograr esta acción de manera de alcanzar el objetivo de cumplir con las metas referentes a la seguridad de la información. Entre los procesos se encuentran: la identificación y evaluación de los riesgos, la revisión, el monitoreo y la selección e implementación de controles.



**Figura 2.4** Proceso de percepción de la Seguridad.

### 2.7.1. Identificación de los riesgos

Es una medida que busca encontrar vulnerabilidades en los activos que puedan ser explotados por terceros. Es necesaria la identificación de los riesgos que puedan existir en la organización. Es importante considerar los distintos ámbitos de la implementación de la seguridad alrededor de donde se encuentra la información.

Entre los aspectos a considerar se encuentran:

1. **Técnico:** se refiere al conocimiento que se tiene de la configuración de los componentes de toda la infraestructura tecnológica de respaldo, comunicación, procesamiento, tránsito y almacenamiento de la información. Los activos en este ámbito son aplicaciones, equipos informáticos y de comunicación, datos, documentación, manuales, consumibles, servicios ofrecidos a usuarios internos y externos. Este aspecto requiere la realización de un inventario de los activos antes mencionados que permite:
  - Contar con un registro actualizado de los activos de información.
  - Facilitar la detección de vulnerabilidades.
  - Conocer la sensibilidad de la información que se manipula, clasificándola en función al grado de importancia para la institución.
  - Identificar los posibles objetivos de los ataques o de los intentos de intrusión.
  - Recuperar datos importantes de forma organizada y eficiente.

De la misma forma se hace necesario identificar los puntos de accesos a la red y los tipos de conexiones utilizadas.

2. **Humano:** referido a las maneras en que las personas se relacionan con los activos de información, como también de las prácticas que se tienen en materia de seguridad de la información. De esta manera es



posible detectar cuáles vulnerabilidades provienen de acciones humanas para dirigir recomendaciones y garantizar la continuidad de las actividades de la organización. Para su identificación se debe:

- Determinar la formación del personal en materia de seguridad
- Determinar las prácticas en materia de seguridad de la información.

3. **Físico:** pretende identificar la infraestructura física. El enfoque principal de este ámbito de análisis son los activos de la organización, pues son los que proveen el soporte físico al entorno en que está siendo manipulada la información. Para lograr este objetivo se deben realizar las siguientes acciones:

- Identificar las condiciones físicas y ubicación donde se encuentran los equipos computacionales.
- Identificar los servicios requeridos como electricidad, comunicación, agua, entre otros.
- Identificar los controles de accesos físicos existentes.
- Identificar los controles de protección y extinción de incendios.

### 2.7.2. Evaluación de los riesgos de seguridad

Una vez que se obtiene la lista de riesgos esta se debe someter a evaluaciones para determinar, cuantificar y clasificar los elementos más importantes relacionados con los objetivos relevantes para la organización.

La evaluación de los riesgos debe conseguir como resultado un conjunto de recomendaciones para la selección y corrección de los controles sobre los activos de manera que puedan ser protegidos adecuadamente.

La evaluación de los riesgos de seguridad deben tener presente y definido el alcance que va a tener para que la política sea efectiva. La evaluación de los riesgos procura determinar:

- Amenazas al funcionamiento normal de la organización.
- La medición del impacto de la concreción de un ataque.
- La posible frecuencia con la que podrían ocurrir ataques.

Los resultados de la evaluación deben guiar y determinar las acciones en el tratamiento de los riesgos. Esta evaluación puede que requiera ser realizada periódicamente cuando se tengan cambios significativos, nuevos requerimientos de los sistemas, situaciones de riesgos, amenazas, vulnerabilidades, o cualquier cambio que podría influir en el normal funcionamiento de los procesos de la organización.

Las evaluaciones se pueden aplicar a toda la organización, a parte de ella, a un sistema de información en particular o a componentes específicos del sistema. Los riesgos deben ser aceptados por toda los empleados de manera objetiva. De ser necesario hay que transferir los riesgos a terceros como proveedores o aseguradoras.

Hay herramientas para la evaluación de vulnerabilidades que permiten conocer la situación real de un sistema y mejorar su seguridad, verificando que los mecanismos de seguridad funcionen correctamente. Con esta información obtenida es posible justificar la implantación de nuevas medidas de seguridad, así como de priorizar las medidas a implementar en función a las vulnerabilidades detectadas.

Dentro de las evaluaciones de la seguridad de los sistemas informáticos se realizan las pruebas de penetración internas y externas. Una prueba de penetración consta de las siguientes etapas:

- Reconocimiento del sistema para averiguar qué tipo de información podría obtener un atacante o usuario malicioso.
- Detección y verificación de las vulnerabilidades en los servidores y aplicaciones desarrolladas por la organización.
- Intento de utilizar las vulnerabilidades detectadas.
- Generación de informes, con el análisis de los resultados.

### 2.7.3. Selección de los controles

Luego de evaluar los riesgos de seguridad se decide el tratamiento que se debe seguir para evitar la aparición de fallas en los sistemas informáticos. Este procedimiento se conoce como mitigación de riesgos, y se realiza seleccionando los controles que aseguren un nivel adecuado de seguridad para la organización. Se realiza una investigación sobre las posibles soluciones existentes para cada uno de los riesgos identificados de cada ámbito, por ejemplo, en el ámbito técnico se hace una investigación de las tecnologías existentes que cubran los riesgos identificados (cortafuegos, redes privadas virtuales, protocolos de comunicación seguros, sistemas de detección de intrusos de red y estaciones de trabajo, sistemas de escaneo de puertos, entre otros).

En el ámbito humano, una medida efectiva es el dictado de charlas y de cursos de seguridad de tal manera que se puedan sensibilizar a las personas que interactúan con los sistemas informáticos.

En el ámbito físico, la instalación de circuitos cerrados de televisión, instalación de controles físicos, remodelación o reforzamientos del centro de datos.

Es importante considerar el gasto de los controles de seguridad, ya que este debe equilibrarse con el daño probable que resulta de las debilidades en la seguridad de la información. Si el gasto de los controles es mucho mayor al posible daño que pudiera resultar, la institución pudiera asumir el riesgo de ocurrencias de incidentes de seguridad por esa debilidad en la seguridad de la información y no colocar el o los controles de seguridad.

Existen controles que se consideran principios orientativos y esenciales, que proporcionan un punto de partida adecuado para implementar la seguridad de la información como son las políticas de seguridad. En este sentido se deben considerar las siguientes acciones:

- Aprobar, documentar, publicar y comunicar las políticas de seguridad a todos los miembros de la organización de forma adecuada, utilizando como herramientas charlas y/o cursos en materia de seguridad.
- Asignar las responsabilidades de seguridad a miembros de la organización.
- Identificar los procedimientos de seguridad asociados a los activos de información.
- Definir y documentar los niveles de autorización.
- Registrar las incidencias y mejoras de seguridad.
- Desarrollar e implementar procedimientos de gestión de continuidad de actividades para disminuir la interrupción causada por los desastres y fallas de seguridad.
- Salvaguardar los registros de la organización. Se deben proteger los registros importantes de la organización frente a su pérdida, destrucción o falsificación.
- Sensibilización y formación de los miembros de la institución en materia de seguridad de la información

### 2.7.4. Implementar los controles seleccionados

Es recomendable que los controles en el plano técnico se implementen en un ambiente de pruebas antes de colocarlos en el ambiente de producción para no generar inconvenientes en los servicios informáticos.

Se deben configurar e implementar los controles de tal manera que existan varias líneas de seguridad independientes dentro del mismo sistema informático para dar cabida al concepto de seguridad en profundidad.

Esto permite aumentar la conciencia y conocimiento a los miembros de la organización con el objetivo de que puedan reconocer los problemas e incidentes de seguridad de la información, y responder adecuadamente a las necesidades según su rol dentro de la organización.

### 2.7.5. Supervisar y mejorar los controles de seguridad

Los controles de seguridad deberían ser revisados en períodos planificados o cuando ocurran cambios significativos que puedan afectar la eficiencia y eficacia de los mismos.

Se recomienda la realización de pruebas y auditorías periódicas de seguridad. Esto constituye un elemento de gran importancia para poder comprobar la adecuada implantación de los controles de seguridad y medidas definidas en las políticas de seguridad de la información. Para ello se debe realizar:

- Un análisis de posibles vulnerabilidades de los sistemas informáticos, para localizar de forma automática las más conocidas.
- Pruebas de intrusión, en las que no sólo se detecten las vulnerabilidades, sino que se realicen ejecuciones controladas de las que se hayan identificado.
- Registros de incidentes de seguridad de la información.

Con esta información es posible justificar la implantación de nuevas medidas de seguridad, así como de priorizar las medidas a ejecutar en función a las vulnerabilidades detectadas.

## 2.8. Grupo de seguridad de la información

Se propone la formación de un grupo de personas con conocimientos y formación profesional en ciencias de la computación e informática, que tendrá entre sus responsabilidades:

- La supervisión y la realización de pruebas de seguridad en los puestos de trabajo y servidores de la institución, con el objetivo de detectar vulnerabilidades y generar reportes y recomendaciones.
- La investigación en temas relevantes y actuales en el área de seguridad de la información.
- El diseño de mecanismos para detección de ataques, prevención y recuperación de datos en casos de fallas.
- La coordinación de la implementación de controles de seguridad.
- La promoción del uso de herramientas y buenas prácticas en materia de seguridad de la información.
- La realización de auditorías de seguridad, revisión de los registros y actividades de los sistemas para verificar y asegurar que se cumplen las políticas de seguridad y los procedimientos operativos establecidos. Detectar las infracciones y recomendar oportunamente modificaciones en los controles, políticas y procedimientos de seguridad.
- El cumplimiento y adecuación de la institución a los estándares más conocidos en seguridad de la información tal como el *ISO 27001*<sup>2</sup>.

## 2.9. Gestión de contraseñas

El objetivo de la gestión personal de contraseñas es seleccionar palabras lo suficientemente difíciles de romper”, es decir, que no puedan ser generadas paralelamente por un procedimiento que utilice otra persona no autorizada para acceder a los activos de información que la contraseña protege.

El uso de contraseñas es el mecanismo más utilizado para la autenticación en los sistemas informáticos, pero de la misma forma representa uno de los puntos mas débiles en la seguridad de la información. Utilizando técnicas como el *phishing*, espionaje, ingeniería social, engaño, extorsión o fuerza bruta se pueden obtener contraseñas y provocar daños o alteraciones significativas a los activos de información.

Hay muchos usuarios que eligen contraseñas muy cortas o de fácil asociación con datos personales. Existen sistemas informáticos que asignan de manera automáticas contraseñas con un tamaño adecuado (por ejemplo

<sup>2</sup>Para consultar el estándar puede ir a la dirección web: <http://www.iso.org/iso/es/home/standards/management-standards/iso27001.htm>

de longitud mayor o igual a 8) y cuyos caracteres son seleccionados aleatoriamente entre símbolos, números y letras minúsculas y mayúsculas, es decir, que cumplen con la condiciones para una buena contraseña, pero que representan una carga para los usuarios al ser difíciles de recordar.

Existen algunas recomendaciones generales para la generación de las contraseñas que pueden ser útiles para cualquier persona. A continuación se describen algunas reglas a seguir para tener contraseñas de difícil rompimiento:

- No solo se conformen con letras o números, es mejor utilizar la combinación de ambos grupos y que incluyan mayúsculas, minúsculas y caracteres especiales.
- Usar siempre diferentes contraseñas para los distintos sistemas informáticos.
- No utilice palabras que puedan encontrarse en un diccionario (de inglés, español u otro idioma popular).
- No repita el mismo símbolo seguido en la contraseña, por ejemplo evitar palabras del tipo .<sup>a</sup>aaaa.<sup>o</sup> "zzzzzz".
- Use contraseñas de longitud mayor o iguales a 8 símbolos (caracteres). Este es un número mínimo para que la contraseña no sea considerada de débil rompimiento.
- Pruebe la fortaleza de la contraseña con algún servicio certificado (que utilice protocolo https y sea reconocido) en internet.
- No comparta las contraseñas con otras personas. En lugar de ello solicite al administrador del sistema informático que active procedimientos de delegación de tareas donde se le otorga un permiso temporal a un tercero sin compartir la contraseña personal.

Ahora bien, cualquier persona se puede formular la siguiente pregunta: ¿Cómo se puede generar una clave que sea fácil de recordar, que cumpla las recomendaciones descritas anteriormente, que no pueda ser descubierta por cualquier atacante, y que además, no genere una carga para el usuario en su generación, recordación, resguardo y utilización?.

Como respuesta a esta pregunta se han desarrollado sistemas de software integrados con los navegadores web que facilitan la generación y resguardo de claves. Sin embargo, el principal elemento para contar con una buena gestión de contraseñas es la responsabilidad de las personas para generar y resguardar sus claves, y se debe tomar en cuenta que esto depende de las costumbres, el contexto social, el uso consciente, el tipo de información que resguarda y el nivel de riesgo que implica el acceso a determinados activos de información.

### 2.9.1. Tamaños de contraseñas

Suponga que existen 96 caracteres posibles a utilizar en una clave (letras minúsculas y mayúsculas, números y caracteres especiales). En una clave con 8 dígitos existen  $96^8$  (más de 7 trillones) posibilidades para descubrirla y analizando 1.000.000 posibilidades por segundo tardaría 228 años, en probarlas todas (peor de los casos)[3].

Probablemente no se dispone de esa cantidad de tiempo para verificarlos por el método de fuerza bruta. Existen métodos que reducen el tiempo de descubrimiento de las contraseñas como probar primero con palabras de diccionarios, palabras que tenga relación con el usuario, ya que la mayoría de las contraseñas de los usuarios se conforman de esta manera.

Existen técnicas básicas para la selección de contraseñas. Se les puede explicar a los usuarios la importancia de usar palabras difíciles como contraseñas, sensibilizándolos en las posibles implicaciones de una mala gestión de las contraseñas. A continuación se explica un método para construir una contraseña fuerte que permite ser recordada a través de la asociación. Para ello debemos seleccionar una oración que sea fácil de recordar y a partir de ella generar la contraseña. Por ejemplo:

- Oración 1 (Ejemplo 1), *Mi hermana Sofía me regaló una poderosa computadora*

- Oración 2 (Ejemplo 2), *Pase todas las materias con 20 puntos*

Si tomamos los primeros caracteres de cada palabra de la oración nos resultaría:

- Oración 1 (Ejemplo 1), MhSmrlpc
- Oración 2 (Ejemplo 2),Pt1mc20p

Si a esto se le incorpora reglas como por ejemplo, cambiar la p por algún símbolo, que para este caso será (%), entonces las oraciones quedarían:

- Oración 1 (Ejemplo 1), MhSmrl %c
- Oración 2 (Ejemplo 2), %t1mc20 %

Como se puede notar, de esta manera se generaría una buena contraseña, que es difícil de romper por un tercero, y fácil de recordar para la persona ya que es generada a partir de oraciones particulares que generalmente están asociadas con el usuario autorizado.

## 2.10. Entornos de la Seguridad de la Información

En una organización se pueden establecer claramente dos ambientes de trabajo asociados a la infraestructura informática que tienen características bien definidas, y por lo tanto tienen sus especificidades a tomar en cuenta. Estos ambientes son los concernientes a los puestos de trabajo y a los centros de datos. En los párrafos siguientes se describen conceptos y herramientas vinculados con estos entornos desde la perspectiva de la seguridad de la información.

### 2.10.1. Puesto de trabajo

Un puesto de trabajo es el lugar físico o lógico donde al usuario se le asignan ciertos privilegios de acceso a los recursos. El puesto de trabajo es el lugar que le permite al usuario autorizado el desarrollo y cumplimiento de las tareas, funciones y actividades que ejecuta para la institución. Los puestos de trabajos forman parte de los bienes o activos de la institución y debe existir una responsabilidad por parte de la persona asignada para su mantenimiento, correcto uso y funcionamiento.

### 2.10.2. Centro de datos

El centro de procesamiento de datos se define como una infraestructura y plataforma tecnológica (cómputo, almacenamiento y comunicaciones), que tiene como objetivo prestar la mayoría de los servicios informáticos y de comunicaciones. En el centro de datos se concentran y procesan todos los recursos lógicos con que opera la organización.

## 2.11. Tipos de Seguridad de la Información

### 2.11.1. Seguridad Lógica

Se refiere a la aplicación de mecanismos y procedimientos para mantener el resguardo, la integridad de activos informáticos (archivos, sistemas, datos, entre otros) y el acceso a personas autorizadas a los activos lógicos de la organización.

Un activo lógico o activo de información es un conjunto de datos estructurados que tiene un valor directo o potencial y que su alteración o eliminación no autorizada representa un daño o perjuicio para la organización.

### 2.11.2. Seguridad Física

La seguridad física se refiere a los mecanismos de seguridad que generan barreras físicas y de control de los equipos computacionales como medida de prevención y protección de los activos informáticos de la organización, evitando el acceso no autorizado a los equipos y a los medios de almacenamiento de datos.

## 2.12. Cuenta de usuario

Es el conjunto de autorizaciones para ejecutar acciones sobre un sistema informático asociadas a un nombre de usuario y se vincula con una persona natural o jurídica a través del registro de una serie de datos personales.

### 2.12.1. Cuenta de usuario crítica

Son aquellas cuentas que dan accesos a recursos, servicios e información que se consideran importantes o vitales para el normal funcionamiento de los recursos o servicios de la organización como por ejemplo: cuentas de administración de los equipos de computación (que en algunos sistemas se denomina *root*).

## 2.13. Vulnerabilidades de los sistemas de información

Se refiere a las fallas presentes en los esquemas de autenticación y autorización de los sistemas informáticos, y que pueden afectar los niveles de confidencialidad, integridad, disponibilidad de los datos y aplicaciones.

### 2.13.1. Causas de las vulnerabilidades de los sistemas informáticos

Entre las causas que se consideran responsables de las vulnerabilidades que afectan a los sistemas informáticos se tienen:

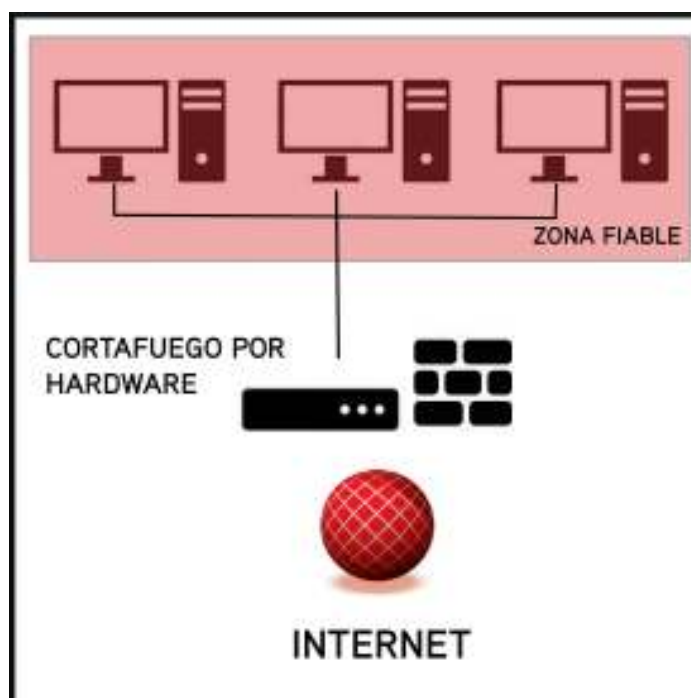
- Debilidad en el diseño de los protocolos utilizados en las redes, como por ejemplo los protocolos de transmisión de datos en texto claro.
- Fallos en los diseños y/o codificación de los programas.
- Configuración inadecuada de los sistemas informáticos.
- Políticas de seguridad deficientes o inexistentes.
- Desconocimiento y falta de sensibilidad de los usuarios y de los responsables de informática. Todas las soluciones tecnológicas que la organización pueda implementar (sistemas de detección de intruso, cortafuego, entre otros) resultan inútiles ante el desinterés, falta de información, falta de preparación en materia de seguridad. La falta de sensibilización de los directivos y responsables de la organización, que deben estar conscientes de la necesidad de destinar recursos a esta función.
- Poca y pobre documentación de software y hardware.
- La instalación incorrecta de software o hardware, o fallas en la configuración y su mantenimiento.

La organización podría utilizar herramientas para realizar análisis y evaluación de vulnerabilidades, que permitan conocer la situación real de los sistemas y de acuerdo con esa información se podrían reajustar las políticas de seguridad, implantación de mecanismos o medidas de seguridad.

## 2.14. Herramientas para la seguridad de la información

### 2.14.1. Cortafuegos

Un cortafuegos es un sistema que permite filtrar las comunicaciones entre dos o más redes (por ejemplo la red de una institución (red privada) e Internet) a partir de unas reglas definidas de acuerdo con las políticas de seguridad de la organización, en procura de proteger la red y los activos de información de ataques provenientes de una red que no es confiable como la Internet.



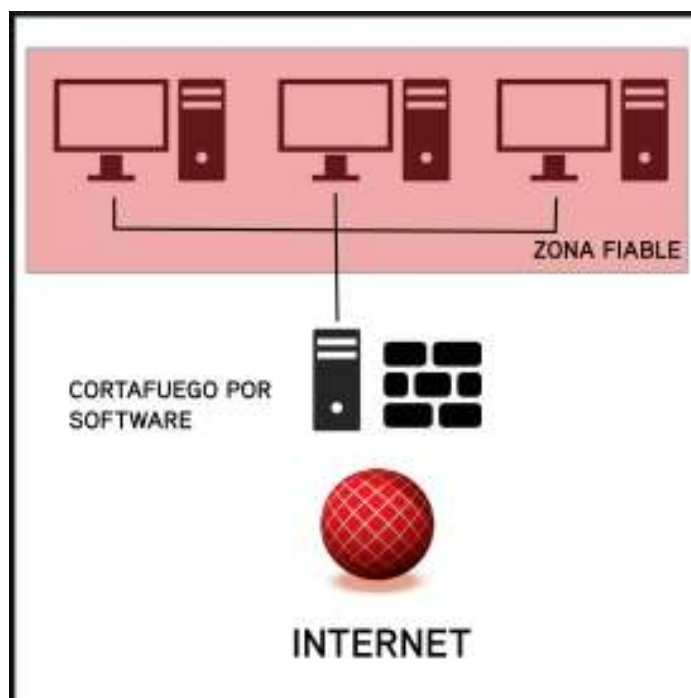
**Figura 2.5** Cortafuegos por Hardware.

Existen cortafuegos por software (Figura 2.6) y por hardware (Figura 2.5). En el cortafuegos por software, hay que definir y probar la mayoría de las reglas, ocupa espacio y procesamiento en el servidor donde está instalado, son mucho más baratos y por lo general son utilizados en organizaciones pequeñas.

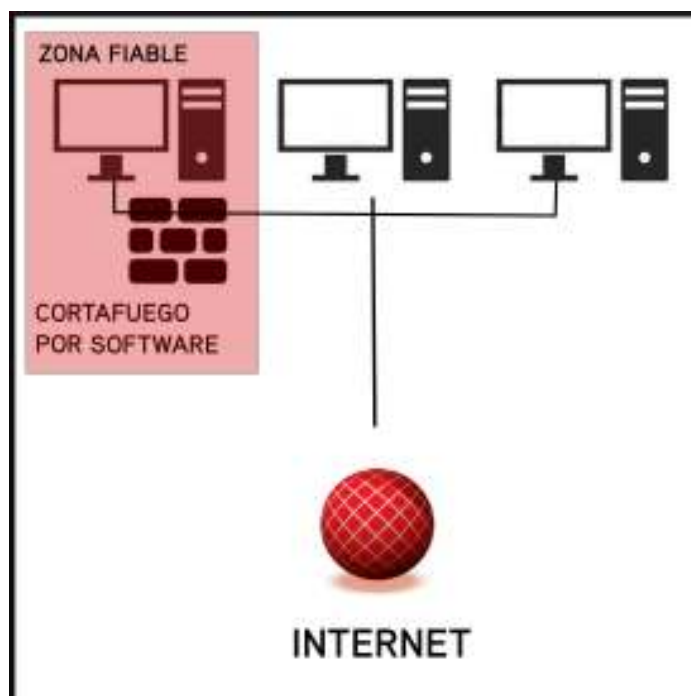
Todo el tráfico entrante y saliente de la institución debe pasar a través del cortafuegos por lo que el administrador puede permitir o denegar el acceso a la Internet y a los servicios de la institución: un segmento de la red interna, una máquina en específico, de manera selectiva.

También se puede instalar un cortafuegos en un computador dentro de la red interna — *cortafuegos personal* — (Ver figuras 2.7, 2.8 ) que sólo controle el tráfico que entra y sale desde y hacia esa computadora respectivamente, de esta manera se pueden agregar reglas de filtrados de acuerdo a la necesidad del usuario.

**Cortafuegos personal:** es el término utilizado para los casos donde el área protegida se limita sólo al computador donde está instalada la protección contra atacantes.

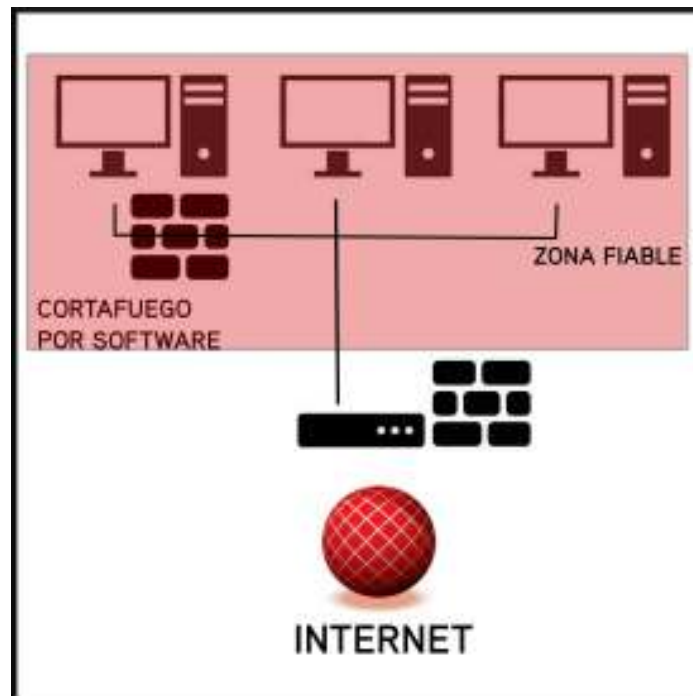


**Figura 2.6** Cortafuegos por Software.



**Figura 2.7** Cortafuegos personal.





**Figura 2.8** Cortafuegos personal combinado.

### 2.14.2. Utilidad de un cortafuegos

Es una herramienta de seguridad, que ofrece los siguientes servicios:

- Restringir el acceso a determinados programas, segmento de red de la organización, servicios de internet, ciertas paginas web, bloqueando el tráfico no autorizado por la organización y no permitiendo ataques a las computadoras desde el exterior e interior de la red.
- Ocultar equipos internos de la organización, de forma que éstos no puedan ser detectados ante ataques que provengan del exterior. Asimismo pueden ocultar información sobre la topología de la red interna, los nombres de los equipos, tipo de protocolos utilizados, etcétera.
- Auditar y registrar el uso de la red de datos.
- Mejorar el aprovechamiento del ancho de banda utilizado en la organización.
- Coadyuvar en la supervisión sobre ataques e intentos de intrusión a la red de la institución.

### 2.14.3. Consideraciones para la instalación y configuración de cortafuegos

Se deben tener las siguientes consideraciones para la instalación y la configuración de un sistema cortafuegos, ya sea éste en software o hardware:

- Conocer los protocolos y servicios de internet.

- El equipo debe encontrarse libre de virus <sup>3</sup>, de programas espías (*spyware*), programas maligno (*malware*).
- Analizar los servicios requeridos de internet y de la información que se maneja en los puestos de trabajos o servidores.
- Clasificar o estructurar la red interna por zonas (de red) de acuerdo a las necesidades de seguridad.
- Mantener actualizado el software del cortafuegos.

Finalmente, las reglas de filtrado son difíciles de definir y de verificar, por lo que deberían ser revisadas frecuentemente por los administradores de la red.

#### 2.14.4. Sistemas de detección de intrusiones (IDS)

Los IDS son sistemas que tienen el objetivo de detectar y reaccionar de forma automática antes los incidentes de seguridad que tienen lugar en las redes y computadoras de una organización. Los IDS funcionan en base a patrones que identifican comportamientos sospechosos o ataques que ya han sido establecidos por defecto. La mayoría de estos sistemas admiten agregar patrones definidos por el usuario, en este caso por el administrador del sistema, de manera que se evite o detenga la intrusión.

Un IDS lo conforman los siguientes elementos:

- Una fuente de eventos del sistema.
- Una base de datos con los patrones de comportamiento que se consideran como normales, así como los perfiles de posibles ataques.
- Motor de análisis de los eventos para detectar las evidencias de intentos de intrusión.
- Módulo de respuesta que, de acuerdo al análisis de los eventos, realice determinadas acciones.

La figura 2.9 muestra la estructura funcional básica de un IDS.



**Figura 2.9** Estructura funcional básica del IDS.

<sup>3</sup>si se utiliza software libre la probabilidad de que el equipo se encuentre infectado será muy baja

Un IDS puede presentar problemas y limitaciones que podrían generar falsas alarmas tales como **falsos negativos** que se producen cuando no pueden detectar algunas actividades relacionadas con incidentes de seguridad que están ocurriendo en la red o en los equipos informáticos, o bien falsos positivos, que se presentan cuando los sistemas registran y generan alertas sobre determinadas actividades que no son problemáticas o no representan una amenaza.

## 2.15. Identificación de los riesgos a terceros

Cuando se da acceso a terceras personas ajenas al funcionamiento rutinario de los activos de información de la organización, en primer lugar se debe llevar a cabo una evaluación de los riesgos para determinar las implicaciones en la seguridad y los requisitos para establecer los controles. Para cada grupo externo de personas se debe llevar a cabo la evaluación y definición de los controles de seguridad.

Para este tipo de riesgos se recomienda registrar los siguientes datos:

- Los medios de procesamiento de información a los cuales se necesita tener acceso.
- Evaluar el nivel de confidencialidad de los datos a los que se accede.
- Expresarle (por escrito, si es posible) a las terceras personas las políticas de seguridad de la información de la organización .
- Evaluar el nivel de confianza, entendido como qué tanto se confía para que terceros no dañen o usufructúen los activos de información de la organización. Esto puede realizarse utilizando una historia detallada de incidentes de seguridad, la cuál puede resumirse utilizando herramientas estadísticas.
- Configurar los recursos informáticos requeridos.
- Cargar los procesos en la realización de la actividades para el cumplimiento de las políticas de seguridad.
- Especificar el nivel de seguridad físico (espacio físico) en su estancia dentro de las instalaciones de la organización.
- Disponibilidad de una red inalámbrica o cableada con sólo determinados servicios de acuerdo a las necesidades de las personas.
- Establecer las responsabilidades de los empleados por actos de las personas que utilicen activos de información como el uso del correo institucional, acceso a la información confidencial a terceros, ataques o intento de intrusión contra equipos utilizando la red de la organización.

## 2.16. Seguridad lógica en los puestos de trabajo

El puesto de trabajo se entiende como el conjunto de activos físicos y lógicos asignado a un miembro de la organización, el cual tiene la responsabilidad de usarlo siguiendo las políticas de la organización y en particular las específicas sobre seguridad de la información. Entre las recomendaciones referentes a controles para los puestos de trabajo se listan las siguientes:

- Determinar y clasificar el grado de criticidad de la información que se maneja en los sistemas de almacenamiento ubicados en los puestos de trabajo.
- Las contraseñas de administración de los equipos computacionales sólo deben ser conocidas por las personas responsables del puesto de trabajo. La contraseña principal de acceso a cada equipo debe ser seleccionada siguiendo las recomendaciones propuestas en la sección 2.9.

- Realizar cambios de las contraseñas cuando se tenga el menor indicio de vulnerabilidad o se sospeche que personas no autorizadas tengan acceso a datos confidenciales.
- Definir políticas para generar, eliminar, y modificar las claves de usuarios en los puestos de trabajo evitando la carga de trabajo para las personas.
- Mantener el sistema operativo y aplicaciones actualizadas.
- Utilizar herramientas y procedimientos que verifiquen la integridad y la fuente de los paquetes a instalar (mecanismos de verificación de integridad y autoría).
- Utilizar el correo institucional con la activación de métodos criptográficos para proteger la confidencialidad e integridad de los mensajes.
- Establecer políticas referentes al bloqueo automático de las sesiones de trabajo cuando el responsable del puesto no se encuentre en él.
- Recomendar la instalación y configuración de cortafuegos personales para incrementar la seguridad en el puesto de trabajo.

## 2.17. Seguridad lógica en los centros de datos

- Seleccionar los protocolos de comunicación en función a las necesidades de la institución.
- Segmentar la red de la institución por grupos de usuarios, servicios internos y externos.
- Utilizar sistemas de detección de intrusos, para detectar el acceso no autorizado a los activos de información de la institución.
- Respalidar la información local y de los servidores de forma periódica.
- Cerrar todas las sesiones de red después de ser utilizadas. Para esto se pueden utilizar programas que automáticamente realicen este tipo de acciones.
- Controlar el acceso remoto a los equipos de la red institucional a través de herramientas seguras.
- Utilizar sistemas de controles de cambios para verificar las modificaciones realizadas en los equipos de computación.
- Utilizar buenas prácticas de seguridad en el uso y selección de las contraseñas (ver sección 2.9).
- Utilizar contraseñas para proteger el acceso a la configuración de hardware.
- Configurar los servidores de manera segura. En este particular se pueden realizar las siguientes acciones:
  - Desactivar servicios y cuentas que no vayan a ser utilizadas.
  - Instalar los últimos parches de seguridad y actualizaciones publicadas por el fabricante. Convendría comprobar su correcto funcionamiento en otra máquina de pruebas antes de su uso en la máquina de producción.
  - Utilizar sólo los protocolos y servicios necesarios.
  - Activar los registros de actividades de los servidores (*logs*).
  - Disponer de una copia de seguridad completa del sistema operativo de cada servidor tras una configuración correcta.
  - Instalar herramientas que permitan comprobar la integridad de los archivos del sistema.

- Modificar el mensaje de inicio de sesión para evitar que no se pueda mostrar información sobre la configuración y recursos del sistema a un posible atacante.
- Llevar un control de registro y eliminación de los usuarios con sus respectivos roles y niveles de acceso a los activos de la institución
- Eliminar o bloquear inmediatamente los privilegios de acceso de los usuarios que han cambiado de área, departamento o han dejado la institución.

## 2.18. Seguridad física en los puestos de trabajo

En el área de seguridad física referida a los puestos de trabajo se pueden seguir las siguientes recomendaciones:

- De acuerdo a la información que se maneje se determinará la ubicación y seguridad física de los puestos de trabajo. Se recomienda que los puestos de trabajo deben estar ubicados en locales cerrados, utilizando perímetros de seguridad.
- Los equipos deben contar con fuentes o suministros de poder (*UPS*), para regular la corriente y proporcionar energía eléctrica continua. Un pico de tensión alta puede ocasionar que se dañe algún componente eléctrico de la computadora, o los pequeños y repetidos picos de voltajes pueden acortar la vida útil de sus componentes.
- Los equipos deben estar ubicados en un ambiente de trabajo adecuado (temperatura, humedad, polvo, según las características de las computadoras).
- Las ubicación de los equipos y el cableado deben ser colocados de tal manera que se evite golpes u otros hechos que puedan acarrear su daño o alteración. Los cables no pueden ser pisados ni cortados, ni se les debe colocar otros objetos encima o contra ellos.
- Durante la permanencia en el puesto se debe tener cuidado al consumir alimentos o ingerir líquidos.
- Contar con planes de mantenimiento de los equipos de los puestos de trabajos, en concordancia con las especificaciones de valores y servicios recomendados por el proveedor de los equipos. De esta manera se pueda alargar su la vida útil y se pueden detectar a tiempo fallas graves.

## 2.19. Seguridad física en los centros de datos

Para establecer la seguridad física se deben tener en consideración varios aspectos (físico, lógico y ambiental) que permitirán una configuración apropiada y segura para el centro de datos. En esta área por lo general se encuentra un alto porcentaje de los activos de información de la institución. En él se concentran y se procesan todos los recursos lógicos con que opera la institución. Para configurar un centro de datos confiable y seguro se debe considerar:

### 2.19.1. Servicios que prestan o prestarán los centros de datos

- Tipos de servicios a prestar tanto a los usuarios internos como externos.
- Cantidad de usuarios que ingresan y permanecen en el centro.
- Tipo de usuarios que se beneficiarán de los servicios prestados.

- Estimación de crecimiento: incluir nuevos servicios internos, externos que requieran la instalación de nuevos equipos computación.
- Registrar las características y especificaciones técnicas de los equipos.

Con esta información se pueden establecer las relaciones con la capacidad de procesamiento, cantidad de equipos computacionales requerido, espacio físico y acondicionamiento del espacio (aire acondicionado, capacidad de la planta eléctrica, entre otros).

### **2.19.2. Ubicación y condición física de los centros de datos**

La selección de la ubicación de un centro de datos, es un factor determinante en su correcto funcionamiento, puesto que de esto depende la mayor protección y seguridad de una de las áreas más importantes de cualquier institución.

Para la ubicación del centro de datos se recomienda que:

- Se encuentre alejado de instalaciones eléctricas como radares, microondas, u otro equipo que genere ondas electromagnéticas, para que no influyan en el funcionamiento de los equipos de computación del centro de datos.
- Se encuentre lejos de estaciones de materiales volátiles, estaciones de servicio (bombas de gasolina), porque representan peligros por incidentes intencionados o fortuitos.
- Se encuentren en lugares no desolados o desprotegidos.

Entre los factores inherentes a la localidad se debe que considerar:

- Que el terreno donde se encuentra ubicado no presente problemas de hundimiento.
- Que no existan condiciones climatológicas adversas: áreas de constantes lluvias y descargas eléctricas, altas temperaturas, u otra condición similar.
- Que el centro de datos no esté ubicado en un área con constantes actividades sísmicas.
- Que el centro de datos no esté ubicado en áreas propensas a inundaciones.

Además se debe contar con todos los servicios que requiere el centro de datos para comunicación tales como:

- Líneas telefónicas.
- Instalaciones eléctricas.
- Antenas de comunicación.

### **2.19.3. Especificaciones técnicas de los centros de datos**

Con respecto a las especificaciones técnicas se debe considerar:

- Espacios amplios disponibles por la organización con todos los servicios que requiere el centro de datos.
- El acceso a los equipos de computación y del personal al centro de datos debe ser lo más cómodo y seguro posible para evitar que se presenten incidentes, como por ejemplo en los traslados de los equipos de computación desde y hacia el centro de datos.
- Buen diseño de las instalaciones de suministro eléctrico, que garantice el suministro y la disponibilidad de la energía eléctrica estable, y además sea independiente del resto de las instalaciones del edificio de la institución.

Al diseñar un centro de datos se debe evaluar el suministro eléctrico, ya que si no se efectúa un buen cálculo sobre la carga que se va a utilizar, podría ocasionar serios problemas al utilizar los equipos.

Se requiere de la disposición de planta generadora de corriente para evitar la paralización de las actividades del centro de datos en los períodos de corte de energía eléctrica. Las características de las plantas eléctricas y su instalación estará en función a las necesidades eléctricas del centro de datos.

Contar con sistemas de puesta a tierra, que permitan absorber las descargas eléctricas. Por último, contar con fuentes o suministro de poder (*UPS*) para proteger a los equipos electrónicos por fluctuaciones de poder.

- Se debe contar con un acondicionamiento térmico del local que controle la humedad y la temperatura requeridas por los equipos computacionales del centro de datos.
- Instalación de pisos falsos, para evitar que las descargas eléctricas afecten a los equipos por su característica conductiva, y para una óptima distribución de cableado, canaletas, aire acondicionado.
- Se debe considerar la resistencia del piso falso que soporte el peso de los equipos de computación y personal que se encuentran en el centro de datos.
- Se debe preservar las condiciones térmicas del local de los centros de datos y para evitar la entrada de cualquier sustancia extraña que pueda generar algún incidente.
- Para las paredes y techos de los centros de datos se recomienda usar pinturas plásticas lavables para ser limpiados fácilmente y evitar la erosión.
- La altura del techo debe estar entre los 2,70m y 3,30m para permitir la movilidad del aire dentro del centro de datos.
- Se debe contar con ductos lisos y sin desprendimiento de partículas con el paso del aire que pudiera afectar a los equipos de computación
- El cableado del centro de datos se recomienda que esté dispuesto por debajo del piso falso, ubicado de forma separada en función al tipo de cable (de alto voltaje, de bajo voltaje, de telecomunicación, y los de señales para dispositivos de detección de fuego).
- Evitar conectar múltiples dispositivos en el mismo toma corriente para evitar sobrecargas en los circuitos eléctricos del centro de datos.

#### **2.19.4. Control de acceso físico a los centros de datos**

Los sistemas de control de acceso deben ser flexibles y confiables para controlar, supervisar, registrar y verificar los datos de acceso para permitir el acceso del personal autorizado para ingresar a las instalaciones o áreas restringidas de la institución. Los sistemas de control de acceso involucran al personal de seguridad, a la política de seguridad, al hardware y el software.

Se recomienda tomar en cuenta lo siguiente:

- Identificar el personal que entra y sale del centro de datos.
- Durante la noche, el fin de semana, los descansos o cambios de turnos el control debe ser tan estricto como en el horario normal.
- Identificar, controlar y vigilar las actividades que realizan las terceras personas durante su estadía en el centro de datos. Entre las personas que se consideran como terceras personas están los visitantes, personal de limpieza, personal de mantenimiento de los diferentes equipos.
- Instalación de Torniquetes.

- Utilizar cerraduras electromagnéticas.
- Utilizar circuitos cerrados de televisión.
- Utilizar detectores de movimiento.
- Utilizar tarjetas de identificación o cualquier otro mecanismo de por lo menos Nivel 2<sup>4</sup>.
- Utilizar control de aperturas de puertas.
- Utilizar control de acceso mediante sistemas electrónicos con tarjetas de proximidad.

#### **2.19.5. Sistema de aire acondicionado**

Los equipos modernos de computación generan grandes cantidades de calor, es por ello que se debe contar con un sistema de aire acondicionado para mantener una temperatura o clima adecuado que permita que los equipos funcionen bien. En este sentido, se tiene que considerar lo siguiente:

- Considerar los riesgos que representa los aires acondicionado, el mal funcionamiento ocasiona que los equipos sean apagados, se pueden producir incendios e inundaciones.
- El aire acondicionado debe ser exclusivo para el centro de datos por las condiciones especiales que se requieren.
- Se debe contar con aire acondicionado de respaldo, en el caso que el principal presente problemas. Con esto se evita que se tengan que apagar los equipos computacionales.
- Habilitar dispositivos con controles y alarmas que permitan el ajuste de temperatura y humedad a los niveles recomendados de operación de los equipos de computación.
- Tener los controles y las alarmas de temperatura y humedad que permitan la detección y la acción oportuna de corrección de los niveles de temperatura y humedad sin afectar los equipos de computación del centro de datos.
- Tener la suficiente capacidad de los equipos de aire acondicionado en función de las necesidades de los equipos instalados en el centro de datos y su posible tasa de crecimiento.

#### **2.19.6. Protección, detección y extinción de incendios**

Para evitar los incendios se debe tener en cuenta las siguientes condiciones:

- Los materiales de las paredes y de los techos deben ser resistentes al fuego.
- Se debe incorporar canales aislantes en los espacios físicos.
- Se debe contar con un sistema de drenaje en el piso firme.
- Se debe contar con detectores de fuego alejado del aire acondicionado.
- Las alarmas de fuego deben estar conectadas al sistema de detección temprana de humo.
- Disponer de equipos contra fuego como extintores.

<sup>4</sup>El Nivel 2 indica que el usuario autorizado para ante un sistema de control debe presentar algo que sabe (contraseña) y algo que tiene (tarjeta)



## 2.20. Especificación de las Políticas de seguridad de la información en los centros de datos

Para especificar las políticas de seguridad de los sistemas informáticos para el personal de la organización se deben contemplar los siguientes aspectos:

- Los procedimientos para la creación de nuevas cuentas críticas.
- Los niveles de acceso físico y lógico de los recursos computacionales, para establecer quiénes están autorizados para realizar determinadas actividades y operaciones; a qué datos, aplicaciones y servicios, desde qué equipo computacional puede acceder, quiénes pueden acceder al centro de datos.
- Los procedimientos para eliminar o bloquear las cuentas y los posibles escenarios que puedan incurrir en esta medida.
- El personal que delegará la responsabilidad del control de: usuarios, claves, entre otros, en los momentos cuando no esté el responsable principal.
- Las políticas de respaldo y recuperación ante incidentes para garantizar el continuo funcionamiento de los sistemas de la institución.
- Los procedimientos para respaldar o eliminar información o sistemas de los equipos de computación (ver sección 2.21).
- Las posibles violaciones y consecuencias derivadas del incumplimiento de las políticas de seguridad.
- Las sanciones a los responsables por la violación de las políticas de seguridad.
- Clasificar la información e identificar los activos de información.

Entre las actividades y responsabilidades que se deben delegar y considerar para las políticas de seguridad se tienen:

- Mantener en óptimas condiciones el funcionamiento de la red para garantizar su disponibilidad.
- Revisar periódicamente el estado físico del cableado horizontal y vertical de la red de la institución.
- Realizar periódicamente mantenimientos preventivos y correctivos a los equipos de telecomunicaciones. Se recomienda que el mantenimiento se realice semestral, además deberá ser registrado en bitácoras.
- Supervisar y mantener adecuadamente las instalaciones de la infraestructura de red.
- Administrar y operar los servidores de la red interna de la organización.
- La red interna no será instrumento de experimentos que pongan en riesgo la integridad de la información.
- Configurar y supervisar los equipos de comunicaciones.
- Construir un mapa de red y actualizarlo ante cambios.
- Asegurar las contraseñas críticas como: administrador (*root*), aplicaciones como cortafuegos, servidores, entre otros.
- Ubicar los equipos en salas (centro de datos) con acceso restringido y medidas de seguridad física, utilizando estándares o certificaciones.

## 2.21. Políticas de respaldo y recuperación

Es imprescindible contar con políticas de respaldo y recuperación para garantizar el continuo funcionamiento de los sistemas de la organización. La recuperación de los sistemas posterior a la interrupción de índole natural o accidental como incendios, mal funcionamiento de los sistemas, errores humanos, entre otros, resulta necesario, requiriendo de una acción rápida para asegurar la disponibilidad.

Con el objetivo de garantizar la disponibilidad de los servicios es necesario contar con planes de contingencias ante desastres y para esto se requiere aplicar las políticas de respaldo y recuperación:

### 2.21.1. Normas para las políticas de respaldo y recuperación

Entre las normas a aplicar para el respaldo y la recuperación se pueden mencionar las siguientes:

- Las copias de respaldo de datos y archivos de servidores deben ser realizadas y supervisadas por personal debidamente autorizado.
- Planificar las copias de respaldo que se deben realizar en función del volumen y del tipo de información generada por los sistemas informáticos.
- Todas las copias de respaldo y medios de almacenamiento utilizados deben estar bien identificadas con información tal como: a qué equipo de computación pertenece, contenido de la copia de respaldo, fecha y hora de ejecución del respaldo, cronogramas de ejecución del respaldo, tipo de respaldo (completos, incrementales, diferenciales), cuantos medios de almacenamiento fueron utilizados, identificación de la persona que ejecuta el respaldo, ubicación asignada para su almacenamiento, personas responsables del almacenamiento.
- Establecer los sistemas técnicos que se van a emplear para garantizar la privacidad e integridad de los datos que se almacenen.
- Contar con un lugar de resguardo para los respaldos, físicamente seguro y que posea controles de acceso.
- Generar en un tiempo determinado dos copias de los respaldos, unas de esas copias, se debe resguardar en otro sitio fuera del edificio, este sitio debe igualmente cumplir con determinados características de seguridad al sitio principal. Además, el acceso y traslado de las copias deben ser realizados por personal debidamente identificado y autorizado para ejecutar el procedimiento.
- Efectuar las pruebas de recuperación en un tiempo determinado y definido para verificar el estado de los soportes y el correcto funcionamiento de las copias de respaldo.
- Para los casos de aplicaciones críticas se recomienda implementar técnicas de sincronización automática, por hardware y software de forma que si la aplicación principal deja de funcionar la otra aplicación espejo tome el control inmediatamente o en un tiempo mínimo requerido para su ejecución, este procedimiento es llamado redundancia.

## 2.22. Gestión de incidentes de seguridad

Un incidente de seguridad es cualquier evento que pueda ocasionar la interrupción o degradación de los servicios de los sistemas. Estos incidentes pueden ser ocasionados de forma intencional, por error de aplicación de las políticas y procedimientos de seguridad, de desastre natural o del entorno como las inundaciones, incendios, tormentas, fallos eléctricos entre otros.

Entre las actividades y tareas que se deben tener en cuenta están las siguientes:

### 2.22.1. Antes del incidente de seguridad:

- Se debe contar con un equipo de personas para la solución del incidente, que será el equipo encargado de activar y coordinar el plan de contingencia. Este equipo debe estar constituido por personas que cuenten con la experiencia y formación necesaria que pueda dar respuesta ante cualquier incidente de seguridad. Debe existir una lista de números telefónicos y direcciones actualizadas para la ubicación de las personas que conforman este equipo en el momento que ocurra un incidente de seguridad.
- Identificación de las áreas críticas y operativas de la institución. Para la misma se consideran los servicios, equipos, aplicaciones, infraestructura, existentes dentro de la institución.
- Hacer inventario de los equipos y servicios. Se requiere de una descripción detallada de la ubicación, configuración, características, y procedimientos de respaldo y recuperación.
- Considerar los posibles escenarios de incidentes de seguridad que puedan ocurrir en cada área crítica identificada. Los mismos deben estar bien documentados.
- Describir clara y detalladamente los planes de contingencia de todos los posibles escenarios de incidentes de seguridad, donde se indiquen los procedimientos de actuación necesarias para la restauración rápida y eficiente.
- Efectuar reuniones al menos una vez al año para la revisión del plan de contingencia, en función de evaluar y actualizar las condiciones del sistema informático.
- Detectar incidentes de seguridad. La institución debe prestar especial atención a los indicadores de incidentes de seguridad, como una actividad a contemplar dentro del plan de respuesta a incidentes. Entre estos indicadores se tienen:
  - Cambio de configuración de los equipos de red con acciones tales como la activación de nuevos servicios, la verificación de puertos abiertos no autorizados, entre otros.
  - Caída en el rendimiento de la red o algún servidor debido a un incremento inusual del tráfico de datos.
  - Caída o mal funcionamiento de servidores como: reinicio inesperado, fallos en algún servicio.
  - Existencia de herramientas no autorizadas en el sistema.
  - Aparición de nuevas cuentas de usuarios o registro de actividades inusuales en algunas cuentas como: conexión de usuarios en horarios poco usuales.

### 2.22.2. Durante el incidente de seguridad:

Cuando ya se tiene certeza del incidente a través de datos que lo confirman, se debe actuar de forma oportuna y diligente. En esta fase del incidente, se pueden seguir las siguientes recomendaciones:

- Analizar el incidente de seguridad con el objetivo de determinar el alcance (aplicaciones afectadas, información confidencial comprometida, equipos afectados, entre otras), para ayudar al equipo de solución a tomar soluciones adecuadas y permitan establecer prioridades en las actividades que se deben llevar a cabo.
- Poner en marcha el plan de contingencia de acuerdo al incidente de seguridad presentado.
- Contener, erradicar y recuperar. El equipo de solución debe llevar a cabo una rápida actuación para evitar que el incidente de seguridad vaya a tener mayores consecuencias a la institución.

### 2.22.3. Después del incidente de seguridad:

Después de la ocurrencia del incidente de seguridad, es decir, cuando ya se encuentre en pleno funcionamiento el sistema informático, se recomiendan ejecutar las siguientes actividades:

- Análisis y revisión del incidente. Causas del incidente, valoración inicial de los daños y sus posibles consecuencias
- Una completa documentación del incidente facilitará su posterior estudio. Entre los aspectos que debe tener reflejado la documentación se tiene:
  - Descripción del tipo de incidente: ataque a la seguridad, procedimientos de seguridad, desastres naturales.
  - Hechos registrados (como por ejemplo: logs de los equipos).
  - Daños producidos en los sistemas informáticos.
  - Decisiones y actuación del equipo de respuesta.
  - Lista de evidencias obtenidas durante el análisis y la investigación
  - Posibles actuaciones y recomendaciones para reforzar la seguridad y evitar incidentes similares en un futuro.
- Actualización de los planes de contingencia de ser necesario.
- Realizar un seguimiento o supervisión del sistema en búsqueda de vulnerabilidades omitidos o recreados luego de la recuperación de los sistemas.
- Aplicación de *informática forense*. Esta proporciona los principios y técnicas que facilitan la investigación de los eventos informáticos ocurridos, mediante la identificación, captura, reconstrucción y análisis de evidencias. Entre las etapas para el análisis forense se tienen:
  - Identificación y captura de las evidencias.
  - Preservación de las evidencias.
  - Análisis de la información obtenida.
  - Elaboración de informe con las conclusiones del análisis forense.

### 2.23. Plan de recuperación ante desastres

El "Plan de recuperación ante desastre"<sup>es</sup> un elemento que contribuye a la práctica efectiva de medidas de seguridad para garantizar una adecuada recuperación de la operatividad mínima luego de una contingencia, en donde se vean afectados los procesos y recursos informáticos que funcionen en la organización.

Los desastres pueden ser naturales o accidentales como incendios, inundaciones, corte en el suministro de energía eléctrica, entre otros eventos no planificados. El plan de recuperación ante desastres debe especificar los objetivos y prioridades a tener en cuenta por las instituciones. Es necesario contemplar la disponibilidad de los recursos y medios adecuados que permitan restaurar el funcionamiento de los sistemas informáticos de la institución, así como de la recuperación de los datos, aplicaciones y servicios básicos. La práctica de recuperación que se acostumbra a realizar es:

- Disponibilidad de un centro alternativo para la ubicación de los principales recursos informáticos (servidores, aplicaciones, bases de datos, entre otros). Este centro debe contar con las mismas medidas de seguridad que las instalaciones principales de la institución.
- Existencia de políticas de respaldo y recuperación.

- Herramientas para llevar a cabo una replicación de los documentos y las bases de datos.
- Detección y respuesta al desastre en el centro principal, adoptando las medidas de contención previstas dependiendo del tipo de desastre: incendio, inundación, explosión, entre otros.
- Traslado de las actividades a un centro alternativo, junto con el personal necesario para la puesta en marcha de los servicios, equipos informáticos, copias de seguridad más recientes y con las medidas de seguridad que correspondan, entre otros.

## REFERENCIAS

---

1. Vicente Aceituno Canal. *Seguridad de la información*. Noriega Editores, México D.F., México, 2003.
2. R. Nichols and P. C. Lekkas. *Seguridad para comunicaciones inalámbricas*. McGraw-Hill, Mexico, 2003.
3. Bruce Schneier. Choosing secure passwords. <http://boingboing.net/2014/02/25/choosing-a-secure-password.html>, 2014.



# SISTEMAS ANÓNIMOS

---

RODOLFO SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

Tal como se plantea en [6], se puede indicar que la privacidad se trata de una necesidad natural e inherente de los seres humanos, la cual responde a la libre voluntariedad de escoger con quiénes cada uno se quiere relacionar, o se trata de elegir la información que se desea sea conocida en esa relación. Esto se deriva de la intimidad humana, como espacio de crecimiento y desarrollo personal, y de protección del ámbito privado personal, en el que la personas se pueden comportar y expresar de forma libre y sin temor o reticencia ante la presencia o intervención indeseada de terceras personas. Esto implica que se puede representar como la contraparte al ámbito público, el cual es un espacio en el que las interacciones sociales son constantes y necesarias, y se encuentran influenciadas y limitadas por normas y regulaciones jurídicas, sociales, culturales, religiosas, entre otras, las cuales determinan en todo momento las conductas a seguir y por lo general se establecen sanciones en los casos de violación de alguno de esos preceptos.

La privacidad también se puede pensar como una necesidad que se ha adquirido en el transcurso del tiempo, debido principalmente a factores como:

1. El reconocimiento y protección de los derechos humanos fundamentales en el mundo. Históricamente, se observa que desde tiempos antiguos se manejaba la noción de un espacio propio de cada persona, que

permitiera su crecimiento personal. Se penalizaban las violaciones a ese espacio, pero más por razones de seguridad pública y por relacionarlo a derechos patrimoniales.

2. Las discusiones acerca de un derecho a la intimidad, a la vida privada, a la privacidad se presentan con mayor fuerza luego del surgimiento de la prensa escrita, ya que es el medio que empieza a posibilitar la transmisión de una misma información a gran número de personas.
3. Se ha planteado como una necesidad que se ha visto influenciada y potenciada por la aparición, crecimiento y masificación de las TIC (computadores personales, la Internet, televisión, telefonía fija y móvil, etc), ya que éstas permiten la fácil divulgación de gran cantidad de información en poco tiempo.

Sin embargo, no es necesario apelar a los artículos de la carta sobre los Derechos Humanos establecida por la Organización de las Naciones Unidas para darse cuenta que cada una de las personas que habitan este planeta tiene el derecho de decidir sobre el destino de su información privada. Esto incluye no sólo decidir quién, cómo, dónde y cuándo terceras partes puedan tener acceso a sus datos en general, sino que se debe prestar una particular atención a los que están relacionados con la identidad, el perfil social, cultural, personal, etc.

Tanto en las organizaciones privadas, como en las públicas, y a nivel individual, la protección de la información no sólo debe incluir los aspectos típicamente enmarcados dentro de la integridad, confidencialidad y disponibilidad de los datos, sino que debe ampliarse al resguardo de la privacidad donde, entre otros, se procura evitar que se revele la identidad de las partes comunicantes. Se han desarrollado varias estrategias, mecanismos, técnicas y sistemas que tienen ésto como objetivo, y que pueden enmarcarse en lo que se denomina las tecnologías que mejoran la privacidad (se conoce en inglés como *Privacy Enhancing Technologies o PET*).

Este tipo de tecnologías han tenido sus frutos en escenarios de diversa índole, que van desde aplicaciones militares, donde se procura evitar que el adversario pueda descubrir las conexiones estratégicas, pasando por aplicaciones científicas/comerciales, que evitan revelar información sobre las comunicaciones hechas entre socios científico/comerciales, hasta las aplicaciones de particulares que le ayudan a mantener en privado sus datos personales: los referentes a su salud, su estado financiero, sus preferencias de consumo, etc. Uno de los puntos críticos de la privacidad es el encubrimiento de la identidad de las partes comunicantes, es decir, es la procura de que las comunicaciones sean anónimas: anonimato.

Cada una de las técnicas y mecanismos utilizados tienen sus ventajas y desventajas en cuanto al perfil de ataque considerado. Es decir, dependiendo del tipo de atacante que se considere, cada una de éstas posee un conjunto de fortalezas y debilidades asociadas. Adicional al perfil del atacante, se debe incluir su radio de acción, esto quiere decir, que se debe considerar su capacidad para manejar ciertos volúmenes de usuarios, su heterogeneidad, su distribución y localización.

Además se debe considerar el tipo de comunicación anónima que se desea o necesita entablar: mensajería instantánea, correos electrónicos, servicios web, etc.

En las siguientes secciones se presentan algunas técnicas, sistemas y mecanismos que se orientan a proporcionar privacidad basándose en el anonimato.

### 3.1. Técnicas para proporcionar privacidad

Tal como se menciona en [2] las personas en general utilizan la Internet para poder comunicarse, para el envío de correo electrónico, para la investigación en diversas áreas de interés, para la interacción con distintos organismos públicos o privados, etc. Al mismo tiempo, gran cantidad de estos organismos públicos y privados en distintas regiones del planeta buscan maximizar la interacción electrónica en todos los niveles entre los usuarios y sus centros tecnológicos, intercambiando información a través del uso de bases de datos controladas por ellos mismos, buscando utilizar herramientas de la informática para tener el control de la información concerniente a innumerables aspectos relacionados a los individuos, tales como las preferencias en sus consumos diarios, la interacción con su alrededor, sus estilos de vida, sus opiniones, sus preferencias, y todo esto en niveles que en gran medida son desconocidos por los mismos usuarios. En respuesta a lo anterior, y procurando minimizar este tipo de control, se han propuestos diferentes mecanismos y sistemas que buscan reforzar o



mejorar la privacidad (Privacy Enhancing Technologies) del individuo (visto en un contexto amplio, es decir, pudiéndose considerar como individuo a un conjunto de personas, e incluso a organizaciones completas).

Este tipo de tecnologías pueden asistir a los organismos en su cumplimiento de los principios de protección de la privacidad establecidos en la declaración universal de los derechos humanos [3], dándole a los usuarios mayor poder para controlar su información, pudiendo éstos decidir cómo y cuándo puede ser utilizada por terceras partes. Existen sistemas tales como los navegadores web anónimos y servicios especiales de correo electrónico que le permiten comunicarse sin necesidad de revelar su verdadera identidad. Los sistemas para el manejo de la identidad potencialmente le permiten a los individuos acceder a los servicios y recursos sin tener que proveer información sobre ellos. Esto implica involucrar a una o varias organizaciones sobre las cuales se deba tener cierto grado de confianza”, que puedan verificar la identidad de los usuarios, y además puedan generar cierto tipo de certificación electrónica que no contenga información sobre la identidad, pero que permita acceder a los recursos y servicios ofrecidos por terceras partes.

Las tecnologías que mejoran o refuerzan la privacidad no son sólo aquellas destinadas a proveer un cierto grado de anonimato, sino que se extienden a la protección y mejora de la privacidad en general del individuo, incluyendo el cumplimiento de sus derechos sobre la protección de sus datos, en este sentido se pueden mencionar, como ejemplos de este tipo de tecnología, los siguientes:

- Los sistemas de acceso biométrico cifrado, que permiten el uso de las huellas dactilares como mecanismo para autenticar la identidad de un individuo sin necesidad de retener su huella dactilar actual.
- Los accesos seguros a los datos personales de los usuarios en línea.
- Programas que permiten a los navegadores detectar automáticamente las políticas de privacidad de los sitios web y permitan compararlas con las preferencias expresadas por los usuarios.
- Sistemas de alertas y avisos que son anexados a la misma información y que previenen su uso en caso del no cumplimiento de las políticas de privacidad.

### 3.1.1. Bases del Anonimato

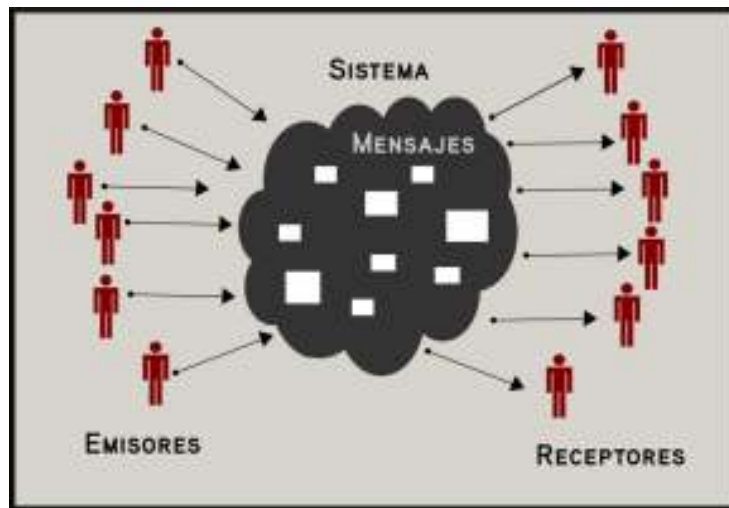
En la sección 1.2.4 se habla sobre los conceptos y bases del anonimato, y para comprenderlo de manera general es conveniente utilizar la configuración de un sistema general de comunicación tradicionalmente compuesto por un emisor, un receptor, quienes utilizan una red de comunicación para transmitir un mensaje. En la figura 3.1 se muestra el diagrama general de este modelo.

Este sistema está delimitado por los componentes antes mencionados, por lo cual los involucrados que se encuentren fuera de esta delimitación, en cada uno de los casos que se describen se consideran participantes externos.

Cada uno de los casos de estudio presentados serán considerados desde la perspectiva del atacante, quien puede monitorear las comunicaciones, estudiar sus patrones, e incluso puede hacerle cambios al manipular su contenido. El atacante puede estar dentro del sistema o puede ser uno de los participantes externos.

En todas las definiciones de los términos relacionados con las tecnologías asociadas a la mejora o refuerzo de la privacidad, se considera un sujeto (subject) a una entidad (ente o ser) que tiene la posibilidad de actuar en el sistema, por ejemplo, un ser humano, una persona jurídica, un computador, etc.

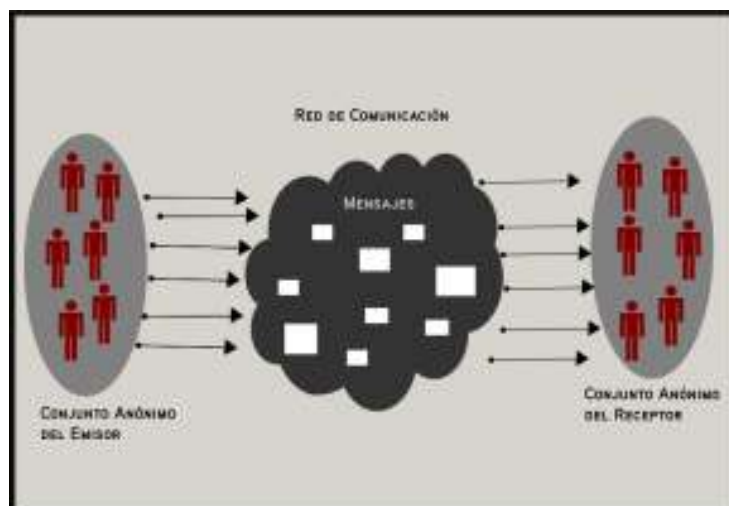
Como se mencionó en la sección 1.2.4.1 un sujeto es anónimo cuando no puede ser identificado dentro de un conjunto de sujetos, denominado el conjunto anónimo. Este conjunto está conformado por todos los posibles sujetos que pueden causar (o estar relacionados con) una acción. No ser identificado significa que ese sujeto no puede ser caracterizado de forma única o particular dentro de ese conjunto. Un sujeto actúa anónimamente cuando, desde el punto de vista del adversario, su acción no puede relacionarse con su identidad, dado que hay un conjunto de sujetos que podrían ser los causantes potenciales de la acción (y el adversario no puede distinguir a su verdadero causante). El anonimato debe permitirle a un sujeto utilizar un recurso o servicio sin revelar su identidad, esto implica que el anonimato por sí mismo no procura proteger la identidad de un usuario en un ámbito general, lo que pretende es evitar que otros usuarios o sujetos puedan determinar la identidad de un usuario cuando éste genera una acción u operación en particular.



**Figura 3.1** Configuración del Sistema General

Con respecto a las entidades que podrían generar una acción, el conjunto anónimo se conforma por los sujetos que pueden generar una acción en un instante de tiempo específico; desde el punto de vista de las direcciones o ubicaciones de las entidades, el conjunto anónimo está conformado por los sujetos que pueden estar relacionados a una ubicación o dirección. Lo anterior quiere decir que el anonimato se podría clasificar según las entidades involucradas o según la ubicación de las mismas.

De esta forma, para permitir el anonimato de un sujeto siempre tiene que existir un conjunto apropiado de sujetos que posean potencialmente los mismos atributos. Ser los emisores y los receptores de mensajes particulares son ejemplos de estos atributos. Un emisor de un mensaje puede ser anónimo sólo si constituye parte de un conjunto de emisores potenciales (con atributos similares), el cual es su conjunto anónimo, y puede ser un subconjunto de todos los sujetos a nivel global quienes pueden enviar un mensaje en un tiempo específico. Lo mismo aplica para los receptores de mensajes. Este esquema se representa en la figura 3.2. El conjunto anónimo es relativo al tiempo, es decir, puede variar según los cambios que se den en el sistema.



**Figura 3.2** Conjuntos Anónimos

Con lo anterior se especifica que existe un conjunto anónimo para el emisor de un mensaje, existe otro conjunto anónimo para el receptor de ese mensaje, y estos conjuntos pueden ser disjuntos, pueden solaparse o pueden ser el mismo conjunto.

Por otro lado el anonimato además de estar relacionado al conjunto anónimo y al tiempo en el que se está ejecutando la acción, también tiene relación al contexto donde se aplica, es decir, un sujeto puede ser anónimo en relación al contexto envío y recepción de correos electrónicos, pero puede no serlo en ese mismo instante de tiempo para el contexto interacción con una base de datos. Esto se debe a que según el contexto de estudio pueden existir distintos atributos que caractericen al conjunto anónimo, y por ende al anonimato del sujeto.

Como se mencionó el conjunto anónimo está directamente relacionado con el atacante, esto quiere decir, que el conjunto anónimo se delimita según el grado de conocimiento que posee el atacante. De esta forma, el fin último del anonimato es procurar que el atacante posea la misma información antes y después de su ataque.

Dado que el anonimato es dependiente del contexto, definido por sus atributos, las variaciones del mismo podrían cambiar los niveles de anonimato. Si se pretende diferenciar entre “niveles” de anonimato, es necesario poder cuantificarlo (medirlo) con el fin de poder hacer distinciones entre distintos sistemas anónimos.

### 3.1.2. Técnicas de Anonimato

Tal como se mencionó en el apartado anterior el anonimato de un sujeto es el estado de no ser identificable dentro de un conjunto de sujetos, denominado el conjunto anónimo. También se ha mencionado, ver [1], que el emisor de un mensaje puede ser anónimo sólo dentro de un conjunto de potenciales emisores, que corresponde al conjunto anónimo del emisor, el cual a su vez puede ser un subconjunto de todos los sujetos a nivel mundial quienes podrían enviar mensajes en determinados instantes de tiempo. Este tipo de anonimato es llamado anonimato del emisor. Lo mismo ocurre para el receptor, quien puede ser anónimo sólo dentro de un conjunto de receptores posibles, llamado el conjunto anónimo del receptor, y a este tipo de anonimato es llamado anonimato del receptor. Además hay un tercer tipo de anonimato, el de relación, el cual consiste en tener la propiedad de no poder relacionar quién se comunica con quién. La no relacionabilidad significa que dentro del sistema las distintas entidades, aquí denominadas ítems de interés o IDI (mensajes, emisores, receptores, etc.) no están ni más ni menos relacionadas con respecto a la información que se tenía antes de que el adversario ejecute un ataque (información a priori). En otras palabras, el anonimato del emisor/receptor puede ser definido como las propiedades de que un mensaje particular no pueda ser relacionado con ningún emisor/receptor, y que cualquier mensaje no pueda ser relacionado con ningún emisor/receptor en particular, entonces el anonimato de relación es la propiedad de no poder relacionar o determinar quién se comunica con quién.

El anonimato se fortalece mientras más grande sea su conjunto anónimo, y mientras más uniforme sea la distribución de probabilidad de la ejecución de las acciones por parte de los sujetos dentro del conjunto, es decir, el nivel de anonimato no sólo depende del tamaño del conjunto sino también de la probabilidad de que un sujeto en particular pueda generar cierta acción. De esta forma se puede definir el entorno de acción que acota las técnicas de anonimato para las comunicaciones: Colectar un conjunto apropiado de usuarios para que un usuario en particular pueda ser anónimo cuando se comunica con los demás.

Los sujetos no pueden tener el mismo nivel de anonimato contra todos los tipos de ataques posibles generados por participantes internos o externos. El conjunto de los posibles sujetos y la probabilidad de que ellos puedan causar una acción puede variar dependiendo del conocimiento del atacante. Se asume que desde el punto de vista del atacante, el nivel de anonimato sólo puede disminuir, es decir, se asume que el atacante no olvida la información que tiene y que ha logrado recolectar durante su observación e influencia sobre la comunicación en el sistema.

Para definir las diferentes técnicas de anonimato se utilizan los siguientes criterios:

- **Objetivo de la protección:** define cuál tipo de anonimato puede ser provisto (del emisor, del receptor, o de la relación).

- Nivel de seguridad: se debe definir cuál es el nivel de seguridad alcanzado por el objetivo de la protección (la seguridad desde la perspectiva de la teoría de la información o incondicional y la seguridad criptográfica/computacional con los supuestos asociados a mecanismos como los de clave pública).
- Modelo de atacante: contra qué tipo de atacantes protege el sistema (externos, participantes, proveedores de servicios).
- Modelo de confianza: en quién confía el usuario (en los proveedores de servicios, en los participantes externos, en otros usuarios, etc.).

### 3.1.2.1. *Redes de mezcla:*

Esta idea se describe en [1]. El método utiliza criptografía de clave pública y fue diseñado para que los sistemas de envío de correo electrónico proporcionaran anonimato del emisor, del receptor y de relación sin necesitar un servicio de confianza central (por ejemplo una autoridad certificadora). En general, los mezcladores o mixes pueden ser entendidos como una cadena de proxies seguidos uno detrás del otro. Se considera que el atacante puede observar todas las comunicaciones y puede controlar todos los mixes a excepción de uno.

#### **Topología Mix**

Este concepto funciona aun cuando se dispone de un solo mix, pero en este caso el usuario debe confiar en este mix. Típicamente hay más de un mix en la red organizados en forma de cadena. Existen diferentes métodos para organizar la cooperación dentro de la red. Uno de ellos puede ser que cada mix existe independientemente en la red y los participantes libremente deciden a través de cuál de ellos enrutarán sus mensajes. Así cada nodo puede comunicarse con el resto conformando lo que se denomina una topología de red mix o red de mezcla.

Otra posibilidad es utilizar una cadena de mixes predefinida. A esta cadena se le denomina mix en cascada. Además de los dos extremos antes mencionados, se pueden utilizar variaciones que resulten en diseños híbridos. Un análisis y comparación de ambas ideas se presenta en [9, 7].

En una red mix, el usuario puede decidir con cuáles mixes desea interactuar, proporcionando de esta manera un buen nivel de escalabilidad y flexibilidad. Además, debido a que los usuarios escogen aleatoriamente los mixes, un atacante no podrá determinar cuáles de ellos debería controlar para poder observar un mensaje enviado, para esto debería controlar gran parte de la red.

Por otro lado, un atacante sabe con exactitud cuáles mixes debe controlar en una red en cascada (mix en cascada). Este diseño es vulnerable a los ataques de denegación de servicio, ya que al detener un solo mix en la red, lograr detener todo el sistema.

Por otro lado en [9] exponen que la red mix (pero no la red en cascada) es vulnerable a ciertos tipos de atacantes con altos niveles de control, es decir, que controlan a todos los mixes a excepción de uno. Mencionan que este tipo de red es vulnerable a los ataques  $n - 1$ . Otra desventaja es que algunos mixes pueden que no sean casi utilizados (se subutilizan) y otros se sobrecarguen. Los objetivos de protección que se logran son el de anonimato del emisor, y el de relación.

La topología mix provee protección contra atacantes que pueden observar toda la red y que pueden controlar muchos mixes. Es susceptible a ataques de denegación de servicio y ataques  $n - 1$ . Desde el punto de vista de la confianza, se debe confiar en al menos un mix de la ruta seleccionada.

#### **Funcionalidad básica**

En este enfoque los usuarios o clientes no envían sus solicitudes directamente al servidor (o a otro destino), sino que las envía a nodos (enrutadores) intermedios denominados mix. Para poder ocultar la comunicación de los participantes, los mixes no envían instantáneamente los mensajes que reciben, en vez de esto, ellos almacenan varios mensajes de diferentes clientes por un tiempo definido, los transforman, y luego los reenvían simultáneamente a los servidores de destino o a otros mixes en la red. Un observador que puede ver todos los mensajes entrantes y salientes de un mismo mix no podrá determinar cuáles mensajes de entrada corresponden a cuáles mensajes de salida.

## Preprocesamiento

El preprocesamiento es la transformación de los mensajes. El objetivo principal de la transformación de los mensajes es evitar que un atacante pueda trazar un mensaje (descubrir su recorrido) a través de la comparación de los patrones de bits correspondientes a los mensajes que entran y salen de un mix. Para poder enviar un mensaje, el cliente primero lo debe preparar. Para esto, el primer paso que debe dar es escoger el camino por el cual se transmitirá el mensaje, este camino estará compuesto por los mixes que haya escogido, y debe incluir el orden específico de reenvíos antes de que llegue a su destino final. Para mejorar la seguridad del sistema, se recomienda utilizar más de un mix en cada camino. El siguiente paso, es utilizar las claves públicas de los mixes escogidos para cifrar el mensaje, en el orden inverso en el que fueron escogidos, es decir, el mensaje se cifra primero con la clave pública del último mix, luego con la del penúltimo, y así sucesivamente hasta cifrar por ultima vez con la clave pública del primer mix en el camino seleccionado. Cada vez que se cifra se construye una capa, y se incluye la dirección del siguiente nodo (ya sea el destino final u otro mix). Así cuando el primer mix obtiene el mensaje preparado, lo descifra con su clave privada, y obtiene la dirección del siguiente nodo al que debe reenviarle el resto del contenido que quedó después de su descifrado.

Este esquema puede ser descrito de la siguiente manera:

$A_1, \dots, A_n$  pueden ser la secuencia de las direcciones y  $c_1, \dots, c_n$  la secuencia de la claves de cifrado conocidas públicamente y pertenecientes a la secuencia  $Mix_1, \dots, Mix_n$  escogidos por el emisor. Incluso  $c_1$  puede ser una clave secreta en un sistema de cifrado simétrico.  $A_{n+1}$  puede ser la dirección del receptor o del destino final del mensaje, al cual se le denomina, por simplificación,  $Mix_{n+1}$ , y  $c_{n+1}$  sería su clave de cifrado.  $z_1, \dots, z_n$  puede ser una secuencia de bits aleatorias. El emisor crea los mensajes  $N_i$  que son recibidos por el  $Mix_i$ , y en la base del mensaje  $N$  es lo que el receptor final debe recibir ( $Mix_{n+1}$ ) supuestamente:

$$N_{n+1} = c_{n+1}(N) \quad (3.1)$$

$$N_i = c_i(z_i, A_{i+1}, N_{i+1}) \text{ para } i = n, \dots, 1 \quad (3.2)$$

El emisor le envía  $N_1$  al  $Mix_1$ . Después que se decodifica, cada mix recibe la dirección del siguiente mix y el mensaje que está destinado a ese siguiente mix. Debido a las implementaciones de los sistemas de clave pública o asimétrica se necesitan las cadenas aleatorias de bits. Para asegurar que un atacante no pueda trazar un mensaje (seguir su trayectoria) a través de un mix, es necesario que todos los pares de entrada-salida de los mensajes no tengan características que permitan identificarlos, por ejemplo, el tamaño de los mismos. Una solución a esto es establecer tamaños fijos para los mensajes, y cuando los mensajes tengan un tamaño inferior al fijado, se deberán rellenar con información falsa, y cuando lo superan se deberán fragmentar en varias piezas.

## Reordenamiento

Mezclas por grupos (pool) o mezclas por lotes (batch): Cuando un mix opera en modo "por lotes." "batch", éste recolecta un número fijo  $n$  de mensajes, cifrándolos y reordenándolos antes de reenviarlos a todos en un solo envío. En contraste, un mix que opera en modo "por grupos" o "pool" tiene siempre un número  $n$  de mensajes almacenados en su memoria temporal o "buffer" denominado "pool". Si un nuevo mensaje llega al mix, entonces se escoge aleatoriamente y se reenvía uno de los mensajes almacenados. El número  $n$  representa al tamaño del "pool".

## Prueba de reenvío

Uno de los tipos de ataques más frecuentes es el denominado ataque de reenvíos. Un atacante podrá copiar un mensaje que desea monitorear y enviarle una o varias copias de éste al mix. Estas copias del mensaje podrían tomar el mismo camino en la red que el mensaje original, dado que los algoritmos de envío y descifrado trabajan determinísticamente. Así puede ser encontrado un patrón característico del mensaje sólo con observar la red. Con el fin de evitar este tipo de ataque, las copias de los mensajes deben ser identificadas y eliminadas a través de un filtro. Una posibilidad para identificar los mensajes inválidos es a través del uso de estampas de

tiempo. Cuando un mix obtiene un mensaje, también obtiene una etiqueta que le informa la franja de tiempo durante la cual el mensaje es válido. Si el mensaje llega muy tarde (después de lo que la franja de tiempo le indica), el mix niega el reenvío del mensaje. Otra posibilidad es que el mix almacene una copia de los mensajes que ya haya enviado, y así los mensajes nuevos que lleguen pueden ser comparados con esta base de datos. Por razones de seguridad y rendimiento, es conveniente restringir el tamaño de esta base de datos. Los mensajes deberían ser almacenados por un corto período de tiempo antes de que se borren.

### Tráfico de relleno o dummy

Aun cuando ninguna información está siendo transmitida, es posible enviar información falsa o de relleno en la red. Esto tendría el mismo efecto de no enviar ningún mensaje, pero un observador (atacante) no podría distinguir entre los mensajes reales de los que se envían como relleno. El envío de este tipo de mensajes de relleno es denominado tráfico dummy. Con respecto a la idea de los mixes, un mix podrá aleatoriamente enviar tráfico dummy a otro en la red. Este mecanismo también beneficiaría a los mix que trabajan en el modo batch, ya que normalmente estos mixes tienen que esperar hasta que un número predefinido de mensajes hayan llegado antes de que todos los mensajes sean reenviados simultáneamente, y evitaría los posibles retrasos que podrían ocurrir cuando no hayan envíos suficientes de mensajes al mix, y éste puede hacer su respectivo reenvío. Es decir, el tráfico dummy evitaría estos retrasos, ya que si no hay suficientes mensajes reales enviados, el número de mensajes necesarios para hacer el reenvío se pudiese alcanzar con los mensajes de relleno.

### Anonimato del receptor (Direcciones de retorno no trazables)

El hecho de permitir que un receptor pueda permanecer anónimo se le caracteriza por tener una dirección de retorno que no pueda ser registrada o trazada por un atacante. Esta dirección de retorno es un mensaje especial que tiene que ser creado por el receptor y tiene que ser utilizado por el emisor para el envío del mensaje al receptor anónimo. La idea de base de este tipo de direccionamiento es que el receptor, y no el emisor, define sobre cuáles mixes y el orden en el que van a ser utilizados para la entrega de cierto mensaje de respuesta. La dirección de retorno preparada por el receptor contiene una clave simétrica para cada mix en el camino que éste utilizará para cifrar el mensaje enviado por el emisor. Finalmente, el receptor recibirá un mensaje cifrado múltiples veces con claves simétricas como él mismo especificó. Dado que el receptor conoce todas las claves simétricas, para poder desarrollar esta técnica, éste puede descifrar el mensaje. Dado que la claves simétricas son desconocidas por el emisor y la codificación del mensaje cambia en cada uno de los mixes (debido al cifrado), el emisor no puede trazar el mensaje hacia el receptor.

Este esquema se explica de la siguiente forma:  $A_1, \dots, A_m$  pueden ser la secuencia de las direcciones y  $c_1, \dots, c_m$  pueden ser la secuencia de las claves públicas conocidas de la secuencia de mixes  $Mix_1, \dots, Mix_m$  escogida por el receptor, donde  $c_m$  puede ser una clave secreta de un sistema de cifrado simétrico. El mensaje añadido a la dirección de retorno pasará por estos mixes en orden ascendente dependiendo de sus índices.  $A_{m+1}$  puede ser la dirección del receptor llamado  $Mix_{m+1}$ . De forma similar, al emisor se le llama  $Mix_0$ . El receptor crea una dirección de retorno no trazable  $(k_0, A_1, R_1)$  donde  $k_0$  es una clave de un sistema de cifrado simétrico generada para este propósito.  $Mix_0$  se supone que utiliza esta clave para codificar el contenido del mensaje con el fin de garantizar que el  $Mix_1$  no sea capaz de leer este mensaje.  $R_1$  es parte de la dirección de retorno, la cual se transmite a través del  $Mix_0$  y contiene el mensaje generado y que ha sido cifrado utilizando  $k_0$ .  $R_1$  inicialmente se crea escogiéndose aleatoriamente un único nombre de la dirección de retorno en un esquema recursivo como el que se muestra a continuación:

- $R_j$  es la parte de la dirección de retorno que será recibida por el  $Mix_j$ .
- $k_j$  es la clave de un sistema de cifrado simétrico, con el cual  $Mix_j$  codifica la parte legible del mensaje.

$$R_{m+1} = e \quad (3.3)$$

$$R_j = c_j(k_j, A_{j+1}, R_{j+1}) \text{ para } j = m, \dots, 1. \quad (3.4)$$

El mensaje  $N_j$  está constituido por la parte de la dirección de retorno  $R_j$  y el contenido  $I$  del mensaje (codificado varias veces) generado por el emisor (también llamado parte  $I_j$  del contenido). Los mensajes  $N_j$  son creados por el  $Mix_{j-1}$  y son enviados al  $Mix_j$  de acuerdo al siguiente esquema recursivo. Estos son creados y enviados por el emisor  $Mix_0$  y así, en secuencia, se pasan a través de los mixes  $Mix_1, \dots, Mix_m$

$$N_1 = R_1, I_1; I_1 = k_0(I) \quad (3.5)$$

$$N_j = R_j, I_j; I_j = k_{j-1}(I_{j-1}) \text{ para } j = 2, \dots, m+1 \quad (3.6)$$

El receptor  $Mix_{m+1}$  recibe  $e$ ,  $N_{m+1} = e(km(\dots k1(i))\dots)$  y puede descifrar y extraer el contenido  $I$  ya que conoce todas las claves secretas  $k_j$  asignadas para el nombre  $e$  de la parte de la dirección de retorno en el orden correcto.

### Verificación del tamaño del conjunto anónimo

Si un atacante bloquea el mensaje de un participante específico, este mensaje se aísla del conjunto anónimo. Lo mismo sucedería si un atacante rodea a un participante específico, manipulándolo a través de la generación de mensajes con fines ilícitos para el sistema. Este tipo de ataque es conocido como el ataque de mezcla o  $n-1$ . No existe una solución específica contra este tipo de ataques en ambientes abiertos, como por ejemplo en aquellos donde los participantes entran y salen del sistema a su discreción. Se podría utilizar una protección básica si el mix puede identificar a cada participante, así de una forma confiable el mix puede verificar si los mensajes que tiene almacenados en su memoria temporal ("buffer") fueron enviados por un número relativamente adecuado de usuarios.

### Canales Mix

Los canales mix son utilizados para manejar en tiempo real las cadenas continuas de datos o que contengan sólo pequeños retrasos a través de una cadena de mixes. Para este caso, es necesario que se divida el ancho de banda: una parte para la señalización y otra parte para el envío de los datos, ambos utilizados para la transmisión del mensaje.

Se podría asumir que existe un sólo canal para la señalización, y varios canales para la transmisión de datos. Con el fin de establecer el canal, se envía un mensaje sobre el canal de señalización, el cual contiene la clave  $k_i$  que deberá ser utilizada entre el emisor y el  $Mix_i$ , la cual se cifra de forma asimétrica con la clave pública de dicho mix. Con esto, se define un canal de igual forma para todos los mixes, sobre el cual será transmitido el mensaje.

Se podría utilizar un canal para el envío y otro canal para la recepción. Un canal de envío es análogo a un cifrado híbrido: el emisor establece un canal, y codifica continuamente su información  $N$ , transformándola en  $k_1(k_2(\dots k_m(N)\dots))$  y enviándola al mix  $Mix_1$ . Cada mix  $Mix_i$  para  $(i = 1, \dots, n-1)$  decodifica los mensajes recibidos continuamente utilizando  $k_i$  y transmitiendo el resultado de la decodificación al mix  $Mix_{i+1}$ . El mix  $Mix_m$  crea el mensaje en texto plano en el final de la cadena. Esto le permite al emisor enviar anónimamente los mensajes, pero en este caso el receptor no será anónimo. Un canal de recepción es en realidad un canal de envío el cual se utiliza en dirección opuesta, es decir, el receptor es el que establece el canal. El emisor le envía al mix  $Mix_m$  la cadena  $N$  de información que no está especialmente codificada por el mix  $Mix_m$ , luego lo codifica utilizando la clave  $k_m$  y conduce  $k_m(N)$  un paso atrás, hacia el mix  $Mix_{m-1}$ . Los otros mixes hacen lo mismo, por ejemplo, el mix  $Mix_1$  envía la cadena  $k1(\dots km(N)\dots)$  codificada. Dado que el receptor conoce todas las claves públicas  $k_i$ , tiene la disponibilidad de descifrar  $N$ . Esto le permite al receptor recibir los mensajes anónimamente mientras que el emisor no es anónimo.

Para alcanzar ambos niveles de anonimato, en [8] sugieren la creación de canales Mix como enlaces de los canales de envío y recepción. El emisor establece un canal de envío que finaliza en el mix  $Mix_m$  y el receptor establece un canal de recepción que inicia en el  $Mix_m$ . El mix  $Mix_m$  traspasa las cadenas de información que llegan por el canal de envío hacia el canal de recepción. Los canales que están supuestamente enlazados, se etiquetan con una marca común que se recibe consistentemente en ambos canales que establecen los mensajes

asociados al mix  $Mix_m$ . Los datos transferidos están coordinados con un mensaje de entrada al mix cifrado asimétricamente, el cual contiene la información del mix que conecta a los dos canales, y el usuario emisor del mensaje de entrada al mix actúa como un emisor o un receptor. Cada mix en la cadena puede descifrar este mensaje de entrada al mix y en el último paso, el texto plano se difunde a todos los suscriptores. Ahora, los canales pueden ser establecidos utilizando los mensajes de establecimiento de ambos participantes. Estos escogen los mixes por el canal de transferencias de datos del mix  $Mix_m$  y los mantienen en secreto. Así todos conocen sólo la mitad del camino y el mix  $Mix_m$  reenvía los mensajes entrantes del canal de envío del mix al canal de recepción del mix. Cada emisor/receptor debe tener el mismo número de canales de envío/recepción, porque de lo contrario serían observables, por tal razón convendrá utilizar canales “dummy”.

Para poder entender mejor el funcionamiento de la redes de mezcla se presentan las figuras 3.3 y 3.4, en la que se puede observar que para el envío de un mensaje de un punto inicial a uno final, primero debe pasar por varios puntos intermedios, donde se realiza el proceso de mezcla con otros mensajes provenientes de otros nodos de origen y con diversos destinos. En cada nodo mezclador también se generan mensajes de relleno o dummy.

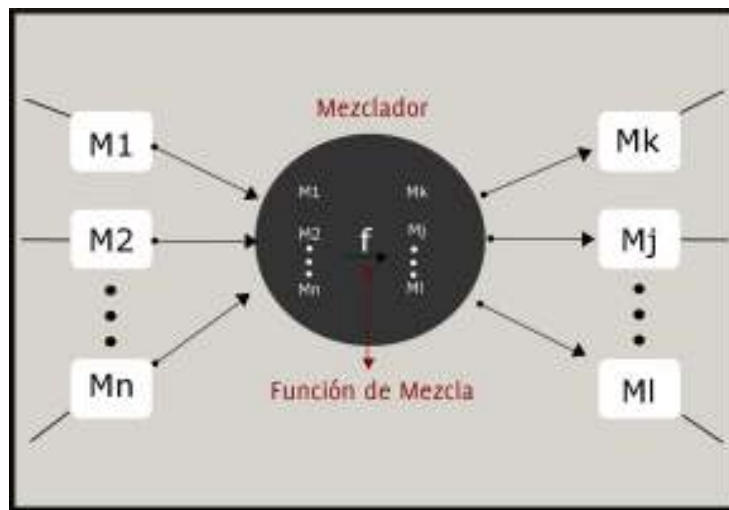


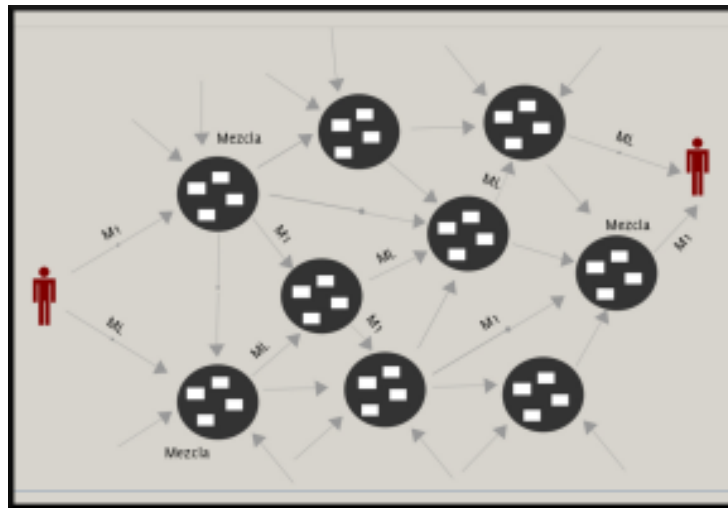
Figura 3.3 Redes de Mezcla

### 3.1.2.2. Enrutamiento cebolla:

Este mecanismo fue propuesto y estudiado en [9, 10, 11]. Es equivalente a una red de mixes, pero en el contexto de enrutamiento basado en circuitos. En vez de enrutar cada paquete separadamente, el primer mensaje lo que hace es abrir un circuito, etiquetando una ruta. Cada mensaje que tiene una etiqueta en particular se enruta por un camino predeterminado. Finalmente, un mensaje se envía para que cierre o clausure un camino. Con frecuencia se hace referencia a flujo anónimo como la información que viaja por estos circuitos. Su objetivo es dificultarle la tarea al análisis de tráfico, uno de los tipos de ataques más conocidos. Este sistema procura proteger la no relacionabilidad de dos participantes que se comunican a través de terceras partes, y procura proteger la identidad de las partes comunicantes. En vista de que las redes ISDN son difíciles de implementar en Internet, lo que procuró el enrutamiento cebolla es adaptar esta idea distribuyendo la red anónima y adaptándola para que se ejecute en el tope del modelo TCP/IP. El primer mensaje enviado en la red se cifra en capas, que pueden ser descifradas en una cadena de enrutadores cebolla (*onion routers OR*) los cuales utilizan sus respectivas claves privadas.

El primer mensaje tiene el material que debe ser compartido entre el emisor y los enrutadores, también las etiquetas y la información de direccionamiento del próximo nodo. Tal como sucede en los mixes de Chaum





**Figura 3.4** Topología Mix

[1], se provee la no relacionabilidad a nivel de bits, de esta forma el camino que toma el primer mensaje no es trivial de seguir con sólo observar el patrón de bits de los mensajes.

También se propuso un tipo de enrutamiento dinámico donde los enrutadores que reenvían el flujo a través del camino establecido no se especifican únicamente en el mensaje inicial, esto con el fin de incrementar el anonimato. Los datos que circulan por la red en un circuito establecido están cifrados con las claves simétricas de los enrutadores. Las etiquetas se utilizan para indicar a cuál circuito pertenece cada paquete. Se utilizan etiquetas diferentes para los distintos enlaces, asegurando así la no relacionabilidad, y además las etiquetas de los enlaces también se cifran utilizando una clave que se comparte entre los pares de enrutadores OR. Lo anterior previene los ataques de observadores pasivos que puedan determinar cuáles paquetes pertenecen al mismo flujo anónimo, pero no le oculta la información a un enrutador que pueda ser subversivo.

OR es susceptible a un conjunto de ataques, tal como el ataque de tiempo. Esto se debe a que los patrones pudiesen ser analizados por un atacante en ausencia de un gran volumen de tráfico pesado. Para este sistema se afirma proveer anonimato en la navegación web la cual requiere comunicaciones con baja latencia, por tal razón se ha excluido toda la dinámica de los mezcladores o mixes, dado que pudiese incrementar demasiado los tiempos de respuesta. En ausencia de este tipo de características, lo hace vulnerable a distintos tipos de ataques superados por los mixes, por ejemplo el ataque de correlación del tráfico de mensajes, donde se pudiese determinar cuáles mensajes entrantes corresponden con los salientes, con respecto a un enrutador.

Los enrutadores se pueden configurar para que trabajen sólo con un determinado subconjunto de clientes, ya sea por zonas o de forma particularizada. Además se puede configurar para que trabajen sólo con un subconjunto de otros enrutadores.

### **Tor: la segunda generación de OR**

El proyecto OR fue retomado en el año 2004, con el diseño e implementación de lo que se denominó la “segunda generación del onion router” o TOR, por sus siglas en inglés, la propuesta se muestra en [4]. Su política es la del reenvío de flujo TCP sobre una red de reenvíos, y junto con la ayuda de otra herramienta, el Privoxy<sup>1</sup>, está especialmente diseñada para el tráfico web.

Este sistema utiliza una arquitectura de red tradicional: una lista de servidores voluntarios se obtiene desde un servicio de directorio ofrecido por otro(s) servidor(es). De esta forma, los clientes crean caminos utilizando

<sup>1</sup><http://www.privoxy.org>

al menos tres nodos intermedios escogidos de forma aleatoria dentro de la lista, y sobre los cuales se hace la comunicación de la información. A diferencia de la arquitectura anterior, donde se enviaba y distribuía el material criptográfico, TOR utiliza un mecanismo interactivo: el cliente se conecta con el primer nodo, y le solicita a éste que se conecte con el segundo nodo, de esta forma un canal bidireccional se utiliza en cada paso para desarrollar un intercambio de claves autenticado mediante el algoritmo DF (Diffie-Hellman). Este garantiza el reenvío en forma secreta y la resistencia a la compulsión, debido principalmente a que solo son necesarias claves de corta duración. Este mecanismo fue inicialmente propuesto en Cebolla (ver [13]), y no está cubierto en la patente de OR (ver [10]).

Otra notable diferencia entre TOR y los intentos anteriores por anonimizar el tráfico de flujo, es que TOR no ofrece seguridad contra los atacantes que pueden observar la red entera, es decir, contra atacantes pasivos globales. Un conjunto de técnicas de Análisis de Tráfico (ver [14, 15, 16, 17, 18]) han sido desarrolladas a través de los años para trazar el flujo de tráfico continuo viajando por redes de baja latencia como TOR. En estos estudios se ha demostrado que este tipo de ataques son muy difíciles de contrarrestar, a menos que se utilicen técnicas que implicarían latencias elevadas, o que requieran la inyección de grandes cantidades de tráfico cubierto (tráfico inservible o “dummy”), los cuales representan soluciones muy costosas. Por esta razón en TOR se opta por obtener un nivel de seguridad que se pueda alcanzar en un sistema altamente utilizable y muy económico de utilizar (ver [19, 20]). Como resultado si un adversario puede observar el flujo entre dos puntos de la red, puede de forma trivial generar el mismo tráfico, y lograr ataques del tipo etiquetado o “tagging”. Sin embargo, dada esta vulnerabilidad, aun se necesita estimar la probabilidad de que un adversario pueda estar monitoreando la red en múltiples puntos sobre un camino o ruta establecida.

TOR también ofrece mecanismos para ocultar los servidores. Un servidor oculto abre una conexión anónima y la utiliza para publicar un punto de contacto. Si un cliente quiere contactar a un servidor, debe conectarse con un punto de contacto y negociar un canal anónimo separado del que se utiliza para el reenvío de la comunicación actual. Un ataque propuesto en [21] demuestra la vulnerabilidad de esta idea. La intuición detrás de este ataque está en el hecho de que un adversario puede abrir múltiples conexiones hacia un mismo servidor oculto, y secuencialmente o en paralelo podría controlar el flujo hacia ese servidor. Para esto, el atacante necesitaría controlar al menos un enrutador, y debe esperar a que el servidor escoja una de las conexiones de su enrutador como un primer nodo de un camino anónimo cualquiera.

## REFERENCIAS

---

1. Endira Mora et. al. Gestión de anonimato. <https://tibisay.cenditel.gob.ve/gestionanonimato/wiki/PlanDeTrabajo%3A>, 2014.
2. Information Commissioner Office. Data protection technical guidance note: Privacy enhancing technologies (pets). Technical report, Information Commissioner Office, April 2006.
3. Organización de las Naciones Unidas. Derechos humanos para todos. declaración universal de los derechos humanos. Technical report, Organización de las Naciones Unidas, 1948.
4. A. Pfitzmann and M. Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. [http://dud.inf.tu-dresden.de/Anon\\_Terminology.shtml](http://dud.inf.tu-dresden.de/Anon_Terminology.shtml), 2000.
5. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4, 1981.
6. O. Berthold, A. Pfitzmann, and R. Standtke. The disadvantages of free mix routes and how to overcome them. *Proceedings of Privacy Enhancing Technologies Workshop*, pages 30–45, 2001.
7. George Danezis. *Better Anonymous Communications*. PhD thesis, University of Cambridge, July 2004.
8. Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. ISDN-mixes: Untraceable communication with very small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems*, pages 451–463, February 1991.
9. S. Mauw, J. Verschuren, and E.P. de Vink. A formalization of anonymity and onion routing. In P. Samarati, P. Ryan, D. Gollmann, and R. Molva, editors, *Proceedings of ESORICS 2004*, pages 109–124. LNCS 3193, 2004.
10. Paul Syverson, Michael Reed, and David Goldschlag. Onion Routing access configurations. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX 2000)*, volume 1, pages 34–40. IEEE CS Press, 2000.
11. Paul Syverson, Gene Tsudik, Michael Reed, and Carl Landwehr. Towards an Analysis of Onion Routing Security. In H. Federrath, editor, *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, pages 96–114. Springer-Verlag, LNCS 2009, July 2000.
12. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium*, 2004.

13. Zach Brown. Cebolla: Pragmatic IP Anonymity. In *Proceedings of the 2002 Ottawa Linux Symposium*, June 2002.
14. George Danezis. The traffic analysis of continuous-time mixes. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 35–50, May 2004.
15. Brian N. Levine, Michael K. Reiter, Chenxi Wang, and Matthew K. Wright. Timing attacks in low-latency mix-based systems. In Ari Juels, editor, *Proceedings of Financial Cryptography (FC '04)*, pages 251–265. Springer-Verlag, LNCS 3110, February 2004.
16. Andrei Serjantov and Peter Sewell. Passive attack analysis for connection-based anonymity systems. In *Proceedings of ESORICS 2003*, October 2003.
17. Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati, and Wei Zhao. On flow correlation attacks and countermeasures in mix networks. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 207–225, May 2004.
18. Xinyuan Wang, Shiping Chen, and Sushil Jajodia. Tracking anonymous peer-to-peer voip calls on the internet. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 81–91, November 2005.
19. Nick Mathewson and Roger Dingledine. Practical traffic analysis: Extending and resisting statistical disclosure. In *Proceedings of Privacy Enhancing Technologies workshop (PET 2004)*, volume 3424 of *LNCS*, pages 17–34, May 2004.
20. Adam Back, Ulf Möller, and Anton Stiglic. Traffic analysis attacks and trade-offs in anonymity providing systems. In Ira S. Moskowitz, editor, *Proceedings of Information Hiding Workshop (IH 2001)*, pages 245–257. Springer-Verlag, LNCS 2137, April 2001.
21. Lasse Øverlier and Paul Syverson. Locating hidden servers. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE CS, May 2006.

## CAPÍTULO 4



# FUNDAMENTOS JURÍDICOS

---

ENDIRA MORA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

### 4.1. El ordenamiento jurídico venezolano y las nuevas tecnologías de la información

La información se ha convertido en uno de los factores principales de la civilización, haciéndose más compleja y abundante con el pasar de los días. Gracias al computador la información se almacena en formato electrónico, dando paso nuevas formas de comunicación y en algunos casos complicaciones de orden, social, económico y jurídico. A raíz de ello surgen entonces nuevos Derechos Humanos entre los que se encuentra el derecho a la información, que está integrado por tres elementos: la facultad de recolectar información, difundirla y controlarla no sólo por el signatario de la misma sino por los Estados [1]. Esto amerita que el ordenamiento jurídico internacional y nacional se acople a los cambios en la materia y regule las relaciones producto de la interacción de los ciudadanos por medios electrónicos, a fin de mantener el orden social.

La dinámica que ha tomado el manejo de la información en las últimas décadas hace necesario que se asegure a todos los ciudadanos el derecho a estar informados, sin embargo el ejercicio de este derecho puede causar efectos perjudiciales sobre otros derechos que le son inherentes como individuo, esto amerita que se tomen medidas pertinentes para prevenir consecuencias indeseables producto del inadecuado manejo o

difusión de la información, cabe mencionar que en tal sentido la *Directiva para la Protección de los Datos personales adoptada en el parlamento Europeo* y por el Consejo Europeo indica en el preámbulo, que los sistemas de tratamiento de datos deben estar al servicio del hombre, de los derechos fundamentales y de la libertad de éstos, en particular de la intimidad, establece además que debe contribuir con el desarrollo social, económico, el bienestar de los individuos. Con ello procura la protección de derechos fundamentales, tales como la identidad, integridad e intimidad, así como el consentimiento informado de todas las actividades de tratamiento de datos vinculadas con la salud, procura asimismo la protección de los datos, el acceso a las nuevas tecnologías, avances científicos y tecnológicos entre otros.

Desde hace algunas décadas se ha venido regulando el tema de la Tecnologías de la Información, en este sentido es oportuno señalar las primeras legislaciones en la materia; la Primera Ley Nacional de Protección de datos del mundo y fue en Suecia en 1973, luego en 1974 en Estado Unidos de Norteamérica, las agencias estatales se vieron obligadas a seguir ciertas directrices para la utilización de información personal en donde se exigía la notificación del informado por el almacenamiento de sus datos [2]. Posteriormente la Ley de Firma Digital de Utah fue puesta en vigencia en mayo de 1995 en esa región de los Estado Unidos de Norteamérica, en la que se prevén procesos que regulan aspectos tales como: el sistema de doble clave para la verificación, validación y autenticidad de la transacciones realizadas a través de la web, protección de datos entre otros y tiene por objeto: 1. Facilitar las transacciones mediante mensajes electrónicos confiables; 2. Reducir al mínimo la posibilidad de forjar firmas digitales y del fraude en las transacciones electrónicas. 3. Instrumentar jurídicamente la incorporación de normas pertinentes, tales como la X.509 (ver sección 1.3.2); 4. Establecer, en coordinación con diversos Estados, normas uniformes relativas a la autenticación y confiabilidad de los mensajes electrónicos [3]. En el mismo orden de ideas, para 1996 la Comisión de la Naciones Unidas para el Derecho Internacional (UNCITRAL/CNUDMI), presenta el modelo de Ley Sobre Comercio Electrónico resolución 51/162, que contempla normas que buscan estandarizar el uso de la firma electrónica, modelo que serviría de base para el desarrollo de las legislaciones nacionales [4], de la cual se hablará un poco al final del capítulo.

Con respecto a América Latina, desde 1997 se han venido dando iniciativas legislativas que establecen principios generales sobre la protección de datos, que regulan la procedencia y resguardo de los datos de los individuos [5], a continuación se listan algunos de éstos:

- La formación de datos será lícita siempre y cuando se tomen en consideración las leyes y reglamentos que en la nación rigen al respecto.
- Los archivos no pueden contener información o cualidades contrarias a la norma establecida en las naciones y a la moral pública; dejando claro con ello que es ilícito crear archivos que contengan pornografía.
- Los datos de personas, relacionados a la identidad, a los efectos de su tratamiento deben contener información cierta, adecuada y pertinente, sin exceder el ámbito para el cual fue obtenida, es decir la información y los datos que no deben ser empleados libremente para usos comerciales o ilícitos.
- La recolección de datos debe hacerse por medios lícitos y en la forma que la ley estable para ello. En el caso de venezolano, debe considerarse particularmente el artículo 60 de la Constitución de República Bolivariana de Venezuela <sup>1</sup>.
- Los datos deben ser exactos y actualizarse de ser necesario. En caso de que se trate de datos inexactos éstos se deben destruir, suplantar o completar por los responsables de recabarlos o de administrar la base de datos donde se hospeden, una vez que tengan conocimiento de la dificultad que presente la información. Este derecho es garantizado a los titulares de datos en el Estado Venezolano mediante la acción de *Habeas Data*, que se describirá más adelante.
- Los datos deben ser almacenados de manera tal que permitan el acceso de sus titulares cuando éstos así lo requieran, y deberán ser destruidos cuando dejen de tener el valor para el cual fueron creados.

<sup>1</sup> Artículo 60 CRBV. "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."

En Venezuela, con la entrada en vigencia de la Constitución de la República Bolivariana de Venezuela en el año 1999 y la posterior creación de le Ministerio de Ciencia y Tecnología, hoy ministerio del Poder Popular para la Educación Universitaria Ciencia y Tecnología, se le otorga a la Ciencia y Tecnología, por ende las Tecnologías de la Información y Comunicación, valor con preponderancia constitucional. Así se expresa en el artículo 110 de la CRBV donde se reconoce el interés público de ellas y del conocimiento, la innovación, sus aplicaciones y los servicios de información necesarios, y se indica el valor superior de la ciencia y la tecnología para el desarrollo de la nación, la seguridad y soberanía nacional. En este artículo se proporciona fundamento constitucional a las regulaciones en materia de Tecnologías de la Información y Comunicación (TIC), ciencia y tecnología en general, y se establece que el Estado asume la responsabilidad de garantizar estos principios éticos y legales mediante modos y medios que determinará la Ley. Entre las leyes que desarrollan estos preceptos se encuentran, la Ley Orgánica de Ciencia Tecnología e Innovación<sup>2</sup>, Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónica<sup>3</sup>, Ley Especial Contra Delitos Informáticos<sup>4</sup>, Ley de Bancos y Otras Instituciones Financieras<sup>5</sup>, Ley de Infogobierno<sup>6</sup>, Ley de Orgánica Telecomunicaciones<sup>7</sup> como algunos de los instrumentos desarrollados por el Estado Venezolano a fin de regular la materia.

La protección por parte del Estado a los ciudadanos venezolanos, la informática y a la información que de ella se puede difundir o extraer, está expresamente regulada en artículo 60 de la CRBV:

“Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos”.

Éste es uno de los fundamentos novedoso que aparece en la CRBV 1999, que da respuesta a la exigencia que se plantean a los Estados en torno a la regulación de las TIC al ligar el honor y la privacidad con limitaciones al uso de la informática, siendo considerado un Derecho Humano de cuarta generación[6],

## 4.2. Derecho de *Habeas Data*

Forma parte de los fundamentos constitucionales que dan respuesta a la regulación de las Tecnologías de la Información, en materia de Identidad Digital, el derecho de *Habeas Data* estipulado en el artículo 28 de la CRBV:

“Toda persona tiene **derecho de acceder** a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y **de solicitar ante el tribunal** competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, **podrá acceder** a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley”.<sup>8</sup>

El constituyente ha planteado el *Habeas Data* no sólo como un Derecho sino como Garantía Constitucional, ya que le otorga a los ciudadanos el derecho de “acceder a la información” y además establece los medios para hacer efectivo este derecho. El *Habeas Data* tiene por objeto determinar, entre otras cosas, la violación de la privacidad o intimidad, como punto de partida de un ilícito cometido, siendo, en el ámbito de las tecnologías de la información, el único mecanismo de tutela para la protección de datos informáticos [5] que se plantea en la Constitución. Finalmente, la Sala Constitucional señaló que a la luz del artículo. 28, los dos primeros derecho,

<sup>2</sup>Gaceta Oficial de la República Bolivariana de Venezuela. Número 39.575, 16 de diciembre de 2010.

<sup>3</sup>Decreto N° 1.204, 10 de febrero de 2001. Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.148, 28 de febrero de 2001.

<sup>4</sup>Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.313, 30 de octubre de 2001.

<sup>5</sup>Decreto N° 1.526, 3 de noviembre de 2001. Gaceta Oficial de la República Bolivariana de Venezuela. Número 5.555 Extraordinario, 13 de noviembre de 2001.

<sup>6</sup>Gaceta Oficial de la República Bolivariana de Venezuela. Número 40.274, 17 de octubre de 2013.

<sup>7</sup>Gaceta Oficial de la República Bolivariana de Venezuela. Número 39.610, 7 de febrero de 2011.

<sup>8</sup>Énfasis del autor.

acceder y conocer, pueden generar amparos autónomos, y solo el tercero, solicitar actualización, rectificación o destrucción puede engendrar propiamente el **Habeas Data**. Este criterio jurisprudencial cambió a partir de la Ley Orgánica del Tribunal Supremo de Justicia del 01 de octubre de 2010. (ver artículo 167), único aparte donde queda incluido bajo **Habeas Data** todo lo que se plantea en la CRBV.

#### 4.2.1. Derechos que otorga el *Habeas Data*

Con el fin de resguardar la información y los datos sobre las personas naturales o jurídicas que se inscriban en los registros, se otorga una serie de derechos a la ciudadanía en el artículo 28 de la CRBV; derechos que se pueden condensar de la siguiente manera:

- **De conocer** sobre la existencia de registros de datos personales;
- **De acceso** individual a la información, que puede ser normativa; o el tipo de información donde la persona queda vinculada a comunidades o a grupos.
- **De respuesta**, que permite controlar y conocer información que sobre la persona se ha recolectado;
- **De conocer sobre el uso y finalidad** que se le da a la información por parte de quien la registra.
- **De actualización**, con el fin de corregir información inexacta, que ha sido modificada o se ha vuelto inexacta por el transcurrir del tiempo o por errores de recolección de datos.
- **De rectificación** de información inexacta o incompleta.
- **De destrucción** de aquellos datos que afecten la integridad de la persona o grupo.

Según [2] el *Habeas Data* es un derecho que asiste a toda persona a solicitar judicialmente la exhibición de los registros (públicos o privados), en los cuales estén incluidos sus datos personales, para tener conocimiento de su exactitud y adecuado uso o requerir la actualización, rectificación o supresión de datos inexactos, obsoletos o que impliquen una violación a sus derechos. Estos datos son considerados parte integrante de la persona y quienes los administran están obligados a: estar legitimados para su obtención, llevar un correcto registro (sin falsedades, lo que incluye también su actualización), asegurar su confidencialidad y no proveer información sino mediante autorización del titular o a solicitud de autoridad competente y evitar su deterioro o destrucción.

El ciudadano o ciudadanos que hagan uso de este derecho, **una vez acreditada su cualidad**, podrán solicitar toda la información que en bancos de datos públicos (CNE, CICPC, CGR, Hospitales) o privados (Clínicas, Bancos) contengan sobre él o ellos, sin que necesariamente acuda a un tribunal. Ahora bien, si por alguna circunstancia esta información contiene datos que pertenecen a otros titulares, solo serán revelados aquellos que conciernen directamente al titular solicitante, excepto cuando se trate de comunidades o grupos. En este particular se ha dejado evidencia mediante jurisprudencia vinculantes<sup>9</sup> que la acción podrá iniciarse únicamente por los titulares de la información o datos, y no por terceros que se supongan afectados.

El artículo 28 de la CRBV deja claro los derechos que asisten en materia de *Habeas Data* a los particulares y colectivos, sin embargo ¿Qué sucede con los que tienen la función de recolectar datos o información? ¿Pueden éstos recolectar información?, al respecto la Sala Constitucional ha determinado en sentencia de fecha 14 de Marzo de 2001, caso INSACA C.A., que el artículo 28 de la CRBV otorga a las personas el derecho de recopilar información sobre las personas, y sus bienes. En criterio de la Sala, este derecho a recopilar comprende tanto los datos que han sido aportados de forma voluntaria como aquellos que provienen de publicaciones, contratos, tarjetas de crédito, transmisiones telemáticas entre otros, con o sin la autorización de la persona involucrada e incluso sin que ella tenga conocimiento del almacenamiento de los mismos, además de no hacer distinción del trato que se le debe dar a la información de carácter público o privado, sin más limitaciones que las que estable

<sup>9</sup>Según [7] Es el conjunto de sentencias y decisiones dictadas por los tribunales, principalmente por el juzgado jerárquicamente superior dentro de la organización judicial de un país.



el artículo 60 Constitucional (antes mencionado), ni infringir otros derechos y garantías contemplados para los ciudadanos venezolanos en la CRBV, asimismo podrá limitarse o restringirse la recopilación de información por razones de Seguridad Nacional, Orden Público, Salud o Moral Pública<sup>10</sup>.

#### 4.2.2. Procedimiento de *Habeas Data*

El procedimiento aplicable para ejercer la acción de *Habeas Data* se rigió hasta el año 2010 por el procedimiento establecido en el Código de Procedimiento Civil para el Juicio Oral, con variantes dirigidas a la oralidad, brevedad, la inmediación y la concentración de este tipo de procesos, hasta el año 2010 sostuvo, con relación al tribunal competente, lo planteado en sentencia de la Sala Constitucional de fecha 20 de enero y 1º de febrero de 2000:

“que las normas constitucionales tienen vigencia plena y aplicación directa, y que cuando las leyes no han desarrollado su ejercicio y se requiere acudir a los tribunales de justicia, debido a la aplicación directa de dichas normas, es la jurisdicción constitucional, representada por esta Sala Constitucional, la que conocerá de las controversias que surjan con motivo de las normas constitucionales aún no desarrolladas legislativamente, hasta que las leyes que regulan la jurisdicción constitucional, decidan lo contrario. Existiendo en el país una Sala Constitucional, específica para conocer lo relativo a las infracciones de la Carta Fundamental, no parece lógico, ante el silencio de la ley, atribuir el conocimiento de estas causas a tribunales distintos. Tal interpretación es vinculante a partir de esta fecha y así se declara”.

Sin embargo desde el año 2010 la Ley Orgánica del Tribunal Supremo de Justicia en el título XI de las Disposiciones Transitorias en el capítulo IV artículos 167 al 178, establece el procedimiento aplicable en cuanto a la acción de *Habeas Data*<sup>11</sup>.

En primer lugar, se define *Habeas Data*: como el Derecho que asiste a toda persona a conocer sobre los datos que a ella se refieran así como la finalidad de uso, haciendo una descripción análoga a lo que establece el artículo 28 de la CRBV, a diferencia del artículo antes referido, en este caso se indica con precisión que sólo podrá interponerse la acción de *Habeas Data* en caso de que el administrador de datos no suministre o se abstenga de suministrar los datos requeridos previamente por el agraviado hasta 20 días hábiles posteriores a la formulación de la solicitud [5]. Dejando en claro el momento y las circunstancias en que se puede interponer la acción de *Habeas Data*, siendo los principios de Celeridad y Publicidad<sup>12</sup> los que regirán el procedimiento de dicha acción, el cual se describe a continuación:

##### ■ Requisitos de la demanda

Los Tribunales de Municipio con competencia en lo Contencioso Administrativo y con competencia territorial en el domicilio del solicitante son los encargados de conocer sobre estas causas, para lo cual el solicitante agraviado deberá presentar un escrito con los instrumentos que acrediten su pretensión o en su defecto con aquellos que indiquen la no posibilidad de presentar dichos instrumentos para el momento de la solicitud; en este punto en particular es pertinente señalar que actualmente son pocos los Estados venezolanos donde están formalmente conformados los Tribunales de Municipio con competencia Contencioso Administrativa. Con relación a esto la Ley Orgánica en lo Contencioso Administrativo en la Disposición Transitoria Sexta, indica que: “Hasta tanto entren en funcionamiento los Juzgados de Municipio de la Jurisdicción Contencioso Administrativa, conocerán de las competencias atribuidas por esta Ley a dichos tribunales los Juzgados de Municipio”.

##### ■ Informe del agravante

Admitida la acción, el Tribunal ordenará al supuesto agravante (administrador de datos) que emita los

<sup>10</sup> Artículo 19 de la Ley aprobatoria del Pacto de Derechos Civiles y Políticos.

<sup>11</sup> Ley Orgánica del Tribunal Supremo de Justicia año 2010.

<sup>12</sup> Artículo 168. Para la tramitación del Habeas data todo tiempo será hábil y no se admitirán incidencias procesales. Artículo 177. Todas las actuaciones serán públicas. El Tribunal, de oficio o a solicitud de parte, cuando estén comprometidas la moral y las buenas costumbres, o cuando exista disposición expresa de ley, podrá ordenar la reserva del expediente y que la audiencia sea a puerta cerrada. Ley Orgánica del Tribunal Supremo de Justicia año 2012

informes y documentación correspondientes en un lapso de cinco (05) días hábiles a partir de la notificación. Si por alguna razón no se emitiese el informe correspondiente, el supuesto agraviante podrá ser sancionado con multa de hasta 200 Unidades Tributarias, sin perjuicio de otras sanciones a las que hubiere lugar, reservándose el tribunal la potestad de solicitar las pruebas que juzgue necesarias con ocasión de esclarecer los hechos.

■ **Observaciones al informe**

Una vez sean recibidos los informes o elementos probatorios requeridos se tendrán tres (03) días para que el solicitante formule las observaciones pertinentes; pasado este lapso, en los cinco (05) días siguientes el Tribunal tomará una decisión. Antes de ello, cuando la complejidad del caso lo amerite, el Tribunal podrá convocar una audiencia pública para esclarecer los hechos, la cual se regirá bajo los principios de concentración e inmediatez<sup>13</sup> a fin de esclarecer los hechos. Esta audiencia deberá realizarse en presencia de las partes, si el agraviado llegase a faltar se entenderá por desistida la acción y se dará por terminado el procedimiento, a menos de que el Tribunal considere que se trata de un asunto de orden público, en cuyo caso se puede inquirir sobre los hechos alegados en un lapso breve, en caso de *litis consorcio*, cualquiera de los *litis consortes* puede representar al consorcio. Una vez concluido el debate el Juez debe deliberar en cuyo caso, podrá decidir de manera inmediata, o podrá publicar el fallo en los cinco (05) días siguiente en la cual se dictó; podrá a su vez diferir la audiencia por estimar la presentación o evacuación de pruebas o recaudos necesarios para tomar una decisión.<sup>14</sup> el pronunciamiento de su decisión. La sentencia completa deberá ser publicada dentro de los diez días de despacho posteriores a la conclusión del debate en la audiencia pública, o al vencimiento del plazo de diferimiento que el Tribunal haya establecido.

- Para las notificaciones al presunto o presunta agraviante aplican lo establecido en los artículos 91, 92 y 93 de la Ley del Tribunal Supremo de Justicia. En ese sentido podrá acudir a los medios tradicionalmente empleados para esos fines, tales como la emisión de boleta o cualquier medio de comunicación interpersonal, a fin de evitar excesivos formalismos. En todo caso las notificaciones deberán contener una clara advertencia de las consecuencias procesales de su incumplimiento. La secretaria o secretario del Tribunal dejará constancia expresa en el expediente de haber practicado las notificaciones y de sus consecuencias.

■ **Contenido de la sentencia**

Si la sentencia es declarada con lugar, el agraviante de forma inmediata deberá hacer la corrección, supresión, rectificación, confidencialidad, actualización o uso de los datos a los que se refiera la acción, la negativa a realizar cualquiera de las acciones a las que haya lugar acarreará pena de prisión de seis (06) meses a un (01) año.

■ **Apelación**

En los tres (03) días siguiente de publicada o notificada la decisión se abrirá el lapso de apelación ante la instancia correspondiente, Tribunal Superior, una vez recibida por éste se tendrán un lapso de cinco (05) días de despacho para que las partes presenten sus escritos. Concluido este lapso en los treinta (30) días continuos siguientes el Tribunal tomará una decisión, la cual no podrá ser objeto de casación.

En caso de que la acción de *Habeas Data* trate sobre la corrección de errores de tipo numérico, mayúsculas, letras erradas u omisión letras, palabras mal escritas o errores ortográficos, traducción y/o transcripción errónea de nombres, apellidos o otros términos, el procedimiento se limitará a demostrar el error ante el Juez.

El *Habeas Data* aún debe ser desarrollado ampliamente, ya que en los términos en que se plantea en estos momentos es una acción reactiva. reactiva y muy poco se desarrolla su potencial como acción preventiva; esta situación proviene de el *Habeas Data* se rige en la actualidad por normas transitorias, que buscan suplir la carencia de leyes que lo aborden como asunto principal. Es necesario entonces que las instancias del Poder Público competentes se avoquen a crear una legislación completa en materia, la cual debería desarrollar cada

<sup>13</sup>En virtud de este principio, desarrollado en el artículo 157 de la Ley Orgánica del Tribunal Supremo de Justicia, el Tribunal atenderá en forma inmediata y concentrada — sin participación de otras instancias — tanto la exposición de la controversia como la evacuación de pruebas y resolución de incidencias.

<sup>14</sup>En el marco de un proceso ante un Tribunal, los días de despacho son aquellos en los que éste tiene previsto dar atención al público

uno de los derechos otorgados en el artículo 28 de la Constitución, haciendo énfasis en lo concerniente a la Soberanía Nacional y la Seguridad de Estado, temas abordados por la Ley de Infogobierno. En tal sentido la Comisión Nacional de las Tecnologías de Información propiciar el espacio para que se inicie el procedimiento correspondiente a fin de que se dicte la norma correspondiente, dejando claro allí los organismos de prevención control y supervisión de la información, además de hacer la clasificación de tipos de información en : Publica, Privada, Mixta o de Estado. En este punto en particular se debería indicar también cuando no se podrá obtener información por Seguridad de la Nación, así como el uso y tratamiento que se la dará a la información que provenga de los Organismos del Estado.

### 4.3. Ley Especial Contra Delitos Informáticos (LECDI)

La evolución de las Tecnologías de la Información y la Comunicación ha transformado las estructuras sociales agilizando la interacción digitalizada de la comunidad internacional [8], el uso de aplicaciones que aumentan en gran medida el volumen y la cantidad de formas distintas en que se pueden dar relaciones que traen consigo una serie de riesgos y dificultades que atentan contra la seguridad de personas e instituciones públicas o privadas, abriendo la puerta a una serie de conductas desviadas o antisociales que se manifiestan en formas que no eran conocidas y que cada día van transformándose o adaptándose a los cambios de los sistemas tecnológicos con el objeto de alcanzar el fin que se han propuesto que puede ir desde causar daño (patrimonial o no), pasando por obtener benéficos de carácter económico, hasta llegar a el simple reconocimiento de un grupo de pares.

Los sistemas de información han sido usados de manera tal que permiten, el acceso indebido, el control ellos, el manejo de información táctica y de estrategias de seguridad del Estado y; el uso de técnicas informáticas y telemáticas de forma ilícita, dando lugar a los llamados Delitos Informáticos.

#### 4.3.1. Definición de Delito Informático

Resulta difícil acuñar una definición de delito informático que engrane a todos los elementos básicos para que se configure como tal, por cuanto no existe aún un criterio único para definirlo , ya que para algunos se trata de un nuevo delito y para otros no es más que una forma modificada de las figuras típicas de delitos tales como: los daños y perjuicios, hurto, fraude, estafa, sabotaje entre otros.

Sin embargo en [9] se conceptualizan cuatro posturas Doctrinarias frente a la definición de Delitos Informáticos, que permite agrupar los criterios según elementos en común:

1. **Los que tienen como elemento común el uso de la informática como método y como fin:** consideran que cualquier acto que ha utilizado la informática como método es penalmente perseguible, o que cuando la misma ha sido objeto o fin de dicha conducta, está puede ser denominada Delito Informático, según este criterio se entiende el Delito Informático como:

Todas aquellas conductas ilícitas sancionadas por el ordenamiento jurídico objetivo, donde se hace uso indebido de las computadoras como medio o instrumento para la comisión de un delito, y así mismo aquellas otras conductas que van dirigidas en contra de las computadoras convirtiendo éstas en su fin u objetivo [9].

Esta definición contempla conductas típicas y sancionadas muchos años antes de que surgiera la informática, así las cosas cualquier acto ilícito que use la Tecnología sería Delito Informático, sin tomar en consideración las circunstancias de hecho y las tipificaciones ya existentes. A juicio de [9] eso es un error pues pareciera que se trata de un tipo definible y tipificable *per sede* delitos, que emplean la tecnología como medio o como fin.

2. **Los que establecen la información o los datos procesados electrónicamente como bien protegible en los delitos informáticos:** Separa las figuras de delito clásicas del derecho penal de unos nuevos que surgen por las condiciones que genera la informática y la interacción social producto de ésta, la teoría pretende suscribir el delito Informático dentro de una nueva modalidad estableciendo diferencias claras y precisas entre éstos y las figuras ya existentes, otorgando la siguiente definición:

Toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable, y atente contra el soporte lógico de un sistema de procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados [9].

Para ellos la definición de Delito Informático lejos de ser nueva, no es más que la tipificación de delitos clásicos que emplean la informática como herramienta para perfeccionarlos.

3. **Los que niegan la existencia de un nuevo tipo de delito:** estos doctrinarios parten de la idea de la inexistencia de un nuevo ilícito, que pueda ser denominado delito informático y para ellos simplemente se trata de los mismos tipos penales ya existentes con ciertas variaciones que permiten su consumación, según éstos simplemente se requiere adecuar los tipos penales, pero nunca la creación de uno nuevo denominado delito informático. En tal sentido, en [9] se expresa que el delito informático no constituye una nueva categoría delictiva, sino que los hechos ilícitos se cometen mediante el empleo del computador y son en principio los mismos que desde hace miles de años fueron castigados, delitos contra la persona, el honor, la seguridad pública y de la nación, hurtos entre otros. Estos tipos, en algunos de los casos, muestran inadecuación con respecto de las nuevas modalidades; la postura planteada por estos doctrinarios no significa el desconocimiento del impacto de las nuevas tecnologías, sugiere mas bien, la necesidad de reformar las normas existentes en vista de las nuevas modalidades que han surgido.
4. **Teoría Ecléctica:** quienes la adoptan consideran que si bien pueden existir delitos, el bien jurídico protegido ésta por definirse, también creen que no pueden ser encuadrados dentro de los tipos penales ya conocidos.

En este caso se entenderá por delito informático, todo comportamiento ilícito que atente contra los sistemas de procesamiento de información o los datos procedentes de éstos, que pueda ser tipificado y sancionado por el Derecho penal.

#### 4.3.2. Clasificación de los Delitos Informáticos

Estos delitos pueden ser clasificados en dos tipos; **de resultado o de medio**. Los primeros están vinculados a aquellos hechos cuyo objeto es causar daño a los sistemas que usan tecnologías de la información, es decir aquellos donde el bien jurídico protegido es la información y su almacenamiento, tratamiento, procesamiento automatización y transmisión, un ejemplo de ellos es el robo, el hurto, y los daños tanto al sistema lógico como al físico. Tellez en Estrada 2008 indica que dentro de esta clasificación esta: la programación de instrucciones que producen un bloqueo total al sistema, la destrucción de programas por cualquier método, daño a los dispositivos de almacenamiento, el atentado físico contra la máquina o sus accesorios, el sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados, el secuestro de soportes magnéticos en los que figure información valiosa con fines de chantaje [10] Los segundos, de medio, son aquellos que usan las tecnologías de la información de forma indebida como único medio para ir en contra de bienes jurídicos protegidos [11], por ejemplo la clonación de una tarjeta, la estafa o el espionaje, la difamación, injuria y la violación a la privacidad de la información [9].

De la misma forma la ONU reconoce los siguientes tipos de delitos informáticos según la actividad <sup>15</sup>.

Fraudes cometidos mediante manipulación de computadoras:

- Manipulación de los datos de entrada
- Manipulación de programas
- Manipulación de datos de salida
- Fraudes por manipulación informática.

<sup>15</sup>Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente – Delitos relacionados con la informática; abril de 2000

En cuanto a las Falsificaciones Informáticas:

- Como objeto: Cuando se alteran datos de documentos almacenados en forma computarizada.
- Como instrumento: cuando son usadas las computadoras para alterar documentos a través de escáner u otros que permiten hacer copias de alta resolución.

En cuanto los daños o modificaciones de programas de datos computarizados:

- Sabotaje informático: suprimir o modificar funciones sin autorización, empleando técnicas tales como: Virus, Gusanos, Bombas lógicas o cronológicas, acceso no autorizado a servicios de sistemas informáticos, piratas o hackers.
- Reproducción no autorizada a programas informáticos de protección legal.

Esta clasificación ha servido de base para realizar las legislaciones en América Latina.

### 4.3.3. Características de los Delitos Informáticos

Los Delitos Informáticos se caracterizan según Tellez en Estrada 2008 [11] de la siguiente manera:

- Son un tipo delictivo configurado dentro de los delitos de cuello blanco, ya que sólo un número determinado de personas con conocimientos especiales en el área podrá ejecutarlos.
- Son delitos de tipo ocupacional, ya que en la mayoría de los casos se ejecutan por individuos desde sus lugares de trabajo.
- Se ejecutan en oportunidades determinadas que ofrecen un alto porcentaje de efectividad.
- Provocan fuertes pérdidas económicas
- La cifra negra<sup>16</sup> en torno a ellos es muy alta, es más el número de casos ejecutados que los denunciados, en vista de la falta de regulación o el desconocimiento de la población sobre ésta.
- Son muy sofisticados, suelen usarse para ataques militares o contra la seguridad de Estado.
- No son fáciles de comprobar, ameritan de la inspección o peritaje por parte de expertos.
- Ofrece facilidades para ser cometidas por niños, niñas o adolescentes.
- Cada vez se proliferan más, y se modifican con los avances tecnológicos.
- Son en su mayoría ilícitos impunes de manera manifiesta ante la Ley y el Estado.
- Ameritan de regulación más específica.
- Pueden ser perpetrados contra personas y instituciones de carácter público o privado.

Así las implicaciones del mal uso de las tecnológicas de la información y comunicación han hecho que se dicten regulaciones a fin de prevenir y sancionar las conductas contrarias al orden social, caracterizadas por una dinámica de interacción inicial muy democrática pero que con el paso de los años se fue convirtiendo en caótica por la expansión desmedida y poco controlada de las tecnologías de la información. Por ello las leyes, a raíz de estos hechos, fueron más de orden regulador y no sancionatorio, buscando principalmente respetar la libertad de expresión, y el principio de buena fe, es decir suponían que no se daría un uso que fuese en contrario al orden social establecido y menos aún en contra de los bienes socialmente protegidos. Dentro de las primeras normas de ese carácter está la Ley Modelo promulgada por la ONU, que regula el

<sup>16</sup>En éste contexto, el termino **cifra negra** se refiere, a la proporción de delitos que no es denunciada.

comercio electrónico, y que tiene por objeto dictar normas que unifiquen criterios en el derecho interno de los Estados integrantes, logrando su cometido ya que muchas de las normas relativas a la protección de los datos la emplean como fundamento, entre ellas la Ley de Mensajes de datos y Firmas Electrónicas Venezolana. De igual forma la Organización de Cooperación para el Desarrollo Económico promulgó normas de seguridad para los sistemas informáticos y el Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y tratamiento del Delincuente, realizado en Viena el año 2000, buscó investigar qué comportamiento delictivo puede producirse en un entorno electrónico y esbozar los tipos de delito previstos con respecto a las redes electrónicas internacionales y exploran las razones por las cuales esos delitos requieren atención y esfuerzos combinados internacionalmente 2000[11].

Como respuesta a una serie de eventos que se vinieron suscitando a finales de los años noventa, tal es el caso de la clonación de tarjetas de débito y crédito y recargos en facturas telefónicas por llamadas internacionales, en Venezuela se promulga la Ley Especial contra los Delitos Informáticos. Para aquel entonces, era clara la ausencia de leyes que pudieran dar respuesta a este tipo de infracciones, quedando en manos de los jueces la interpretación y adaptación de la norma existente a nuevos tipos penales. Estas interpretaciones carecían de sustento con respecto al principio de legalidad, ya que era casi imposible adaptar una conducta nueva a tipos penales que no fueron creados para ellas, se trataba de delitos diferentes y con recursos desconocidos por los administradores de justicia.

Es por ello que la Asamblea Nacional se plateó dentro la Comisión de Finanzas la creación de una subcomisión para el estudio del fraude electrónico, dando como resultado la mencionada Ley, cuya característica principal es que fue hecha de forma participativa, tal como lo indica la CRBV. Para ello se contó con el trabajo de un grupo de especialistas en lo legal, dedicado a hacer una revisión de las incitativas legislativas que en América Latina se habían venido llevando a cabo en materia de delitos informáticos, acompañados a su vez de expertos en el área Informática, y de representantes de los distintos sectores públicos y privados vinculados a las Tecnologías de la Información [11], dando como resultado una Ley que busca prevenir y no reaccionar contra los ilícitos, con la intención de dar respuesta no sólo a los hechos delictivos suscitados para aquel momento sino a aquellos que podrían llegarse a suscitar en el futuro, o de los que ya se conocía su existencia en otros países.

#### 4.3.4. Tipificaciones de la Ley Especial contra Delitos Informáticos

La Ley Especial Contra Delitos Informáticos<sup>17</sup> buscó plantear los tipos de delitos vinculados a las Tecnologías de Información haciendo una clasificación de los mismos de acuerdo al bien jurídico protegido, y lo hace de la siguiente forma:

- **Delitos contra los sistemas que usan Tecnologías de Información:** en este aparte de la Ley se encuentran tipificados los llamados **Delitos Informáticos de Resultado**, que fueron descritos anteriormente, para los cuales se establecen penas que van de uno a diez años de prisión y multas de 10 a 1000 Unidades Tributarias; son estos delitos los siguientes:
  - **El acceso indebido a los sistemas.**
  - **El sabotaje y daño a los sistemas.**
  - **El favorecimiento culposo del sabotaje o daño.**
  - **Agravantes para el delito de sabotaje y acceso indebido.**
  - **Los supuestos alternativos que prevé el uso de equipos para causar daño o sabotaje**
  - **El espionaje informático**, descrito en el artículo 11 de la Ley referido a la obtención, revelación o difusión de los datos o información mediante acceso indebido o privilegiado al sistema. Se trata del ataque hecho a la toda la base de datos o a una parte de ésta y no a capturar información específica sobre una persona, y usualmente se hace con fines comerciales.

<sup>17</sup>Ley especial contra delitos Informáticos Gaceta Oficial N°37.313 del 30 de octubre de 2001

- **La falsificación de documentos.** Es de importancia preponderante para el tema de la Identidad Digital. Este tipo prevé la falsificación de un documento no sólo con la alteración del contenido del mismo o de los datos que contiene, sino también plantea la posibilidad del ocultamiento del documento para que no sea encontrado oportunamente como parte de la falsificación a fin de obtener algún beneficio. Planteando para éste tipo dos agravantes, una cuando el sujeto activo actúa con el fin de obtener un beneficio para él o un tercero y la otra corresponde a si le causa daño a cualquier persona distinta a los sujetos activos en esta norma tipo [9].
- **Delitos contra la Propiedad:** esta clasificación de delitos y las siguientes que se hacen en la Ley están enmarcadas dentro del tipo de los **Delitos Informáticos de Medio**. Para algunos autores la técnica legislativa empleada en este aparte no es adecuada, ya que se trata de tipos ya establecidos en Código Penal Venezolano cuya única distinción es el medio empleado para la consumación y el bien tutelado, que en este caso puede ser intangible. Las penas establecidas para estos tipos van de uno a seis años de prisión y multas de 200 a 1000 Unidades Tributarias. Se encuentran dentro de esta clasificación:
  - **El hurto informático.** Se presenta cómo un tipo más amplio que el hurto tradicional planteado en el Código Penal ya que prevé el hurto de bienes tangible e intangibles<sup>18</sup>.
  - **El fraude,** Éste que no es similar al establecido en el Código Penal, ya que el sujeto activo no engaña la buena fe sino que manipula un sistema a fin de obtener un provecho injusto y en perjuicio de un tercero [12]. Dentro de este tipo se encuentran los vinculados con el manejo indebido de tarjetas inteligentes (de acceso, pago, crédito, débito, entre otras). En este particular se establecen modalidades vinculadas a las tarjetas inteligentes tales como:
    - Obtención indebida de bienes y servicios.
    - Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.
    - La apropiación de tarjetas inteligentes o análogos.
    - La provisión indebida de bienes y servicios.
    - La posesión de equipos de falsificación.
- **Delitos contra la privacidad de las personas y las comunicaciones:** se prevé aquí la protección de los Derechos Fundamentales vinculados a la privacidad y de está con relación a la protección de las comunicaciones, con penas de dos a seis años de prisión y multas de 200 a 600 Unidades Tributarias. Estos delitos están referidos a:
  - **La violación de la privacidad de los datos o información de carácter personal.** Prevé modalidades de posible invasión de la información que se encuentre en un computador o en sistemas entre las que se encuentra el acceso, la captura, la interceptación, la interferencia, la reproducción, la modificación, el desvío o eliminación de mensajes de datos o señales de transmisión o comunicación ajena; planteando como sujeto activo cualquier persona a la que no esté dirigida la comunicación y como sujeto pasivo las partes de la comunicación interceptada o grabada<sup>19</sup>.
  - **La violación de la privacidad de las comunicaciones.**
  - **La revelación indebida de datos o información de carácter personal.**
- **Delitos contra los Niños, Niños y Adolescentes:** Esta clasificación busca solventar los vacíos que existían previo al momento de la redacción de la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes. Establece penas de dos a seis años de prisión y multas de 200 a 600 Unidades tributarias, abordando el uso ilícito de la Tecnologías de la Información con el fin de:

<sup>18</sup>Bienes tangibles: Son todos aquellos bienes físicamente apreciables, es decir, que se pueden tocar y ocupan un espacio. Bienes intangibles: Son aquellos bienes que no poseen materialidad, por ejemplo una determinada marca comercial. <http://ibethgramajo.blogspot.com/2012/04/bienes-tangibles-e-intangibles.html> 25/07/2014

<sup>19</sup>Gaceta Oficial 39522. Ley Orgánica del Tribunal Supremo de Justicia, del 1ero de Octubre de 2010

- La difusión o exhibición de forma masiva y pública de material pornográfico,
  - La exhibición pornográfica de niños o adolescentes.
- **Delitos contra el orden económico:** establece penas de uno a cinco años de prisión y multas de 100 a 500 Unidades Tributarias, y estipula:
- La apropiación indebida de la propiedad intelectual.
  - Ofertas engañosas.

La LECDI además de las sanciones privativas de libertad y pecuniarias establece también penas accesorias tales como: comiso, trabajo comunitario, inhabilitación de funciones, suspensión de registro o permisos de operación.

En general esta Ley fue una novedad para el momento en que se promulgó, sin embargo aún cuando con ella se buscaba un ley previsiva, que pudiese ser útil con el pasar de los años, en vista de que los avances que materia de tecnologías de la información se dan constantemente, a la fecha resulta ser poco práctica ya que ha venido arrastrando con algunas deficiencias en las tipificaciones establecidas, que no han permitido que este instrumento jurídico proporcione la respuesta esperada ante los llamados Delitos Informáticos, ya que presenta algunos problemas de redacción jurídica que dan lugar a interpretaciones imprecisas por parte del Juzgador [11].

Es propicio entonces plantearse una reforma a la Ley, iniciativa en donde el Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología tenga un papel protagónico, a través de los distintos organismos que lo conforman, en conjunto con los administradores de justicia. Con ello se ha de velar entonces por obtener una Ley, que entre otras cosas tome en consideración la experiencia de Jueces, Fiscales, Defensores Públicos y Privados, así como de la sociedad en general, ya que hoy en día es ingenuo pensar que tan sólo algunos forman parte del sector Tecnología de la Información. Asimismo la redacción de la norma tipo debe cuidar el orden jurídico y técnico, además de ampliar la categorías de clasificación, donde necesariamente, debe existir un aparte dedicado a la Firma Electrónica, la Información y Comunicación, así como a la Seguridad de Estado y Soberanía Nacional, ampliando y mejorando también el aparte dedicado a la Privacidad, regulando el tan discutido tema del anonimato, además de plantear un sistema de colaboración de Justicia a nivel internacional ya que se trata, en muchos de los casos, de delitos cuyo sujeto activo no se encuentra en el territorio nacional.

#### 4.4. Decreto con fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas

Los nuevos patrones que han sido incorporados a la vida del venezolano por el uso de las nuevas Tecnologías de la Información, han resultado en la incorporación en el ámbito Jurídico de normas que permiten dar orden y regular la transferencia de mensajes de forma electrónica, tal es el caso del Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas<sup>20</sup>, Decreto-Ley que encontró fundamento legal en el decreto N° 825<sup>21</sup> en el que el Gobierno Bolivariano declara el acceso y uso de Internet como política pública prioritaria que potencia el desarrollo cultural, social y económico de la República, impulsando el intercambio de información no sólo entre organismos públicos sino entre éstos y particulares o simplemente entre particulares. Asimismo en el marco de la Ley Habilitante del año 2000<sup>22</sup> donde se le otorga al Presidente de la República la facultad, en el Artículo 1, numeral 5, literal b, para dictar medidas que: regulen la actividad informática, con el fin de otorgar seguridad jurídica para el desarrollo y expansión de las comunicaciones electrónicas; promuevan el uso y la seguridad del comercio electrónico y la transmisión de datos y; regulen el uso de la firma,

<sup>20</sup>Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas. Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.148, 28 de febrero de 2001

<sup>21</sup>Decreto N° 825 (sobre el Acceso y Uso de Internet), 10 de mayo de 2000. Gaceta Oficial de la República Bolivariana de Venezuela. Número 36.955, 22 de mayo de 2000.

<sup>22</sup>Ley que autoriza al Presidente de la República para dictar Decretos con Fuerza de Ley en las materias que se delegan. Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.076, 13 de noviembre de 2000. Reimpresa en su Sumario en la Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.077, 14 de noviembre de 2000.



tramitación y formalización de documentos digitales. En cumplimiento de esta disposición, fueron establecidos como responsables de realizar el Proyecto inicial de la Ley de Mensajes de Datos y Firmas electrónicas, a fin de ser presentado ante el Ejecutivo Nacional, a la Cámara Venezolano-Americana de Comercio e Industria, la Cámara Venezolana de Comercio Electrónico (CAVECOM-E) junto con el Ministerio de Ciencia y Tecnología (hoy Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología), tomando como referencia internacional para su concepción la Ley de Comercio Electrónico de 1999 de la República de Colombia, y en forma similar al caso de la Ley Especial contra los Delitos Informáticos, el Modelo de Ley de Comercio Electrónico de la Comisión de Naciones Unidas para Derecho Mercantil Internacional (CNUDMI/UNCITRAL) que tiene por objeto:

“posibilitar y facilitar el comercio por medios electrónicos ofreciendo a los legisladores un conjunto de reglas internacionalmente aceptables encaminadas a suprimir los obstáculos jurídicos y a dar una mayor previsibilidad al comercio electrónico. En particular, la Ley Modelo tiene la finalidad de superar los obstáculos que plantean las disposiciones legislativas y que no pueden modificarse mediante contrato equiparando el trato dado a la información sobre papel al trato dado a la información electrónica. Esa igualdad de tratamiento es esencial para hacer posibles las comunicaciones sin soporte de papel y para fomentar así la eficacia en el comercio internacional” Ley Modelo CNUDMI sobre Comercio Electrónico (1996) [13]

El resultado del trabajo conjunto entre los sectores vinculados a la materia del comercio electrónico y el Ejecutivo Nacional fue un Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas, en lo sucesivo LMDFE, que se constituyó en un verdadero avance jurídico, configurando una serie de disposiciones para que el mensaje de datos y la firma electrónica se encuentren regulados y tengan el mismo valor de instrumentos jurídicos y/o probatorios análogos ya existentes en el ordenamiento Nacional (Código Civil y Código de Procedimiento Civil). En tal sentido se establece en la exposición de motivos de la **LMDFE**, que es indispensable dar valor probatorio al uso de los medios electrónicos antes mencionados, en los procesos administrativos y judiciales, evitando así que sea el Juez quien considere la validez jurídica debido a la ausencia de una regulación expresa [9].

Se crea con esta Ley la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) que entra oficialmente en funcionamiento en enero de 2008 y cuyo objetivo es el de coordinar e implementar el modelo jerárquico de la Infraestructura Nacional de Certificación Electrónica, además de acreditar, supervisar y controlar a los Proveedores de Servicios de Certificación (PSC) y es a su vez el ente responsable de la Autoridad de Certificación Raíz del Estado Venezolano. Asimismo tiene como alcance proveer estándares y herramientas para implementar una tecnología de información óptima en las empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables<sup>23</sup>.

En líneas generales la LMDFE se guía por nueve principios, que son descritos brevemente a continuación:

- **Eficacia Probatoria:** busca otorgar seguridad jurídica a los mensajes de datos otorgándole el mismo valor probatorio de que se le da a los instrumentos escritos y su incorporación al proceso judicial semedante lo establecido en el Código de Procedimiento Civil para Pruebas Libres<sup>24</sup>. A este principio se le denomina también Regla de la Equidad Funcional, que busca equiparar los documentos con soporte electrónico a los documentos con soporte en papel, según Martínez 2000 en Peñaranda 2011 se trata de igualar la validez y los efectos de la firma electrónica a la manuscrita [14].
- **Neutralidad Tecnológica:** más que tratarse de neutralidad, este principio busca la posibilidad de que el Estado escoja el tipo de Tecnología que mejor se acople a las necesidades del mismo, por ende no se podría hablar de neutralidad cómo tal, mas bien se trata de utilidad Tecnológica. Es probable que en el momento de la redacción, y por el tipo de actores que desarrollaron el proyecto inicial, denominaron como neutralidad el emplear tecnologías útiles y adaptables a las necesidades propias de los venezolanos, sin embargo el concepto planteado en la exposición de motivos, cuando dice “se incluirán los desarrollos tecnológicos que se produzcan a futuro: A tal efecto sus normas serán desarrolladas e interpretadas progresivamente (...)” la Ley deja entrever que se trata de buscar la mejor opción, es pertinente entonces mencionar que la Ley de Infogobierno en el artículo 34 establece que:

<sup>23</sup><http://www.suscerte.gob.ve> 4/8/2014

<sup>24</sup> Artículo 365 del Código de Procedimiento Civil

.<sup>25</sup> desarrollo, adquisición, implementación y uso de las tecnologías de información por **el Poder Público**, tiene como base el conocimiento libre. En las actuaciones que se realicen con el uso de las tecnologías de información, sólo **empleará programas informáticos en software libre y estándares abiertos** para garantizar al Poder Público el control sobre las tecnologías de información empleadas y el acceso de las personas a los servicios prestados. Los programas informáticos que se empleen para la gestión de los servicios públicos prestados por el Poder Popular, a través de las tecnologías de información, deben ser en software libre y con estándares abiertos”.

En este sentido las tecnologías, empleadas por el Estado para la implementación de la LMDFE deberán desarrollarse bajo programas informáticos en software libre, con el fin de fomentar la independencia tecnológica y con ello fortalecer el ejercicio de la soberanía nacional, sobre la base del conocimiento y uso de las tecnologías de información libres en el Estado<sup>25</sup>.

Rico 2005 en [15] al respecto del Principio e Neutralidad Tecnológica indica lo siguiente:

“El legislador enfrenta dificultades al redactar normas que resultan absolutamente neutras tecnológicamente ya que el contenido y la estructura de las normas reguladoras , sobre todo en materia de firma electrónica, sigue los esquemas de clave pública basada en criptografía asimétrica, tal es el caso de la firma electrónica avanzada, la cual está basada en la actual tecnología de clave pública y por lo tanto se diferencia de la firma digital, siendo la firma electrónica avanzada<sup>26</sup>, la única que se equipara con la firma autógrafa”.

No asumir una tecnología determinada le permite al legislador no perder eficacia y efectividad con el pasar de los años, a diferencia de lo que ocurrió con otras normas en la materia. Sin embargo con la entrada en vigencia de la Ley de infogobierno, al menos en el caso del Estado Venezolano, deberán emplearse sistemas con **estándares abiertos**, aplicando así mismo las excepciones a que haya lugar.

- **Respeto a las formas documentales preexistentes:** la ley busca generar formas alternativas de validar los negocios o actos jurídicos, no pretende suplantar la firma manuscrita por la electrónica o alterar las formas ya existentes, simplemente le da validez jurídica a los mensajes de datos firmados electrónicamente.
- **Otorgamiento y reconocimiento jurídico de los mensajes de datos y firmas electrónicas:** con la entrada en vigencia del decreto LMDFE se asegura el reconocimiento jurídico de los mensajes de datos, firmas electrónicas y de los proveedores de servicios de certificación Nacionales e Internacionales, estableciendo claramente las funciones y obligaciones de los mismos.
- **Funcionamiento de las Firmas Electrónica:** establece un marco jurídico con los criterios fundamentales para otorgar validez a la firma y así asegura el adecuado funcionamiento de la misma.
- **No discriminación del mensaje de datos firmado electrónicamente:** se le otorga a la Firma electrónica el mismo valor de la firma manuscrita, con lo cual no se permite que la misma sea cuestionada por que se presente bajo formato de mensajes de datos, esto genera a su vez para el Estado el deber que crear medios que permitan crear confianza entre los ciudadano, abriendo con este principio la posibilidad de que aquellos que realicen negocios jurídicos por medios electrónicos tendrán la misma seguridad jurídica de aquellos que se hacen por escrito. Los artículos de la LDMFE 6 y 7 denotan muy bien este principio.
- **Libertad contractual:** las partes podrán realizar las negaciones por vía electrónica sin más limitaciones que las que establezcan las normas, a saber el Código de Comercio, Código Civil, entre otras.
- **Responsabilidad:** le permite a las ciudadanas y ciudadanos exceptuarse de responsabilidad sobre algún mensaje de datos, siempre que demuestren que han hecho lo necesario según las circunstancias, de igual manera los proveedores de servicios certificación pueden limitar su responsabilidad.

<sup>25</sup>Ley de Infogobierno Gaceta Oficial N°40.274 del 17 de octubre de 2013

<sup>26</sup>La firma avanzada esta basada de criptografía asimétrica, es decir que la persona que emite el mensaje tiene dos claves una pública, la cual debe ser accesible para todos, y una privada que sólo es conocida por el titular o incluso puede no ser conocida por éste y puede acceder a ella a través de un número de identificación personal. Rondón A Comentarios generales al Decreto ley de Mensaje de Datos y Firmas electrónicas de la República Bolivariana de Venezuela

#### 4.4.1. Los Mensajes de datos en la LDMFE

El Mensajes de Datos se ha definido como, cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones<sup>27</sup>.

De igual forma el artículo 2 de la LMDFE define mensaje de la siguiente manera:

“Toda Información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio.”

Esta es una definición muy amplia que a los efectos de la interpretación jurídica debe ser restringida, considerando que tal como lo explica [16], no toda información o manifestación realizada a través de la tecnología deriva en efecto jurídicos, como manifestación de la voluntad de los particulares.

El documento tradicionalmente conocido, se trata de un escrito impreso en papel en el que se consigna un hecho que deja constancia de manifestación de voluntad con características que producen efectos jurídicos [17], los mensajes de datos no se miden por la escritura, sino en unidades de información (denominadas Bytes) y de igual forma en ellos se puede dar una manifestación de voluntad produciendo los mismos efectos que un documento escrito.

#### 4.4.2. Eficacia probatoria

En este sentido la LMDFE, establece en su artículo 4 que los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, estableciendo que la promoción, control, contradicción, y evacuación se realizara conforme a lo previsto como pruebas libres en el Código de Procedimiento Civil. Ahora bien para que el mensaje de datos surta efecto como documento electrónico<sup>28</sup>, el mismo debe contener derechos y obligaciones exigibles entre los sujetos que intervienen en la relación; por lo que todo documento electrónico es siempre un mensaje de datos, pero no todo mensaje de datos puede ser considerado un documento electrónico [16].

El Código Civil Venezolano, en el artículo 1355, caracteriza la prueba por escrito<sup>29</sup> como “El instrumento redactado por las partes y contentivo de sus convenciones es sólo un medio probatorio; su validez o su nulidad no tiene ninguna influencia sobre la validez del hecho jurídico que está destinado a probar, salvo los casos en que el instrumento se requiera como solemnidad del acto”. Según 1.356. “La prueba por escrito resulta de un instrumento público o de un instrumento privado”. Según el art 1.357 CC se entiende por **Público** como el Instrumento público o auténtico es el que ha sido autorizado con las solemnidades legales por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para dar fe pública, en el lugar donde el instrumento se haya autorizado; y por su parte el instrumento de carácter de **privado** que se ha definido doctrinariamente como, el redactado por las partes interesadas, con testigos o sin ellos, pero sin intervención de registrador, notario u otro funcionario público que le de fe o autoridad.

Surge entonces la pregunta, ¿qué tipo de tratamiento se le dará al mensaje de datos, como documento público o privado?. A partir de la puesta en vigencia del Decreto con Fuerza de Ley de Registro Público y del Notariado los documentos firmados electrónicamente, usando un certificado emitido por un Proveedor de Servicios de Certificación PSC, que esté acreditado por la Superintendencia de Servicios de Certificación Electrónica (SUS-CERTE), tienen el mismo valor probatorio de los documentos públicos, ya que se reconoce la firma electrónica como análoga a la manuscrita de los registradores (as) y notarios (as)<sup>30</sup>. Asimismo el artículo 26 de la Ley de Infogobierno establece que “Los archivos y documentos electrónicos que emitan el Poder Público y el

<sup>27</sup> Artículo 2 Ley Especial Contra los Delitos Informáticos

<sup>28</sup> Documento electrónico; Documento digitalizado que contiene un dato, diseños o información acerca de un hecho o acto, capaz de causar efectos jurídicos. Ley de Infogobierno artículo 2 numeral sexto

<sup>29</sup> La legislación sustancial utiliza las expresiones documentos e instrumento como equivalente a documentos escritos y para denotar, particularmente, a los que encuentran firmados por sus autores. Bajo la denominación de prueba documental, se comprende primordialmente ese tipo de documentos, aunque las normas procesales pertinentes no excluyen los restantes objetos representativos anteriormente mencionados. Enciclopedia Jurídica <http://www.enciclopedia-juridica.biz14.com/d/documento/documento.html> consultado 22 de oct de 2014

<sup>30</sup> Artículo 24 de la Ley de Registros Públicos y del Notariado

Poder Popular, que contengan certificaciones y firmas electrónicas tienen la misma validez jurídica y eficacia probatoria que los archivos y documentos que consten en físico”.

Brewer y Superlano (2004) en [15] opinan que:

“...la valoración del documento electrónico es idéntica al documento tradicional. En consecuencia su valoración y eficacia como medio probatorio, será igual a la de cualquier documento convencional, sometido a las mismas reglas de apreciación y oposición que rige el sistema Venezolano. Su tasación como plena prueba o mero indicio probatorio, va a depender de las circunstancias y las formalidades bajo las cuales fue otorgado dicho documento, que serán las mismas normas existentes para el otorgamiento de los documentos ordinarios o contenidos en papel. Así el Documento público electrónico será valorado como el documento público ordinario, y el documento privado electrónico idéntico al documento privado convencional”.

Criterio este que es compartido por la autora del capítulo, el mensaje de datos reúne todos los requisitos para ser considerado documento público o privado, ya que en él se puede entre otras cosas manifestar la voluntad de las partes, no sólo para realizar un negocio jurídico sino para también perfeccionar cualquier acto jurídico que no amerite el contacto físico directo entre las partes, y dependerá de las circunstancias de hecho y de derecho, es decir de la naturaleza y origen de los actos que pretenda demostrar, el que se asuma como documento público haciendo prueba erga omnes o como documento privado, haciendo prueba entre las partes. Definir el mensaje de datos únicamente como un documento privado, tal como lo hacen varios autores, sería desconocer la intención del legislador al asociarlo a la firma electrónica avanzada, y crear SUSCERTE con el fin de regular primordialmente la actividad de los PSC, con el fin último de otorgarle a los ciudadanos seguridad jurídica mediante una Ley que regule formas electrónicas de intercambio y soporte de información a fin de garantizar las obligaciones asumidas mediante estos mecanismos<sup>31</sup>.

El mensaje también puede ser valorado con un rango inferior a la prueba por escrito en caso de que no contenga los elementos exigidos por LMDFE, no negando a aquellos que no estén firmados electrónicamente la posibilidad de servir como elemento probatorio. Salgueiro (2008) en [15] señala dos casos: a) un simple correo electrónico que no está asociado a una firma electrónica, el mismo podrá ser valorado por el Juez acompañado por otros elementos probatorios que sustenten el contenido. b) el mensaje impreso que tiene el mismo valor probatorio de las fotocopias.

De igual manera el artículo 4 de la LDMFE establece que; la promoción, control, contradicción y evacuación de los mensajes de datos como medio de prueba, se realizará conforme a lo previsto para las **Pruebas Libres** en el Código de Procedimiento Civil; esto permite que el mensaje de datos pueda trasladarse al expediente en otras formas además de la impresa, mediante la experticia, inspección judicial o experimento judicial, podrá llevarse por otros medios o formatos que determinan el contenido, alcance de aquello que se encuentra plasmado en el documento, para lo cual la parte interesada puede solicitarle al Juez su traslado a un lugar determinado donde se encuentre el sistema de almacenamiento que contenga el mensaje de datos[16].

También se podría solicitar una experticia y/o inspección asistida por expertos computacionales. El Centro Nacional de Informática Forense (CENIF)<sup>32</sup> juega un papel importante ya que es el organismo del Estado encargado del área, su misión es auxiliar a abogados, fiscales y jueces a identificar, preservar y analizar datos almacenados en medios magnéticos y transacciones electrónicas en un litigio judicial o extrajudicial; una vez hecha la valoración forense respectiva se dejará constancia de los elementos que interesan aclarar del mensaje de datos.

#### 4.4.3. Requisitos del Mensaje

Para que el mensaje de datos sea considerado de cualesquiera de las formas descritas **ut supra** deberá reunir una serie de requisitos que se plantean primordialmente en el artículo 7 de la LMDFE:

- Mantener la integridad del mensaje original.

<sup>31</sup>Exposición de motivos Decreto ley de Mensaje de Datos y Firmas electrónicas de la República Bolivariana de Venezuela

<sup>32</sup>El CENIF: es un laboratorio de informática forense para la adquisición, análisis, preservación y presentación de las evidencias relacionadas con la tecnologías de información y comunicación, con el objeto de prestar apoyo a los cuerpos de investigación judicial, órganos y entes del Estado que así lo requieran. <http://www.suscerte.gob.ve/cenif/>

- Que el contenido se mantenga disponible.
- Que el mensaje permanezca en el formato que fue generado.
- Que se conserven los datos que permitan determinar el origen, fecha, recepción y destino del mensaje.
- Que el mensaje permanezca íntegro, manteniéndose inalterable desde que se generó, excepto aquellos que hayan cambiado por procesos propios del sistema.

A su vez Rico (2005) en [15] identifica siete requisitos de veracidad y autenticidad que debe tener para que el documento electrónico sea considerado como medio de prueba:

- La calidad de los sistemas utilizados para la elaboración y almacenamiento del documento, lo que incluye hardware y software.
- Veracidad de la información. El contenido del mensaje remitido debe ser idéntico al del mensaje recibido por el destinatario.
- La conservación del mensaje de datos y la posibilidad de que éste sea recuperado.
- La legibilidad del documento electrónico.
- La posibilidad de identificar a los sujetos participantes y las operaciones realizadas por cada uno ellos en el proceso de elaboración del documento.
- La atribución a una persona determinada en calidad de autor (Autenticidad del mensaje), que se verifica mediante el uso de la firma electrónica.
- La fiabilidad de los sistemas utilizados para la autenticación del documento.

#### **4.4.4. La emisión y recepción de mensajes de datos**

Para que un mensaje de datos sea tomado como válido el receptor debe conocer quién es el signatario remitente para poder establecer las obligaciones que pueden surgir entre ellos. La LMDFE establece en el Capítulo III las normas de emisión y recepción de los mensajes de datos. Así las partes podrán establecer un procedimiento determinado para reconocer el mensaje como emitido, en caso de existir un desacuerdo entre el emisor y el receptor, se entenderá que el mensaje fue enviado cuando<sup>33</sup>:

- El mismo emisor signatario lo haya enviado.
- Una persona autorizada para actuar a nombre del emisor lo haya enviado.
- Un sistema de información ha sido programado por el emisor o bajo su autorización, para que envíe el mensaje de manera automática.

Con relación a la oportunidad de la emisión, el mensaje se tendrá por emitido cuando el emisor lo remita mediante un sistema de información al destinatario, salvo acuerdo contrario entre las partes.

Para la oportunidad de recepción, la LMDFE plantea varias reglas y se tendrá el mensaje por recibidos:

- En caso de que el destinatario cuente con un sistema de información para tales fines (recepción de mensajes) se tendrá por recibido en el momento en que ingrese al sistema.
- En caso de no existir tales sistema de recepción, se entenderá por recibido, salvo acuerdo contrario, en el momento en que el mensaje de datos ingresa a un sistema empleado por el destinatario frecuentemente para tales fines.

<sup>33</sup>Decreto con Fuerza de Ley Mensajes de Datos y Firmas Electrónicas(artículos del 9 al 15), Gaceta Oficial Nº 37148 del 28 de febrero de 2001

El lugar de emisión del mensaje de datos será aquel donde el emisor tenga su domicilio y el lugar de recepción el domicilio del destinatario, salvo prueba en contrario. En cualquiera de los casos, las partes podrán establecer reglas relativas a la emisión y recepción de los mensajes en lo concerniente a la verificación de la emisión, la oportunidad de la emisión, la determinación de la recepción y el acuse de recibo. En cuanto a esto último, el emisor podrá condicionar los efectos de un mensaje de datos a la recepción de un acuse de recibo emitido por el destinatario. Para ello las partes podrán acordar los mecanismos y métodos a utilizar y el plazo para la recepción del acuse de recibo; la no recepción del acuse de recibo en ese plazo implica a que se tenga el mensaje de datos como no emitido y en caso que las partes no haya acordado un plazo para esos efectos, el mensaje de datos se tendrá por no emitido si el destinatario no envía su acuse de recibo dentro de las 24 horas contadas a partir de la emisión del mensaje de datos.

#### 4.4.5. Confidencialidad de los mensajes de datos

La LMDFE establece que los mensajes de datos se regulará por los preceptos Constitucionales con el fin de garantizar el derecho de acceso a la información personal y a la privacidad, en este sentido el artículo 48 la Constitución de la República Bolivariana de Venezuela, establece:

“Se garantiza el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso”.

Argumentos estos que se concatenan con lo establecido en la Ley de Infogobierno en el artículo 25: “...el uso de las tecnologías de información por el Poder Público y el Poder Popular comprende la protección del honor, vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas; en consecuencia, está sujeto a las limitaciones que establezca la ley sobre la materia”, haciendo una analogía con el artículo 60 mencionado *ut supra*.

Queda claro que para que un mensaje de datos sea empleado válidamente en un acto jurídico de cualquier índole deberá respetar estos principios Constitucionales y cualquier violación a éstos acarreará las sanciones a las que haya lugar, y por ende el uso de ese mensaje de datos podrá ser refutado cómo inválido.

#### 4.5. La firma electrónica en la LMDFE

Con el fin de ofrecer garantía sobre los mensajes de datos en la LMDFE se establece la firma electrónica como un mecanismo de control y certificación de la información de importancia vital pues permitirá atribuir la autoría del acto jurídico, otorgándole validez y confiabilidad. En este sentido el artículo 16 de la Ley indica:

“La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y **atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa**”.

Según [15], la firma electrónica está referida al conjunto de datos electrónicos que identifican a una persona en concreto, datos éstos que están vinculados al documento que se envía por medios informáticos, tal como si se tratase de la firma manuscrita o autógrafa, con lo que el receptor tiene la seguridad de quién es el emisor del mensaje y que éste a su vez no se ha modificado de forma alguna.

La LMDFE la define como la “Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado”, de esta definición se desprenden varios elementos que deben ser considerados para otorgarle la validez y eficacia probatoria:

- La información se crea por quien emite el mensaje.
- La información estará vinculada a un mensaje de datos.
- Permite determinar quien es el autor del mensaje de datos.

Para Carrillo (2005) en [15] la firma electrónica que se regula en la LMDFE es la denominada firma electrónica avanzada, que permite identificar cualquier cambio que se haga sobre los datos, además de estar indefectiblemente vinculada al firmante y sus datos de creación. Mientras la firma autógrafa es una forma

de aceptación y reconocimiento del contenido de lo firmado en documento escrito, la firma electrónica busca otorgarle certeza a el contenido del documento electrónico o mensaje digital mediante métodos o tecnologías que se insertan dentro del contenido mismo, que además permiten determinar el origen del instrumento y consecuentemente se aceptan las condiciones y obligaciones jurídicas que allí se plasman [16].

#### 4.5.1. Diferencias entre la firma electrónica y la firma autógrafa

- La manera en que se estructuran es totalmente distinta.
- La firma electrónica se produce a través de un software.
- La firma autógrafa se produce por la manifestación de la voluntad.
- La firma electrónica siempre está asociada a un mensaje de datos o documento electrónico.
- La firma autógrafa siempre está asociada a un documento escrito e impreso en papel.

Sin embargo, a pesar de estas diferencias, la firma electrónica tiene los mismos efectos jurídicos y finalidad sobre los documentos electrónicos que la firma autógrafa sobre los escritos, pues a través de ésta se puede reconocer la autoría y aceptación de los mismos.

#### 4.5.2. Eficacia probatoria de la firma electrónica

El artículo 16 de la LMDFE establece los requisitos que debe tener la firma electrónica para que sea considerada válida [18]:

- Los datos empleados para generarla sólo pueden producirse una vez, asegurando confidencialidad; lo que significa que solo podrá existir una clave privada, evitando la duplicación de claves.
- Debe ofrecer las garantías suficientes de no ser falsificada o alterada con los avances tecnológicos, con el fin de que el mensaje de datos no sea modificado.
- No puede alterar el contenido del mensaje de datos asociada a ésta.

La firma electrónica que no cumpla con estos requisitos no podrá ser equiparada a la firma autógrafa, en cuyo caso, al igual a lo que se estable para el mensaje de datos, podrá servir como elemento de convicción o indicio conforme a las regla de la sana crítica, en cuyo caso el Juez podrá valorar la firma electrónica como presunción de autoría, siempre y cuando sea llevada como elemento probatorio en la oportunidad correspondiente. De igual forma la firma electrónica podrá ser sometida a los mecanismos de control y contradicción a los que se puede someter a la firma autógrafa, obviamente en este caso se hará mediante la experticia tecnológica que permita demostrar la autenticidad, autoría y veracidad de la misma. En tal sentido aquel mensaje de datos que esté vinculado a una firma electrónica debidamente certificada, permite determinar la identidad de las partes intervinientes en un acto jurídico, garantizando la confidencialidad e inalterabilidad por medios tecnológicos del contenido al que está asociada, teniendo éstos el mismo valor probatorio de los documentos escritos con la firma autógrafa<sup>34</sup> y se garantizará mediante la emisión del certificado electrónico, tal cómo lo establece el artículo 38 de la LMDFE.

#### 4.5.3. Obligaciones del signatario

El artículo 19 de la LMDFE establece una serie de responsabilidades y obligaciones que tendrá el signatario o emisor de la firma electrónica:

<sup>34</sup>Artículo 60 CRBV. “Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.”

- Actuar diligentemente con el fin de evitar el uso no autorizado de la firma electrónica, lo que implicaría entonces que la persona debería usar por ejemplo claves que no sean fáciles de identificar, además de modificarlas con cierta frecuencia.
- Notificar al proveedor de servicios de certificación sobre cualquier tipo de eventualidad, uso indebido, con respecto a la firma electrónica.
- Si el signatario o emisor no cumple con estas obligaciones será responsable de las consecuencias del uso no autorizado de la firma electrónica.

#### 4.5.4. Ventajas de la firma electrónica

En [15] se hace alusión a las principales ventajas de la firma electrónica con base a las características fundamentales que debe poseer:

- **Integridad de la información:** Permite detectar cualquier alteración que se haga sobre la información del mensaje de datos, durante los procesos de transferencia, almacenamiento o manipulación telemática, proporcionándole seguridad al usuario.
- **Autenticidad del mensaje de origen:** Garantiza la identidad del signatario del mensaje de datos, descartando la posibilidad de la captación o uso indebido de las contraseñas (ver sección 1.3.3) a través de la Internet.
- **No repudio en origen:** Es uno de los aspectos de seguridad de la firma electrónica ya que al usarla el emisor no puede negar haber enviado el mensaje de datos o haber realizado una determinada transacción, transformándose en un elemento de prueba inequívoco, ya que le otorga responsabilidad al emisor.
- **Imposibilidad de suplantarla:** La firma electrónica debidamente otorgada, por un PSC autorizado por SUSCERTE, al emisor o usuario final mediante los dispositivos electrónicos que contengan la información sobre las claves privadas (usado bajo el exclusivo control del signatario) evita la suplantación de la firma por parte de otro ciudadano(a).
- **Auditabilidad:** Permite el rastreo de las operaciones que se han llevado a cabo por parte del usuario, quedando registradas confiablemente la fecha y hora de las acciones ejecutadas, mediante el estampillado de tiempo (ver sección **subsubsección:estampilladoDeTiempo**).

#### 4.5.5. De SUSCERTE y los PSC

Con la puesta en marcha del Decreto con Fuerza de Ley de Mensajes Datos y Firmas Electrónicas se crea la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), que es un servicio desconcentrado sin personalidad jurídica, integrado a la estructura orgánica del entonces Ministerio del Poder Popular para la Ciencia, Tecnología e Innovación, hoy Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología, según Decreto N° 6.732 de fecha 2 de junio de 2009, publicado en Gaceta Oficial de la República Bolivariana de Venezuela N° 39.202 en fecha 17 de junio de 2009. Es el organismo encargado de coordinar e implementar el modelo jerárquico de la infraestructura Nacional de Certificación Electrónica, acreditando, supervisando y controlando a los Proveedores de Servicios de Certificación (PSC) tal como se establece en el artículo 21 de la LMDFE. Es además responsable de la Autoridad de Certificación Raíz del Estado Venezolano. Asimismo tiene como alcance proveer estándares y herramientas para implementar tecnologías de información óptimas en las empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables<sup>35</sup>.

Se establecen para ella las siguientes competencias<sup>36</sup>:

<sup>35</sup> <http://www.suscerte.gob.ve/quienes-somos/>

<sup>36</sup> Artículo 22 Decreto con Fuerza de Ley Mensajes de Datos y Firmas Electrónicas, Gaceta Oficial N° 37148 del 28 de febrero de 2001



- Otorgar o renovar acreditación a los PSC, una vez se cumplan los requisitos establecidos en la Ley y en el Reglamento de ésta del 14 de diciembre de 2004, publicado en la Gaceta Oficial N°38.086.
- Revocar o suspender la acreditación cuando se incumplan los requisitos y obligaciones que se establecen en la LMDFE.
- Mantener, procesar, clarificar, resguardar y custodiar el registro de PSC.
- Verificar que los Proveedores cumplan con todos los requisitos.
- Supervisar las actividades de los PSC.
- Liquidar, recaudar, administrar las tasas por acreditación, renovación, servicios certificación y de acreditación.
- Liquidar y recaudar multas.
- Administrar los recursos que le sean asignados o que obtengan por el ejercicio de sus funciones.
- Coordinar con organismos Nacionales e Internacionales las actividades relacionadas con el objeto de la LMDFE.
- Fiscalizar e Inspeccionar a los PSC.
- Iniciar de oficio o a instancia de parte, sustanciar y decidir sobre procedimientos administrativos vinculados a supuestas infracciones de la LMDFE
- Requerir todo aquella información que consideren necesaria a los PSC sobre los certificados que se han emitido y que estén relacionados con el ejercicio de sus funciones.
- Actuar como mediador en la solución de conflictos entre los PSC y sus usuarios, cuando así sea solicitado por las partes.
- Seleccionar expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.
- Imponer sanciones.
- Presentar informes ante la autoridad correspondiente, .
- Determinar la forma y alcance de los requisitos para ser PSC y obtener la respectiva acreditación, para lo cual se apoyará en el Reglamento creado para desarrollar la normativa de acreditación.

Los PSC serán entonces los encargados de emitir, revocar y suspender los certificados electrónicos, certiorándose de que éstos estén vinculados a una persona natural o jurídica con el fin de que el receptor pueda asociar inequívocamente el mensaje de datos al emisor. A su vez debe facilitar la creación del mayor número de firmas electrónicas, ofreciendo un archivo cronológico de las firmas certificadas, además la conservación de los mensajes de datos debe garantizar los certificados electrónicos proporcionado por proveedores de servicio extranjeros.

La Fundación Instituto de Ingeniería o PROCERT son los únicos que en Venezuela, a la fecha de esta publicación, pueden garantizar la validez y titularidad de los certificados. A continuación se listan algunos de los datos que contiene un certificado electrónico:

- Identificación del PSC que proporciona el Certificado Electrónico, indicando su domicilio y dirección electrónica.
- El código de identificación asignado al PSC por SUSCERTE.
- Identificación del titular del Certificado Electrónico, indicando su domicilio y dirección electrónica.

- Las fechas de inicio y vencimiento del período de vigencia del Certificado Electrónico.
- La Firma Electrónica del Signatario.
- Un serial único de identificación del Certificado Electrónico.
- Cualquier información relativa a las limitaciones de uso, vigencia y responsabilidad a las que esté sometido el Certificado Electrónico.

#### 4.5.6. Consideraciones finales

La Firma Electrónica se ha constituido como una forma para dar validez al documento electrónico, sin embargo la firma autógrafa incorpora con la escritura elementos propios del signatario que permiten determinar de manera fehaciente su autoría, permite a su vez el traslado y reconocimiento de ella en el exterior; la ausencia de elementos psicológicos es uno de las debilidades más profundas que enfrentan el documento que emplea la firma electrónica frente al documento tradicional.

En el ámbito del Derecho Penal el Código de Procedimiento Penal, establece como regla para las pruebas que sean apreciadas según **Libre Convicción Razonada**, que sería el aplicada al mensaje de datos y la firma electrónica; será la sana crítica la forma en que se valoraran, haciendo uso de la ciencia y la lógica<sup>37</sup>.

La LMDFE busca entonces dar validez a los Mensajes de Datos y a la Firma electrónicas, pues aún cuando no cumplan los requisitos necesarios para determinar su origen y certeza, pueden ser valorados por el juzgador desde las reglas de la sana crítica. Es evidente que con el transcurrir de los años los avances tecnológicos van reformando, a veces sin percibirlo, la norma **in comento** brinda seguridad jurídica, resguardando no sólo la seguridad y privacidad de los usuarios, que ahora tienen más confianza para celebrar actos jurídicos por vía electrónica. Sin embargo aún es muy ambigua, muchos de los conceptos que plantea y los procedimientos no están claros; después de catorce años es pertinente hacer una revisión y considerar el accionar jurídico en torno a ella, ya que al hacer una revisión de la Jurisprudencia vinculada a la materia ésta es muy escasa. Es de suponer que las políticas para difundir los beneficios de la aplicabilidad de la misma no han sido muy efectivas, ya que no es extraño encontrar, jueces, fiscales, defensores públicos y privados, que no sólo, desconocen el uso y aplicabilidad de la norma sino que le dan una errada interpretación, se trata de cambiar la forma tradicional de pensar -documento igual a un papel- y en este sentido debe darse un reimpulso a la LMDFE a fin de que cumpla realmente con el objeto para la que fue creada y sea empleada de una manera mucho más eficaz y eficiente.

#### 4.6. Ley de Infogobierno

En la Ley de Infogobierno (LDI)<sup>38</sup> se establecen las bases y lineamientos que rigen el uso de las tecnologías de la información y la comunicación tanto en el Poder Popular como en el Poder Público. Para ello plantea, entre otros fines, que ha de facilitarse el acceso a la información que las instituciones del Estado Venezolano ofrecen a las personas, establecerse condiciones que permiten mejorar los servicios que el Poder Público proporciona a las personas y promoverse el empoderamiento del Poder Popular. Esta ley desarrolla lo establecido en el artículo 110 de la CRBV al declarar el interés público de las tecnologías de información libres como instrumento para garantizar una adecuada gestión pública, profundizar la participación de la ciudadanía en los asuntos públicos, coadyuvar al empoderamiento del Poder Popular y con la consolidación de la seguridad, defensa y soberanía nacional.

“Con la aprobación de la Ley se abre un nuevo episodio en la lucha por el reconocimiento del saber como bien público. De acuerdo con el primer artículo de la Ley; la misma tiene por objeto: establecer los principios, bases y lineamientos que rigen el uso de las tecnologías de información en el Poder Público y el Poder Popular, para mejorar la gestión pública y los servicios que se prestan a las personas; impulsando la transparencia del sector

<sup>37</sup> Artículo 22 Código Orgánico Procesal Penal

<sup>38</sup> Gaceta Oficial de la República Bolivariana de Venezuela. Número 40.274, 17 de octubre de 2013.

público; la participación y el ejercicio pleno del derecho de soberanía; así como, promover el desarrollo de las tecnologías de información libres en el Estado; garantizar la independencia tecnológica; la apropiación social del conocimiento; así como la seguridad y defensa de la Nación”. [19]

Esta Ley se hace norma para los Órganos y Entes del Poder Público Nacional, Estatal y Municipal — en todos los niveles del Gobierno — así como en Distritos Metropolitanos, Dependencias Federales, el Banco Central de Venezuela, las Universidades y demás instituciones del sector universitario público, las organizaciones del Poder Popular y demás personas de Derecho Público Nacionales, Estadales, Distritales y Municipales. Ella tiene como principios rectores la igualdad, legalidad, transparencia y accesibilidad, entre otros, y establece que una de las bases para alcanzar sus fines es el desarrollo y consolidación de la Plataforma Nacional en tecnologías de la información y la comunicación para fortalecer el acercamiento entre el Estado y las ciudadanas o ciudadanos, apoyando la constitución de un nuevo modelo de organización que propicie el control social y la corresponsabilidad como esquema de interrelación. Asimismo, plantea el uso obligatorio de los servicios de certificación y firma electrónica para garantizar la integridad, confidencialidad, autenticidad, y disponibilidad de la información para que entonces ésta pueda ser considerada como documento público y tenga la misma validez probatoria de estos; también establece el carácter obligatorio del uso de las Tecnologías de Información en el ejercicio de las competencias del Poder Público<sup>39</sup>.

La ley de Infogobierno plantea el uso intensivo de las TIC para [20]:

- Racionalizar los tramites públicos mediante la celeridad y funcionalidad de los mismos.
- Reducir gastos operativos.
- Establecer un modelo que vincule y permita la interoperatividad de la información de las diferentes instituciones del gobierno hacia los ciudadanos.
- Fortalecer el trabajo cooperativo y colaborativo entre las instituciones del Estado.
- Garantizar la Seguridad de la Información y los Procesos en las dependencias de la Nación.
- Reducir la dependencia extranjera en materia Tecnológica, implementado desarrollos propios que respondan a las necesidades del Estado.
- Potenciar los servicios públicos en línea y el uso de las tecnologías de la Información en la Gestión Pública.

#### **4.6.1. Derechos que se otorgan en la Ley de Infogobierno**

Entre los derechos que se otorgan a las personas en la Ley de Infogobierno se encuentran los siguientes:

1. Dirigir peticiones al Poder Público y al Poder Popular mediante las Tecnologías de la Información.
2. Acceder a los documentos y expedientes propios.
3. Obtener información de la Administración Pública Nacional a través de medios electrónicos, siendo tarea del Poder Público garantizar la conservación, seguridad, integridad, autenticidad y — cuando es pertinente — la confidencialidad de los documentos manejados usando esos medios.
4. Participar, colaborar y promover en la promoción de los servicios y uso de las tecnologías de información libres.
5. Recibir protección a su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación mediante las limitaciones en el uso de las tecnologías de información conducentes a la protección de los datos personales.

<sup>39</sup>Ley de Infogobierno. Artículos 6, 24 y 26. Gaceta Oficial de la República Bolivariana de Venezuela. Número 40.274, 17 de octubre de 2013

#### 4.6.2. Uso del software libre en la Administración Pública Nacional

Con esta Ley se sustituye por completo el Decreto 3.390 sobre el uso de software libre en la Administración Pública Nacional (APN)<sup>40</sup> y así lo establece en su disposición derogatoria primera. En ese sentido, también establece lo siguiente:

##### *Del conocimiento libre*

**Artículo 34.** El desarrollo, adquisición, implementación y uso de las tecnologías de información por el Poder Público, tiene como base el conocimiento libre. En las actuaciones que se realicen con el uso de las tecnologías de información, **sólo empleará programas informáticos en software libre y estándares abiertos** para garantizar al Poder Público el control sobre las tecnologías de información empleadas y el acceso de las personas a los servicios prestados<sup>41 42</sup>.

Sin embargo, de acuerdo con lo que establece en el Artículo 66 de la misma ley, la Comisión Nacional de las Tecnologías de la Información — ente cuya creación, atribuciones y funcionamiento están establecidos en los Capítulos II y III de la ley — podrá autorizar la adquisición y el uso de software no libre (únicamente) **cuando no exista un programa desarrollado que lo sustituya**, o cuando se encuentre en **riesgo la Seguridad y Defensa de la Nación**.

Con esta Ley se sustituye por completo el Decreto 3390 sobre el uso de software libre en APN y así lo indica en la disposición derogatoria primera de la LDI estableciendo a su vez en el artículo 34<sup>43</sup>.

Del conocimiento libre: El desarrollo, adquisición, implementación y uso de las tecnologías de información por el Poder Público, tiene como base el conocimiento libre. En las actuaciones que se realicen con el uso de las tecnologías de información, **sólo empleará programas informáticos en software libre y estándares abiertos** para garantizar al Poder Público el control sobre las tecnologías de información empleadas y el acceso de las personas a los servicios prestados<sup>44</sup>.

Sin embargo de acuerdo con lo que establece en el Art. 66 de la Ley de Infogobierno, la nueva comisión Nacional de las Tecnologías de la Información podrá autorizar la adquisición y es el uso de software no libre (unicamente) **cuando no exista un programa desarrollado que lo sustituya**, o cuando se encuentre en **riesgo la Seguridad y la Defensa de la Nación**.

#### 4.6.3. Derecho y Garantía sobre el acceso a la información

En su Título V, Derecho y Garantía de las personas sobre el acceso a la información, la Ley de Infogobierno establece que toda la información contenida en los registros y registros del Poder Público y el Poder Popular es de carácter público, salvo cuando la información trate **sobre el honor, la vida privada, intimidad, propia imagen, confidencialidad y reputación de las personas o la seguridad y defensa de la Nación**<sup>45</sup>. En caso que cualesquiera ente u órgano del Poder Público o del Poder Popular requiera ese tipo de información de las personas deberá informarles:

1. Que la información será recolectada de forma automatizada.
2. Su propósito, uso y con quién será compartida.
3. Las opciones que tienen para ejercer su derecho de acceso, ratificación, supresión y oposición al uso de la referida información <sup>46</sup>.

<sup>40</sup>Decreto N° 3.390, 23 de diciembre de 2004. Gaceta Oficial de la República Bolivariana de Venezuela. Número 38.095, 28 de diciembre de 2004.

<sup>41</sup>Ley de Infogobierno. Artículo 34. Gaceta Oficial de la República Bolivariana de Venezuela. Número 40.274, 17 de octubre de 2013.

<sup>42</sup>Énfasis de la autora

<sup>43</sup>Ley de Infogobierno Gaceta Oficial N° 40274, de fecha 17 de agosto de 2014

<sup>44</sup>Artículo 34 Ley de Infogobierno Gaceta Oficial N° 40274, de fecha 17 de agosto de 2014

<sup>45</sup>Véase artículo 60 de la Ley de Infogobierno de la Constitución de la República Bolivariana de Venezuela.

<sup>46</sup>Véase Derecho de Habeas Data.

4. Las medidas de seguridad empleadas para proteger la información <sup>47</sup>.

#### 4.6.4. Sanciones que contempla Ley de Infogobierno

La Ley de Infogobierno en su Título VI, Régimen Sancionatorio, establece en su artículo 81 que: todas aquellas personas en el ejercicio de una función pública, incurren en responsabilidad, serán sancionadas por la Comisión Nacional de las Tecnologías de Información, según el procedimiento previsto establecido en la Ley Orgánica de Procedimientos Administrativos, con multa comprendida entre cincuenta Unidades Tributarias (50 U.T.) y quinientas Unidades Tributarias (500 U.T.), por las siguientes infracciones:

1. Omitan la elaboración, presentación o implementación del Plan Institucional de tecnologías de información, en los términos señalados en la presente Ley y en la normativa aplicable.
2. Cuando ordenen o autoricen el desarrollo, adquisición, implementación y uso de programas, equipos o servicios de tecnologías de información que no cumplan con las condiciones y términos establecidos en la presente Ley y normativa aplicable a la materia, sin previa autorización de la autoridad competente.
3. Cuando incumplan las normas instruccionales, normas técnicas y estándares dictados por la autoridad competente de conformidad con la ley.
4. Cuando no registre ante la autoridad competente los programas informáticos que utilicen o posean; su licenciamiento, código fuente y demás información y documentación de conformidad con la ley.
5. Cuando en sus actuaciones electrónicas, omitan el uso de certificados y firmas electrónicas<sup>48</sup>.
6. Cuando usen equipos o aplicaciones con soporte criptográfico sin la correspondiente aprobación, certificación y homologación de la autoridad competente.
7. Cuando altere un dato, información o documento suministrado por los servicios de información.
8. Cuando emplee para fines distintos a los solicitados, los datos, información o documentos obtenidos a través de un servicio de información.
9. Cuando niegue, obstaculice o retrase la prestación de un servicio de información.
10. Cuando niegue o suministre en forma incompleta o inexacta información sobre el uso de las tecnologías de información, seguridad informática o interoperabilidad.
11. Al exigir la consignación, en formato físico, de documentos que contengan datos de autoría, información o documentos que se intercambien electrónicamente.
12. Cuando incumplan los niveles de calidad establecidos para la prestación de los servicios de información.
13. Celebrar, por sí o por intermedio de terceros, acuerdos que tengan por objeto, el intercambio electrónico de datos, información o documentos con otros órganos o entes del Estado, sin la autorización previa de la autoridad competente”.

Nótese que este régimen sancionatorio de la Ley abarca, consolida, y contiene en sí mismo las normas, derechos y leyes desarrollados **en las secciones previas**: Derecho de *Habeas Data*, numerales 7mo, 8vo, 9no, 10mo; Ley de Mensajes de Datos y Firmas Electrónicas, numerales 5to y 6to; Ley Especial contra los delitos informáticos, numeral 13ero. Por otro lado, ella incluye en una sola norma los principios generales de todas aquellas que en materia de tecnologías de la información se han venido aplicando hasta la fecha.

<sup>47</sup>Ley de Infogobierno. Artículos 74 y 75. Gaceta Oficial de la República Bolivariana de Venezuela. Número 40.274, 17 de octubre de 2013

<sup>48</sup>Véase Ley de Mensaje de datos y Firma electrónica

En resumen, la Ley pretende establecer el Infogobierno como un eje transversal que fortalezca las políticas públicas que impulsen el alcance de los fines del Estado, mediante la integración de aspectos nacionales, sociales, políticos y económicos asociados con el uso de las Tecnologías de Información por parte del Poder Público y el Poder Popular; con ello procura impulsar un salto cualitativo en la Gestión Pública, promover la apropiación social del conocimiento, la seguridad y defensa de la Nación, la participación y ejercicio pleno del derecho de soberanía.

#### 4.7. Otras normas aplicables

##### 4.7.1. Decreto 825 del 10 de mayo de 2000

Es la base de las normas desarrolladas en materia de Tecnologías de Información y Comunicación en el Estado Venezolano, a partir de él fue declarado el acceso y uso de la Internet como política pública prioritaria; este decreto dispuso las directrices a seguir por la APN para que fuesen incorporadas las tecnologías de información y comunicación en todos los ámbitos del Estado. Él plantea el uso de la internet para el funcionamiento operativo de los Organismos Públicos tanto interna como externamente, además de indicar el uso preferente de ésta en las relaciones con los particulares y para la prestación de servicios comunitarios diversos, así como cualquier otro servicio que ofrezca facilidades y soluciones a las necesidades de las ciudadanas y los ciudadanos de la República<sup>49</sup>.

##### 4.7.2. Ley Orgánica para la Ciencia, Tecnología y Innovación

Establece los principios que deben orientar la ciencia, tecnología y la innovación en Venezuela, definiendo los lineamientos que han de seguir las políticas y estrategias del Estado en esta materia, con la implementación de mecanismos institucionales para el estímulo, fomento y promoción de la investigación y la apropiación social del conocimiento. En su artículo 18, sobre Tecnologías de Información, asigna a la autoridad nacional con competencia en materia de ciencia, tecnología, innovación y sus aplicaciones<sup>50</sup> la tarea de: establecer políticas para la generación de contenidos en la red, respetando la diversidad, así como el carácter multiétnico y pluricultural que caracteriza la sociedad venezolana; resguardar la inviolabilidad de la confidencial de los datos electrónicos obtenidos en el ejercicio de las funciones de los Órganos y Entes Públicos y; Democratizar el acceso a las tecnologías de información<sup>51</sup>.

##### 4.7.3. Ley Orgánica de la Administración Pública

Establece que los Órganos y Entes de la APN a fin de dar cumplimiento a los principios de: **celeridad, eficacia, imparcialidad, honestidad, transparencia, confianza y buena fe**, podrán incorporar tecnologías y emplear cualquier medio informático, electrónico o telemáticos para el cumplimiento de sus fines, su organización, funcionamiento y relación con las personas. Asimismo, establece que los documentos reproducidos por los medios antes mencionados gozan de la misma validez y eficacia del documento original siempre que se cumplan los requisitos que establece la ley y se garantice por que sean presentados de manera íntegra, inalterada y auténtica<sup>52</sup>. A su vez, el Reglamento de esta Ley plantea el fortalecimiento de la ciencia y la tecnología, incentivando las relaciones con y dentro de los distintos sectores productivos del país.

<sup>49</sup>Decreto N° 825 (sobre el Acceso y Uso de Internet), 10 de mayo de 2000. Gaceta Oficial de la República Bolivariana de Venezuela. N° 36.955, 22 de mayo de 2000.

<sup>50</sup>Actualmente el Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología.

<sup>51</sup>Ley Orgánica de Ciencia Tecnología e Innovación, Artículos 1 y 18. Gaceta Oficial N° 39575 del 16 de diciembre de 2010

<sup>52</sup>Decreto N° 6.217, 15 de julio de 2008. Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública. Artículos 11 y 151. Gaceta Oficial de la República Bolivariana de Venezuela. Número 5.890 Extraordinario, 31 de julio de 2008.

#### 4.7.4. Ley de Registro Público y del Notariado

Le da validez a la firma electrónica de los funcionarios investidos con la función de certificación, otorgándole el mismo valor de la firma autógrafa. Asimismo se plantea como objetivo la automatización de los sistemas de registro y notariado, buscando unificar los criterios de actuación de los Registros Civiles, Subalternos, Mercantiles, y Notarias Públicas<sup>53</sup>.

#### 4.7.5. Ley de Instituciones del Sector Bancario

Esta ley identifica en varios de sus artículos conductas ilícitas dentro del ámbito bancario, en donde se utiliza la informática como medio para obtener algún tipo de beneficio indebido, por ejemplo:

**Fraude Electrónico:** Quien mediante la manipulación de herramientas informáticas o análogos, con ánimo de obtener un beneficio de ella, efectuó una transferencia electrónica no consentida en perjuicio del banco, instituciones similares o de un usuario, será penado de 8 a 10 años de prisión, esta misma pena será aplicada a los trabajadores del banco que se vean involucrados en este tipo de delito.

**Apropiación de Información:** Quien a través de la informática haya manipulado o se haya apoderado de documentos, mensajes de correo electrónico o cualesquiera documentación que se encuentre en los archivos electrónicos de un banco o institución análoga será penado con prisión de 8 a 10 años, la misma pena aplicará para aquellos que se apoderen por los medios antes descritos de documentos, papeles o correos que reposen en los archivos del Banco, causando un perjuicio a la institución financiera.

**Violación al Secreto Bancario**<sup>54</sup>: Las instituciones Bancarias, su personal, y en general a todo ente con competencia en el ámbito bancario tiene prohibido suministrar a terceros cualquier información sobre las operaciones activas o pasivas con sus usuarias o usuarios, salvo que sean autorizados por ellas o ellos de forma escrita, o que sea a solicitud de los organismos establecidos en la Ley que regula la prevención de legitimación de capitales o de algunas de las personas que la Ley autoriza expresamente<sup>55</sup> para acceder a esa información reservada. Las personas que violen esta prohibición en beneficio propio o de un tercero serán penadas con prisión de ocho a diez años<sup>56</sup>.

Las Instituciones del Sector Bancario cuentan con el **Sistema de Información Central de Riesgos**, que registra todos los datos crediticios de los usuarios o clientes, es decir, centraliza la información de las carteras de crédito de los Bancos, registrando información sobre la identidad de las personas con créditos, que incluye actividad económica, financiera, garantías y respaldos dados por el deudor, clasificación de riesgo, tipo de crédito y estatus del mismo. En el caso de los tarjeta-habientes, se registra la información referente a su identidad, clasificación de riesgos, saldos, cuotas vencidas y cantidad de tarjetas. Toda esa información está destinada exclusivamente para el uso de los Bancos y entes autorizados por la Ley, o leyes especiales, [21] con las limitaciones establecidas en su artículo 90:

“(…)Queda terminantemente prohibido el uso del Sistema de Información Central de Riesgos para fines distintos a los previstos en esta Ley, incluyendo el ser requerido como requisito para tramitación de préstamos o créditos, aperturas de cuentas de ahorros o corrientes u otros instrumentos o modalidades de captación<sup>57</sup>.”

Este sistema debe servir exclusivamente entonces para organizar y analizar los datos que maneja para los fines que establece la Ley, y no para que se actúe en contra de las usuarias o usuarios, pues busca el uso correcto de la información con el fin de consultar la situación crediticia de las personas. En general, la información que el banco obtiene de sus usuarios debe ser completamente confidencial, con lo que no podrán enajenarla de modo alguno para un objeto distinto del que les fue otorgado, salvo las excepciones previstas en las leyes aplicables.

”Queda terminantemente prohibido el uso del Sistema de Información Central de Riesgos para fines distintos a los previstos en esta Ley, incluyendo el ser requerido como requisito para tramitación de préstamos o créditos, aperturas de cuentas de ahorros o corrientes u otros instrumentos o modalidades de captación<sup>58</sup>.”

<sup>53</sup>Ley De Registro Público y del Notariado de 27 de noviembre de 2001. Gaceta Oficial N° 37.333

<sup>54</sup>Título VI, de la Información. Capítulo III, Sigilo Bancario.

<sup>55</sup>Artículo 89, levantamiento del secreto bancario.

<sup>56</sup>Artículo 221, Revelación de Información.

<sup>57</sup>Artículo 90, Definición y uso del sistema.

<sup>58</sup>Ley de Instituciones del Sector Bancario . Gaceta Oficial N° 6.015 Extraordinario del 28 de diciembre de 2010

Este sistema debe servir exclusivamente entonces para organizar y analizar los datos que maneja para los fines que establece la Ley, y no para que se actúe en contra de las usuarias o usuarios, pues busca el uso correcto de la información con el fin de consultar la situación crediticia de las personas. En general, la información que el banco obtiene de sus usuarios debe ser completamente confidencial, con lo que no podrán enajenarla de modo alguno para un objeto distinto del que les fue otorgado, salvo las excepciones previstas en las leyes aplicables.

#### 4.7.6. Ley de Contrataciones Publicas

Los procedimientos que regula esta Ley<sup>59</sup> pueden hacerse a través de medios electrónicos<sup>60</sup>. En ella se busca incorporar las tecnologías de información y comunicación a fin de fortalecer el cumplimiento de los principios en los que se fundamenta, obteniendo como resultados procedimientos más ágiles, económicos y eficientes sin descuidar las garantías de seguridad y confidencialidad necesarias, de acuerdo a lo que establece su Artículo 79, transcrito a continuación:

“La modalidades de selección de contratistas previstas en esta Ley, pueden realizarse utilizando medios y dispositivos de tecnologías de información y comunicaciones que garanticen la transparencia, honestidad, eficiencia, igualdad, competencia, publicidad, autenticidad, seguridad jurídica y confidencialidad necesaria. A fin de garantizar estos principios, el órgano o ente contratante debe utilizar sistemas de seguridad que permitan el acceso de los participantes, el registro y almacenamiento de documentos en medios electrónicos o de funcionalidad similar a los procedimientos, lo cual deberá estar previsto en el pliego de contrataciones.”

No obstante, la Ley también establece<sup>61</sup> que el uso de medios electrónicos será de carácter optativo, en cumplimiento del principio de no exclusión o discriminación de base tecnológica.

Es claro que con estas disposiciones la norma busca facilitar que los procesos de contratación pública puedan realizarse en forma segura a través de medios electrónicos, por cuanto establece procedimientos que permitan determinar las obligaciones de las partes a fin de garantizar los derechos de quienes intervienen en él a través de esos medios.

#### 4.7.7. Código Orgánico Tributario

Este Código<sup>62</sup> permite que se empleen medios electrónicos o magnéticos para realizar distintas operaciones, además del pago de tributos por Internet, por cuanto así lo establece en su Título IV (de la Administración Tributaria), capítulo I (Facultades, Atribuciones, Funciones, y Deberes de la Administración Tributaria), Sección primera (Facultades, Atribuciones y Funciones Generales):

**Artículo 122.** Los documentos que emita la Administración Tributaria en cumplimiento de las facultades previstas en este Código o en otras Leyes y disposiciones de carácter **tributario, podrán ser elaborados mediante sistemas informáticos y se reputarán legítimos y válidos, salvo prueba en contrario.** La validez de dichos documentos se perfeccionará siempre que contenga los datos e información necesarios para la acertada comprensión de su origen y contenido, y **contengan el facsímil de la firma u otro mecanismo de identificación del funcionario**, que al efecto determine la Administración Tributaria.

Las copias o reproducciones de documentos, obtenidas por los sistemas informáticos que posea la Administración Tributaria, tienen el mismo valor probatorio que los originales, sin necesidad de cotejo con éstos, en tanto no sean objetadas por el interesado. En todos los casos, la documentación que se emita **por la aplicación de sistemas informáticos deberá estar respaldada por los documentos** que la originaron, los cuales serán conservados por la Administración Tributaria, hasta que hayan transcurrido dos (2) años posteriores a la fecha de vencimiento del lapso de la prescripción de la obligación tributaria. **La conservación de estos documentos se realizará con los medios que determinen las leyes especiales en la materia.**

**Artículo 125.** La Administración Tributaria podrá utilizar medios electrónicos o magnéticos para recibir, **notificar e intercambiar documentos, declaraciones, pagos o actos administrativos** y en general cualquier

<sup>59</sup>Ley de Contrataciones Públicas. Gaceta Oficial de la República Bolivariana de Venezuela. Número 39.503, 6 de septiembre de 2010.

<sup>60</sup>Título III, Modalidades de selección de contratistas. Capítulo VII, Contrataciones Electrónicas.

<sup>61</sup>Artículo 81. Carácter optativo.

<sup>62</sup>Código Orgánico Tributario. Gaceta Oficial de la República Bolivariana de Venezuela. Número 37.305, 17 de octubre de 2011.



información. A tal efecto, se tendrá como **válida en los procesos administrativos**, contenciosos o ejecutivos, la certificación que de tales documentos, declaraciones, pagos o actos administrativos, realice la Administración Tributaria, siempre que demuestre que la recepción, notificación o intercambio de los mismos se ha efectuado a través de medios electrónicos o magnéticos.

**Artículo 162.** Las notificaciones se practicarán, sin orden de prelación, en alguna de estas formas: Por correspondencia postal efectuada mediante correo público o privado, por sistemas de comunicación telegráficos, facsimilares, electrónicos y similares siempre que se deje constancia en el expediente de su recepción. Cuando la notificación **se practique mediante sistemas facsimilares o electrónicos, la Administración Tributaria convendrá con el contribuyente o responsable la definición de un domicilio facsimilar o electrónico.**

El legislador busca con estas normas modernizar y actualizar la infraestructura tecnológica de Instituciones administrativas encargadas del sector tributario, implementando para ello mecanismos que fortalezcan el sistema, con el fin de incrementar el control del cumplimiento de las obligaciones tributarias, así como facilitar las operaciones del comercio.

#### **4.8. Legislación Internacional en el Marco de las tecnologías de la información**

El propósito de esta sección es dar una visión general del marco jurídico planteado internacionalmente en relación a las TI con el objeto de comprender la orientación que se ha dado en materia legislativa. Se irán presentando en primer lugar iniciativas que se han empleado como base para el desarrollo de normas y leyes en varios países del mundo así como en el desarrollo de la normativa en la República Bolivariana de Venezuela, para luego pasar a revisar los casos particulares de algunos países.

##### **4.8.1. Convenio Europeo para la protección de los Derechos Humanos y de las Libertades fundamentales**

Busca proteger los derechos y libertades fundamentales de los ciudadanos Europeos y para ello procura, entre otras cosas, resguardar la información personal que ellas o ellos proporcionen a través de la Internet a empresas, filiales u organismos gubernamentales y no gubernamentales cuyas sedes se encuentren físicamente localizados dentro del Continente Europeo o que tengan sus servidores fuera de países miembros de la Unión Europea [22].

##### **4.8.2. Iniciativa Internacional para la protección del consumidor en el marco del Comercio Electrónico**

Adoptada por la Unión Europea en 1999, sirvió como modelo a los Estados Unidos de Norteamérica y a los países miembros de la Organización para la Cooperación y el Desarrollo Económicos (OECD por sus siglas en inglés). Ella desarrolla lineamientos que sirven de base: “A los gobiernos para la revisión, formulación e implantación de leyes, prácticas, políticas y regulaciones en materia de consumo, para lograr una efectiva protección del consumidor en el contexto del comercio electrónico; a las asociaciones empresariales, grupos de consumidores y organismos autorregulatorios, proporcionándoles la orientación relativa a los principios básicos que deben considerarse en la formulación e instrumentación de esquemas en el contexto del comercio electrónico; de manera individual a los empresarios y consumidores involucrados en el comercio electrónico, proporcionándoles una clara guía sobre las características fundamentales que debe contener la información que se difunda por este medio, así como de las prácticas comerciales equitativas que los empresarios deben realizar y que los consumidores tienen derecho a recibir en el contexto del comercio electrónico” [23].

##### **4.8.3. Ley Modelo de la CNUDMI sobre Comercio Electrónico (Law on electronic commerce UNCITRAL)**

Elaborada por la Comisión de las Naciones Unidas para el derecho mercantil internacional CNUDMI (o UNCITRAL, por su siglas en inglés), fue adoptada por las Naciones Unidas en 1996. Este modelo de ley busca

brindar mayor seguridad en el marco del Comercio Electrónico, estipulando entre otros aspectos las formas de validez de un contrato electrónico.

“Los objetivos de la Ley Modelo, entre los que figuran el de permitir o facilitar el empleo del comercio electrónico y el de conceder igualdad de trato a los usuarios de mensajes consignados sobre un soporte informático que a los usuarios de la documentación consignada sobre papel, son esenciales para promover la economía y la eficiencia del comercio internacional. Al incorporar a su derecho interno los procedimientos prescritos por la Ley Modelo para todo supuesto en el que las partes opten por emplear medios electrónicos de comunicación, un Estado estará creando un entorno legal neutro para todo medio técnicamente viable de comunicación comercial<sup>63</sup>.”

Este modelo establece como uno de sus aportes más importantes que la información no puede refutarse como inválida o negarle sus efectos legales solamente por que sea presentada en formato digital. Entre los países que adoptan la Ley Modelo de la CNUDMI sobre Comercio Electrónico están Colombia (1999), México (2000), Panamá y la República Bolivariana de Venezuela (2001), República Dominicana y Ecuador (2002). En líneas generales esta Ley Modelo sirve de base para legislar en materia de comercio electrónico, firmas electrónicas, certificación digital y validez del documento electrónico [24].

#### **4.8.4. Ley Modelo de la CNUDMI sobre Firmas Electrónicas (Law on electronic signature UNCITRAL) del 2001**

Establece una presunción en donde, cuando se alcanzan algunos criterios técnicos mínimos planteados en los compromisos en cuanto a la firma electrónica, a partir de ellos está debe ser considerada igual que a la firma autógrafa u original. La definición para los criterios ésta conformada de una forma que se de bajo un enfoque técnico imparcial, es decir que no potencie o favorezca a ningún tipo de tecnología. Entre los países que han tomado como base este modelo están, Colombia (1999), Argentina (2001) Ecuador (2002) [24], y la República Bolivariana de Venezuela (2001).

En líneas generales, las iniciativas de las Naciones Unidas en las conferencias sobre comercio y desarrollo en los años 90 introdujeron algunas leyes modelo que aún hoy marcan pauta importante en el desarrollo de las legislaciones en materia de Seguridad Informática, el cual ha seguido los criterios empleados en los modelos haciendo las adaptaciones pertinentes, según sean aplicables a la particularidad de cada región.

#### **4.8.5. España**

En el año 1978 aparecen en la Constitución Española limitaciones sobre el uso de la información para garantizar el honor, la intimidad personal y familiar de los ciudadanos. Posteriormente en 1992 es promulgada la Ley Orgánica cinco 05 que regula el tratamiento automatizado de los datos de carácter personal y su objeto principal es la protección de éstos [24]. Por su parte, el código Penal Español incluye normas en torno a la estafa electrónica, tipificando en ellas sólo el ánimo del lucro valiéndose de medios informáticos. Con esto, todos los delitos informáticos son sancionados con analogía a los delitos comunes desde la promulgación de la Ley Orgánica 10/1995 del 23 de noviembre de 1995, publicada en el Boletín Oficial del Estado (BOE) N° 281 del 24 de noviembre de 1995<sup>64</sup> Según Baturones (2008) y Urdaneta (2010), la ley 34/2002 sobre los servicios de la Sociedad de la Información y del Comercio Electrónico y la ley 59/2003 de Firma Electrónica indican que el soporte electrónico en el que conste un contrato celebrado por vía electrónica será admisible como prueba documental y de igual manera el documento firmado electrónicamente, sin embargo para que éstos sean tomados como válidos se comprobarán los requisitos establecidos por la Ley, disposiciones similares a las establecidas en la Ley de Mensajes de Datos y Firmas Electrónicas Venezolana [15].

<sup>63</sup>Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno 1996 con el nuevo artículo 5 bis aprobado en 1998. Sección A.6 del capítulo I (Introducción) de la Guía. [http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453.S\\_Ebook.pdf](http://www.uncitral.org/pdf/spanish/texts/electcom/05-89453.S_Ebook.pdf)

<sup>64</sup><http://prezi.com/r1p2nz4yr6gr/legislacion-de-espana-en-materia-de-derecho-informatico/documento> en línea consultado el 19/08/2014

#### 4.8.6. Alemania

La Ley sobre la Criminalidad Económica de 1986, contempló delitos tales como: espionaje de datos, estafa informática, falsificación de datos probatorios, alteración de datos, sabotaje informático. Además cuenta con la Ley Federal de Protección de Datos [23]. También cuentan con la Ley Alemana de Firma Digital de 1997.

#### 4.8.7. México

El Código Civil Federal, Código de Procedimientos Civiles y el Código de Comercio, incluyen disposiciones en materia de comercio electrónico, referidas a la integración y consentimiento de obligaciones cuando se utilizan instrumentos electrónicos. El decreto 29/5/2000 reforma el Código de Comercio para que la Firma Electrónica tenga valor jurídico. En ese sentido, para que ésta tenga validez debe ser atribuible a las personas obligadas y ser accesible para su posterior consulta [23]. Con relación al Gobierno Electrónico poseen la Ley de adquisición de arrendamiento y servicios del Sector Público, siendo los Órganos Rectores en la materia la Unidad de Gobierno Electrónico y política de tecnologías de la información de la Secretaría de la Función Pública y la Comisión Intersecretarial para el desarrollo del Gobierno Electrónico [24]. Asimismo el Código Penal Mexicano de año 1999 en el aparte correspondiente a los delitos contra el patrimonio prevé el delito informático.

#### 4.8.8. Colombia

El artículo 15 de la Constitución reconoce el *Habeas Data* como un Derecho Fundamental no reglamentado [23]. Según [15] en la Ley 527 se modifica el Código de Procedimiento Civil Colombiano y se reglamenta el acceso y uso de los mensajes de datos además de su fuerza probatoria, el comercio electrónico, las firmas digitales y se promueven también las entidades de certificación. Con relación a los delitos informáticos, la Ley 679 sobre pornografía infantil en redes globales dispone medidas de protección contra la explotación, la pornografía, el turismo sexual y cualquier otra forma de explotación infantil, sin embargo el Código Penal Colombiano del año 2000 no hace referencia a los delitos informáticos como se les conoce en estos momentos en Venezuela [24]. En el ámbito del Gobierno Electrónico Colombia tiene una amplia legislación en donde se encuentra: la Ley 962 de 2005 que dicta disposiciones sobre la racionalización de los trámites administrativos y los organismos del Estado; el documento 30 72 que consagra la agenda de Conectividad como Política de Estado y; la resolución 17 40 que fija parámetros para la calidad de las telecomunicaciones.

#### 4.8.9. Brasil

El *Habeas Data* es recogido en la Constitución de la República Federativa del Brasil de 1988, como un recurso especial en instancia Constitucional, para conocer la información de la persona solicitante que constara en registros públicos de las entidades gubernamentales. Con respecto a la Firma Electrónica y el Mensaje de Datos, se instaura el modelo de llave pública mediante la medida provisoria 2200-2. En relación a los Delitos Informáticos, el uso ilícito de los ordenadores para divulgar programas que permitan poseer información contable sobre la Hacienda Pública sería penado mediante la Ley 8137, asimismo la Ley 9100 pena el acceso a bancos de datos [24].

#### 4.8.10. Argentina

La reforma en el Código Penal del 2008 establece tipos penales como: Pornografía Infantil por la Internet u otros medios similares, el apoderamiento, desvío e interceptación de comunicaciones electrónicas, acceso ilícito a un sistema de Datos Informáticos, daño y fraude informático. A su vez posee una Ley de *Habeas Data* que regula todo lo referente al acceso a la información personal. El decreto 378/2005 establece el plan Nacional de Gobierno Electrónico, que dicta los lineamientos a seguir en la materia en el Estado Argentino; en relación a la Firma Electrónica, la Ley 25506 establece entre otras cosas, que si la firma es desconocida por

el titular corresponderá a quien la invoca, acreditarla, asimismo los decretos 2628 y 724 se hable en ellos de una presunción de **iuris tantum** con relación a la validez de estas [24].

#### 4.8.11. Cuba

Poseen un reglamento de seguridad informática de 1996, que estipula en líneas generales que todos los Entes del Estado deberán analizar y confeccionar un plan de seguridad informática y contingencia. De igual forma cuentan con el reglamento sobre la protección y la seguridad técnica de los sistemas informáticos emitida por el Ministerio de la Industria Sideromecánica y la Electrónica.

#### 4.8.12. Consideraciones Finales

Como se pudo constatar, la mayor parte de los países aquí reflejados siguen pautas similares a las del Estado Venezolano, unos con normativas más específicas pero que buscan el mismo fin que las de Venezuela. Ésto se debe en esencia a que todos toman como fundamento los Modelos de Ley de la (CNUDMI), sin embargo es prudente para las futuras reformas en el ordenamiento jurídico nacional que se haga el estudio comparado de las Leyes que en esta materia tienen tradición jurídica. Si bien es cierto que los países de Europa han avanzado considerablemente con respecto a la regulación de la TI, no es menos cierto que en América Latina en las dos últimas décadas se han dado pasos agigantados que han establecido bases claras para mejorar las prácticas en la materia.

### 4.9. Conclusiones

Las Tecnologías de la Información han traído como una de sus tantas consecuencias la necesidad de generar métodos que regulen las relaciones de las personas naturales y jurídicas con éstas, con el pasar de los días hay más información y se generan nuevas aplicaciones, software y hardware que pueden ser empleados en beneficio o detrimento de la sociedad en general. Venezuela cuenta en este momento con una plataforma legislativa que le permitirá obtener mejores resultados en el ámbito de la regulación de las Tecnologías de la Información y, específicamente en lo que a Identidad Digital se refiere, si bien es cierto que las TI siempre irán algunos pasos adelante de las legislaciones en torno a ellas — en vista de que sus avances y los usos que se les dan son poco predecibles, además que lo que hoy se emplea a favor de la sociedad por estos medios mañana podría emplearse en su contra y a favor de unos pocos — no es menos cierto que los estilos legislativos deben potenciar formas amplias que le permitan mantenerse por periodos prolongados de tiempo sin que éstas puedan ser consideradas obsoletas e inaplicables. Para el caso Venezolano se cumple medianamente con ello, en opinión de la autora deberían generarse reglamentos específicos y procedimentales sobre: el Habeas Data, LECDI, LMDFE; así las cosas en el caso de la Ley de Infogobierno sería prudente que las comisiones que allí se crean sean nombradas a la brevedad del caso a fin de evitar entre otras cosas interpretaciones erradas sobre la Ley, permitiendo con esta designación que el uso que se le de sea el adecuado, permitiendo entonces que una norma que a todas luces se plantea como objeto mejorar las relaciones Estado/Ciudadano a fin desarrollar los servicios públicos y aumentar la credibilidad-transparencia del gobierno. Por otro lado el asunto de las políticas públicas y/o criminales que se tomen alrededor de las normas constituyen un elemento trascendental, ya que a pesar que en la mayor parte de los casos las leyes en materia de TI tienen mas de una década de promulgadas, pareciera que hay un desconocimiento técnico de la regulación debido a la posible falta de formación por parte de los actores del aparato de justicia, dígame Jueces, Defensores Públicos, Fiscales y Abogados, junto a esto se encuentra que las normas parecieran no hacer el énfasis adecuado en el peritaje forense que es un elemento estratégico para la interpretación y aplicación adecuada de las leyes en este ámbito.

Volviendo al Tema de las políticas de Estado para mejorar las relaciones ciudadanos/información/medios tecnológicos es prudente encontrar formas que permitan tener un mayor y mejor control de la información almacenada en en las distintas bases de datos, sería interesante entonces retomar la idea de la Cédula Electrónica, que entre alguna de sus ventajas tendrá el que: la clave de garantía estará en la base de datos, podría afiliar la firma electrónica, toda la información del ciudadano se encontrará en un solo documento, permitirá saber

con exactitud quién eres y evitará falsificación, pues los datos pueden ser cruzados y verificados de inmediato, evitará tramites administrativos y papeleos innecesarios; por otro lado el Estado Venezolano cuenta con la infraestructura tecnológica necesaria para la puesta en marcha de la misma, para lo cual el Ministerio del Poder Popular para Educación Universitaria, Ciencia y Tecnología puede junto con el Ministerio del Poder Popular para Relaciones Interiores, Justicia y Paz hacer alianzas que garanticen una cédula de calidad, segura y eficaz que de garantía a los actos jurídicos emanados de éstas y que pueda ser tomada como fundamento internacional para otras iniciativas.

## REFERENCIAS

---

1. R. Chalbaud. Derechos humanos y su protección constitucional, 2013.
2. M. Oberto and M. Govea. Algunas consideraciones sobre Habeas Data. *Revista Telematique*, 7(3), 2008.
3. Horacio Fernandez Delpech. Ley del estado de Utah sobre la Firma Digital. Código Comentado. Título 46, Capítulo 3, 1996.
4. A. Paredes. Transformación de la cultura de servicios de información: una visión legal y de tecnologías. *Enl@ce revista Venezolana de Información, Tecnología y Conocimiento*, 5, 2008.
5. E. Salazar. Habeas data en el derecho comparado. *Anuario del Instituto de Derecho Comparado de la Universidad de Carabobo*, 2006.
6. Endira Mora et. al. Gestión de anonimato. [https://tibisay.cenditel.gob.ve/gestionanonimato/wiki/PlanDeTrabajo %3A](https://tibisay.cenditel.gob.ve/gestionanonimato/wiki/PlanDeTrabajo%3A), 2014.
7. Pedro Bracho. Jurisprudencia. Concepto y Características. <http://es.scribd.com/doc/81250967/JURISPRUDENCIA-Concepto-y-Characteristicas>, 2010.
8. Zagarra R. Marco. *Marco Legal de las Tecnologías de la Información y comunicación*. 2010.
9. F. Fuentes. *Marco Legal de la Informática y la computación*. Vadell Hermanos, 2007.
10. Beatriz Di Totto. Delitos informáticos. <http://www.universidadabierta.edu.mx>.
11. René De Sola. Los tipos penales en la Ley Especial contra Delitos Informáticos. <http://beatrizditotto.net/2010/01/01/introduccion/>.
12. Fuentes F. Logreria, C. *Análisis critico de la tipicidad prevista en algunos artículos de la Ley Especial Contra Delitos Informáticos Venezolana*. Revista Electrónica de Estudios Telemáticos URBE, 2008.
13. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno, 1996.
14. Héctor R. Peñaranda, H. *La Firma Electrónica Digital en Venezuela*. Universidad del Zulia, 2011.
15. José V. Urdaneta B. *Los Mensajes de Datos y la Firma Electrónica (Seguridad Jurídica que ofrecen y Valor Probatorio)*. ACADEMIA DE CIENCIAS POLÍTICAS Y SOCIALES, 2010.
16. G. Odreman. *Eficacia Probatoria del mensaje de datos y de la Firma electrónica según la nueva Ley de Mensaje de Datos y Firmas Electrónicas*. UCAB, 2003.

17. R. Lonrenzett. *Comercio Electrónico*. Abeledo-Perrot, 2000.
18. A. Rondón. Comentarios generales al Decreto ley de Mensaje de Datos y Firmas electrónicas de la República Bolivariana de Venezuela. *Revista de la Facultad de Ciencias Jurídicas y Políticas*, 2002.
19. M. Montilla and S. Roca. Ley de Infogobierno. *Revista El Clic*, 6, 2013.
20. UCV. Gobierno electrónico, 2014.
21. C. Colina. *Seducir y Controlar*. UCV, 2005.
22. Cristos Velasco. Privacidad y Protección de Datos Personales en Internet, ¿Es necesario contar con una regulación específica en México? *Boletín de Política Informática I*, 2003.
23. L. Flores. *Derecho Informático*. Grupo Editorial Patria, 2009.
24. J. Gamba. *Panorama del derecho Informático en América Latina y el Caribe*. CEPAL, 2010.



# APORTES EN CERTIFICACIÓN ELECTRÓNICA Y ANONIMATO

---





## DESARROLLO DE UNA APLICACIÓN PARA GESTIÓN DE UNA AUTORIDAD DE CERTIFICACIÓN RAÍZ BAJO ESTÁNDAR X.509 UTILIZANDO SOFTWARE LIBRE

---

VÍCTOR BRAVO Y ANTONIO ARAUJO

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

Una Autoridad de Certificación Raíz (AC Raíz) es un componente que tiene el rol de ser el punto más alto de confianza en una ICP. Una ICP genera certificados electrónicos de acuerdo al estándar X.509 proporcionando seguridad lógica, y vinculación legal a las transacciones que realiza el titular del certificado en la Internet. La confianza reside en la protección, a través de esquemas fuertes de seguridad física y lógica, de la clave privada que permite la generación de estos certificados.

Este trabajo muestra el proceso de desarrollo de una aplicación para gestionar una Autoridad de Certificación Raíz utilizando bibliotecas, herramientas, compiladores, sistemas operativos y licencias compatibles con los principios del software libre. En primer lugar, se determinan los requisitos a ser satisfechos en función de una descripción general de las funciones y características de una Autoridad de Certificación; posteriormente, se diseñan funcionalidades y se especifican requisitos, con el objetivo de producir una visión formal de los procesos a automatizar. Se dedica una sección a la implementación que consiste en la codificación en un lenguaje de programación de los procesos previstos en las etapas anteriores, como también, de la incorporación de mecanismos fuertes de validación de identidad de usuarios, registro de eventos, firma de acciones por parte de los administradores de la aplicación, y especificación de conexiones con hardware especializado, como tarjetas inteligentes. Finalmente, se describe el despliegue y configuración de la aplicación, que involucra la instala-

ción en un ambiente seguro (bóveda o centro de datos) y el enlace de la AC Raíz con los demás componentes de la infraestructura.

## 5.1. Introducción

La disponibilidad de Internet como medio digital permite que cualquier persona, empresa, institución, o administración realice transacciones gubernamentales, comerciales o personales en la mayoría de los casos, tal cual, como se realizarían en una oficina o espacio físico de forma presencial. Dado este hecho, al utilizar Internet para establecer relaciones humanas, se está de acuerdo que es necesario trasladar el concepto de “identidad” al medio digital[1]. La criptografía provee algoritmos y mecanismos para construir este concepto en la red, ya que es posible utilizar herramientas que aporten elementos para definir la identidad de un usuario, entidad o institución, de la misma forma de la que se está familiarizado en el mundo real.

En muchas ocasiones para realizar actividades cotidianas personales o de trabajo, se debe establecer contacto con un individuo u organización que no se conoce o del cuál no se tiene ninguna referencia. Mediante un contacto personal o directo, los sentidos humanos permiten percibir un gran número de detalles que le caracterizan, y cuya combinación muy probablemente le hace irrepetible. Esta combinación permite identificar al individuo de forma única y certera. Dicho esto, la identidad se define como el reconocimiento que se hace de las credenciales físicas o informativas, que ese individuo ofrece para que se le acepte como poseedor de una determinada individualidad [2]. Las credenciales físicas pueden ser documentos como la Cédula de Identidad, el Pasaporte, la Licencia de Conducir, entre otros. Todos los documentos citados generalmente incluyen una fotografía que permite la comparación con la apariencia del interlocutor; también usualmente se agrega otra característica informativa que puede ser un nombre, una firma manuscrita y posiblemente un número de referencia.

Cuando se traslada el concepto de identidad al medio informático, se habla de identidad digital, y se hace necesario contar con credenciales traducibles a información binaria. Por otro lado, la criptografía, por sí misma no proporciona este concepto: es el uso de una infraestructura computacional que utiliza algoritmos criptográficos para representar credenciales digitales, como por ejemplo el certificado electrónico, y que son otorgados por terceros de confianza, denominados Autoridades de Certificación (AC), y que se describen como Raíz cuando son el punto inicial de una jerarquía, las que proveen a usuarios y organizaciones de identidad digital, y que cuenta con las mismas connotaciones que tiene este concepto en el ámbito personal y jurídico. Uno de los problemas que aparece en este punto, es la disponibilidad de la infraestructura mencionada anteriormente, la cuál debe contar como un elemento obligatorio una aplicación que gestione, bajo un estándar aceptado, como lo es el estándar X.509[3], los certificados electrónicos que emite la AC. La discusión de importantes aspectos que surgen en las diferentes etapas del proceso de desarrollo de la aplicación de gestión, y que están vinculados con los principios del software libre y los requisitos muy particulares del ambiente de despliegue, subrayan los objetivos propuestos de este trabajo.

## 5.2. Marco Teórico

Con el objetivo de contextualizar los términos “identidad”, “confianza”, o “transacción segura” y “AC Raíz” en el medio digital, y específicamente en relación con la Internet; es imprescindible en una primera aproximación, discutir sobre determinados temas y conceptos vinculados con la seguridad informática. En los párrafos siguientes se abordan brevemente algunos de los puntos más importantes relacionados con el tema.

### 5.2.1. Seguridad Informática

Se ha llegado a un consenso sobre lo que significa seguridad informática [2]. En general, se dice que un activo de información, (información digital con un valor real para una empresa o persona) está asegurado si cumple con niveles aceptables relativos a su valor potencial en los siguientes aspectos:

**Disponibilidad:** es el grado en que un dato está en el lugar, momento y forma en que es requerido por uno o un conjunto de usuarios autorizados. Como premisa, un sistema seguro debe mantener la información disponible para los usuarios autorizados. Disponibilidad también significa que el sistema, debe mantenerse funcionando eficientemente y es capaz de recuperarse rápidamente en caso de fallo.

**Confidencialidad:** es el aspecto de la seguridad que permite mantener en secreto la información y sólo los usuarios autorizados pueden manipularla. Igual que para la disponibilidad, los usuarios pueden ser personas, procesos o programas. Para evitar que ninguna persona no autorizada pueda tener acceso a la información transferida y que recorre la red se utilizan técnicas de cifrado o codificación de datos. Hay que mantener una cierta coherencia para determinar cuál es el grado de confidencialidad de la información que se está manejando, para así evitar un esfuerzo suplementario a la hora de decodificar una información previamente codificada.

**Integridad:** corresponde a garantizar que la información transmitida entre dos entidades autorizadas no sea modificada por un tercero no autorizado. Un mecanismo para lograrlo es la utilización de firmas electrónicas. Mediante una firma electrónica se codifican los mensajes a transferir, de forma que una función, denominada hash [4], calcula un resumen de dicho mensaje y se le añade. La validación de la integridad del mensaje se realiza aplicándole al original la misma función y comparando el resultado con el resumen que se añadió al final cuando se calculó por primera vez antes de enviarlo. Mantener la integridad es importante para verificar que en el tiempo de viaje por la red de la información entre el sitio emisor y receptor ningún agente externo o extraño ha modificado el mensaje.

### 5.2.2. Criptografía

La criptografía es la ciencia o arte de ocultar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas o usuarios autorizados [2]. La criptografía ha tomado gran importancia en los últimos años, ya que es posible transformar las “técnicas matemáticas” en algoritmos que pueden ser comprendidos por una computadora. Se puede clasificar la criptografía en dos tipos, según el tipo de clave que se utilice:

**Criptografía Simétrica:** los sistemas de criptografía simétrica son aquellos que utilizan una única clave para cifrar y descifrar un texto claro. Este tipo de sistema conlleva una desventaja, que consiste en el conocimiento de las partes (emisor y receptor) de la clave única que les permite intercambiar información por un canal seguro. Como respuesta a ello, se hace necesario formalizar un procedimiento que muestre a las partes autorizadas la información sobre la clave, sin que sea develada a un tercero no autorizado.

**Criptografía Asimétrica:** también se conoce como Sistema de Cifrado de Clave Pública [2]. Usa dos claves diferentes, una de ellas es la Clave Pública que puede ser enviada a cualquier persona y otra, que se denomina Clave Privada que es secreta, y no debe ser revelada. A diferencia del sistema de cifrado simétrico donde las partes deben concertar un procedimiento para conocer la clave única, en este tipo de sistema el remitente usa la clave pública del destinatario para cifrar el documento. Una vez que el documento o mensaje ha sido cifrado, solamente con la clave privada del destinatario el mensaje puede ser descifrado.

### 5.2.3. Certificados electrónicos

Un certificado electrónico es un documento de acreditación que permite a las partes tener confianza en las transacciones que realicen en internet. Por tanto, garantiza la identidad de su poseedor mediante un sistema de claves administrado por una tercera parte de confianza. Para validar un certificado basta con conocer la clave pública de la tercera parte conocida como la Autoridad de Certificación (AC). Para cuidarnos de que piratas informáticos cambien su clave pública por la de la autoridad de confianza, la AC debe crear un certificado con su propia información de identidad y a la vez su clave pública y firmar el certificado, este certificado se le conoce como certificado autofirmado. Dado que los certificados son información pública y lo que se desea es que todos tengan acceso a ellos, pueden hacerse copias del certificado para su distribución. Los certificados electrónicos permiten varias cosas, entre ellas se pueden citar que los usuarios pueden añadir firmas electrónicas a los formularios en línea; que los destinatarios pueden comprobar la autenticidad del

correo electrónico confidencial; que los compradores pueden estar seguros de que un sitio web es legítimo; y por último, controla el acceso a bancos y comercios en línea, así como las intranets y extranets.

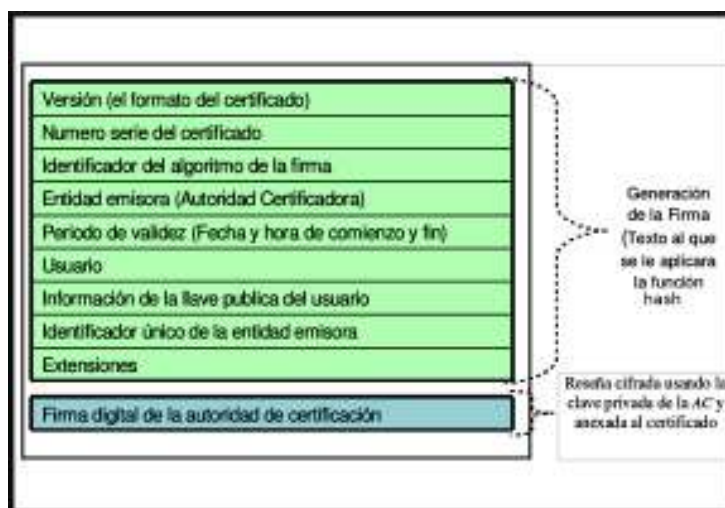
#### 5.2.4. Estándar X.509

X.509 y X.500 fueron originalmente diseñados a mediados de los años 80, antes del enorme crecimiento de usuarios en la Internet. Es por esto que se diseñaron para operar en un ambiente donde sólo los computadores se interconectaban intermitentemente entre ellos. En las versiones 1 y 2 de X.509 se utiliza una lista estandarizada denominada lista de revocación de certificados (CRL por sus siglas en inglés) que contiene la información referente a certificados que han sido revocados.

La versión 3 introduce cambios significativos en el estándar. El cambio fundamental es el hacer el formato de los certificados y las CRL extensible. Ahora los que implementen X.509 pueden definir el contenido de los certificados como crean conveniente. Además se han definido extensiones estándares para proveer una funcionalidad mejorada.

Con la utilización de la tecnología de certificados electrónicos se provee a los clientes (personas o programas) de un nivel más alto en los procesos de autenticación y autorización, ya que se le otorga al cliente algo que puede poseer, incluso incluir dentro de un elemento físico, como una tarjeta inteligente. Los certificados en el formato X.509 v3 contienen datos del sujeto, como su nombre, dirección, correo electrónico, etc. La figura 5.1 muestra un bosquejo de la especificación del estándar X.509 versión 3.

En la versión 3 de X.509, no hace falta aplicar restricciones sobre la estructura del certificado, gracias a la definición de las extensiones de certificados. Se permite que una organización pueda definir sus propias extensiones para contener información específica dentro de su entorno de operación.



**Figura 5.1** Especificación del estandar X.509

Entre los tipos de certificados más comunes están:

- **Certificado de Servidor de Conexión Segura (SSL por sus siglas en inglés):** Permite incorporar el protocolo SSL a un servidor web con el objetivo que toda la comunicación entre el cliente y el servidor permanezca segura, cifrando la información que envía cada parte. El certificado del servidor posibilita la autenticación fuerte, es decir, que el servidor puede exigir certificados personales de navegación a los usuarios para acceder a determinadas carpetas, lo que repercute en la seguridad y en la comodidad por la ausencia de cuentas y contraseñas para la identificación de los usuarios.
- **Certificados personales (Correo electrónico y navegación):** Un certificado electrónico personal es la herramienta necesaria para navegar, comprar y enviar o recibir correo a través de la Internet, de una

manera segura. Con el uso de este certificado se pueden firmar o cifrar los mensajes de correo para tener la seguridad que el receptor será el único lector de nuestro mensaje. Se puede aumentar la seguridad y confianza entre el cliente y el servidor web, al autenticarse también al usuario, esto también va a permitir a las empresas la posibilidad de personalizar los contenidos a un usuario concreto, con la certeza que otros usuarios no podrán ver dicho contenido, tales como información confidencial, ofertas especiales, entre otros.

- **Certificado para firma de código:** El certificado para la firma de código permite a un administrador, desarrollador o empresa de software firmar su software y macros, y distribuirlo de una forma segura. Esta solución de Seguridad es el requisito mínimo que necesitan los clientes o lista de correo, para confiar y tener la seguridad de que el fichero que reciben o se descargan, proviene exclusivamente de una empresa determinada. Con ello se evitan los problemas causados por la suplantación de identidad y la distribución de objetos dañinos o perjudiciales bajo esta supuesta identidad. Cualquier modificación (por ejemplo: inclusión de un troyano o infección de un virus) sobre el software original lo invalidará, con lo que el usuario tendrá la confirmación para rechazarlo al comprobar que la firma electrónica no corresponde con la del software modificado.

### 5.2.5. Lenguaje Unificado de Modelado

El Lenguaje de Modelado Unificado (UML por sus siglas en inglés) permite diseñar sistemas a través de modelos, que se componen de un conjunto de símbolos y diagramas en donde se plasman las ideas de funcionalidad. El UML fue creado por Grady Booch, James Rumbaugh e Ivar Jacobson en el año 1997[5],[6] y [7]. Cada diagrama tiene fines distintos dentro del proceso de desarrollo, su finalidad es presentar diversas perspectivas de un sistema. La clave está en organizar el proceso de diseño de tal forma que los analistas, clientes, desarrolladores y otras personas involucradas en el desarrollo del modelo lo comprendan y convengan con él. Los diagramas que componen el lenguaje son:

- Diagramas de clases
- Diagramas de casos de uso
- Diagramas de estados
- Diagramas de secuencias
- Diagramas de colaboraciones
- Diagramas de distribución
- Diagramas de actividades
- Diagramas de componentes
- Diagrama de despliegue

En este trabajo se utilizaron esencialmente los diagramas de clases, los diagramas de casos de uso y los diagramas de actividades, que se describen brevemente a continuación:

**Diagramas de clases:** son representaciones gráficas de las categorías en que pueden clasificarse los objetos del mundo real. En general, se hace una descripción de las categorías que se utilizan en la aplicación a desarrollar. Las clases se diseñan en función de sus atributos y relaciones con otras clases.

**Diagramas de casos de uso:** son descripciones de las acciones que debe realizar el usuario en el sistema [5]. Por ejemplo: Usuario que tiene la necesidad de expedir un certificado electrónico a una AC de confianza.

**Diagramas de actividades:** muestran el flujo de actividades que ocurren dentro de un caso de uso o dentro de un comportamiento de un objeto[5]. Por ejemplo, las actividades que se realizan para expedir un certificado electrónico.

### 5.2.6. Software Libre

El software libre [8] es un asunto de libertad, no de precio. Para que un programa, aplicación o conjunto concreto se considere “software libre” debe cumplir con las siguientes libertades: 1) Libertad de ejecutar el programa en cualquier sitio, cualquier propósito, por siempre; 2) Libertad de estudiarlo y adaptarlo a nuestras necesidades; 3) Libertad de redistribuirlo a cualquiera, logrando ayudar a un amigo o vecino; y por último 4) la Libertad de mejorar el programa y publicar las mejoras.

Las libertades antes expuestas, proveen muchos beneficios a los usuarios finales. En particular, en el área de seguridad informática. Se pueden nombrar entre los beneficios más importantes: la no dependencia de un único fabricante, y la posibilidad de realizar auditorías y pruebas exhaustivas por parte de terceros, que pueden ser personas, empresas o instituciones diferentes responsables del proyecto de software. Los procesos de adaptación, mantenimiento, integración y auditorías son más transparentes y colaborativos.

## 5.3. Infraestructura de Clave Pública

Uno de los problemas del despliegue de la tecnologías basada en certificados y firmas electrónicas, es contar con un elemento que proporcione una relación fuerte de confianza entre dos o más sujetos que desean realizar una operación o transacción utilizando como medio la Internet. Es por ello, que se recurre a establecer un tercero de confianza, que se define, como un actor encargado de brindar confianza basada en la disponibilidad de una infraestructura robusta que incluya el uso de tecnologías basadas en algoritmos criptográficos estandarizados, y la aplicación estricta de políticas para los procesos de registro, publicación, firma, renovación y revocación de certificados. El tercero de confianza se denomina Infraestructura de Clave Pública (ICP) [3], y consiste en la combinación de hardware y software, políticas y procedimientos que permiten asegurar la identidad de los participantes en un intercambio de datos usando criptografía de clave pública. Una ICP debe proporcionar los tres conceptos de seguridad mencionados anteriormente.

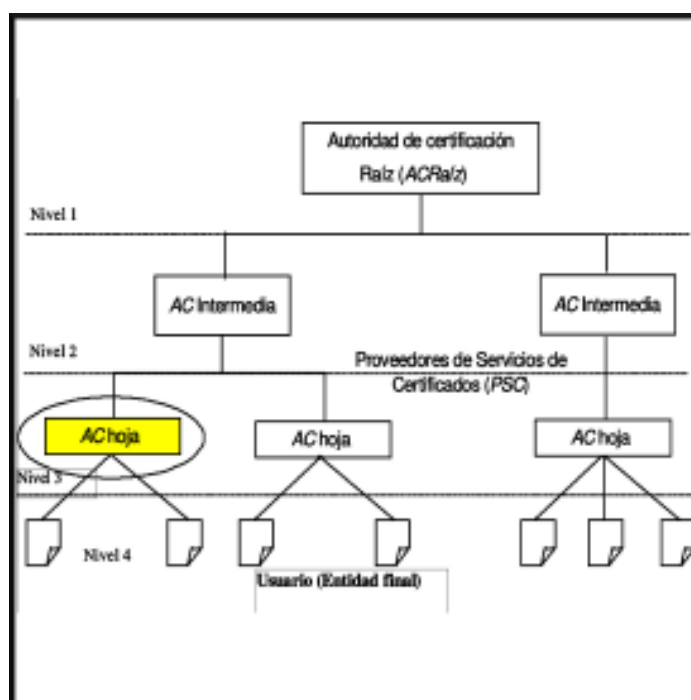
### 5.3.1. Componentes de la Infraestructura de Clave Pública (ICP)

Los componentes habituales que conforman la infraestructura son los siguientes (Ver Fig. 5.8):

- **Autoridad de Registro (AR):** es el nodo o conjunto de nodos responsables del registro y la autenticación inicial de los usuarios a quienes se les expide un certificado, después de aprobada una solicitud de registro.
- **Autoridad de Certificación (AC):** es el nodo central de la infraestructura, se encarga de los procedimientos de firma, renovación y revocación de certificados electrónicos. El procedimiento de firma de certificados utiliza la clave privada de la AC.
- **Interfaz con los clientes (PUB):** es el nodo que brinda toda la información a las entidades finales (usuarios) sobre el estado de su certificado, además de ofrecer una información al público en general sobre los aspectos y servicios relevantes de la ICP.

Los nodos de una ICP pueden ordenarse según diversos modelos. El más utilizado es el modelo jerárquico, que presenta una raíz y nodos hijos que distribuyen los certificados a los clientes o entidades finales. En la figura 5.2 se muestra un ejemplo de modelo de jerarquía de una ICP de cuatro niveles, que se encuentra en el tercer nivel del modelo, que certifica a los usuarios.

Este modelo de establecimiento de relaciones de confianza, es necesario entre múltiples autoridades de certificación para garantizar que los usuarios (entidades finales) no tengan que depender y confiar en una sola AC, algo que haría imposible el manejo de estabilidad, administración y protección. El objetivo es que las entidades finales que utilizan identidades creadas por una AC puedan confiar en ellas, aunque dichas partes tengan una autoridad expedidora diferente.



**Figura 5.2** Modelo jerárquico de una ICP

## 5.4. Desarrollo de la aplicación

En los párrafos siguientes se discuten los aspectos, procesos y técnicas principales, que se siguen a lo largo del desarrollo de la aplicación (software) de gestión del componente Autoridad de Certificación Raíz.

### 5.4.1. Conceptualización

Uno de los objetivos de esta etapa es determinar el rol del componente AC Raíz en la ICP, con la finalidad de obtener los requisitos, procesos y funciones que deben ser implementados por el software. Este rol tiene que ver con la definición de la AC Raíz como elemento central y de máximo resguardo de la infraestructura, ya que este nodo inicial o “Raíz” contiene la clave privada que valida todos los certificados de los otros nodos de la jerarquía.

Se considera como punto importante en esta etapa, distinguir las diferencias entre una AC Raíz y una AC de un Proveedor de Servicios de Certificación (PSC). La diferencia principal entre estos dos tipos de AC, es la cantidad de certificados que deben gestionar (firmar, renovar, revocar, etc.) , en un determinado periodo cada uno de ellos. Esto es, una AC Raíz solo gestiona un número mínimo de certificados, los cuáles sirven para dar inicio a la jerarquía (certificados otorgados a los PSC), por el contrario, una AC de un PSC debe gestionar un número mucho mayor de certificados, ya que la función de este nodo es entregar certificados periódicamente a usuarios, también llamados entidades finales.

La diferencia de escala de los dos tipos de AC conlleva a que la AC Raíz tenga características particulares, que tienen que ver con los niveles y elementos de seguridad tanto físicos como lógicos que deben considerarse en la gestión del componente. Por ejemplo, la desconexión de red del equipo donde se ejecuta la aplicación de gestión hace que la recepción y entrega de certificados se realice a través de unidades de memoria externas y portátiles, debidamente validadas, con las cuáles el software debe mantener una comunicación segura.

La conexión de la aplicación con hardware especializado, como el Módulo de Seguridad en Hardware (HSM por sus siglas en inglés) que permite generar y almacenar claves o las tarjetas inteligentes, es un factor que debe considerarse en el momento de enumerar las funciones iniciales del software de gestión.

La selección del sistema operativo Linux [9] para desplegar la aplicación, ya que cumple con los principios del software libre, y cuenta con gran número de herramientas en el área de programación [10], es un requisito no funcional que se establece en esta etapa.

Considerando los aspectos nombrados anteriormente, en este punto se elabora una lista inicial de requisitos, con la cual debe cumplir la aplicación. Como técnicas utilizadas en esta etapa están la realización de entrevistas a clientes, a posibles administradores y operadores; así como la elaboración de tablas comparativas entre diferentes aplicaciones que existen en las bibliotecas o portales de software libre, con la finalidad de evaluar las herramientas a utilizar en la elaboración de la aplicación.

#### 5.4.2. Diseño

La etapa de diseño consiste en elaborar diagramas formales que permitan en la etapa de implementación la representación de requisitos y procesos de la gestión del componente AC Raíz en un lenguaje de programación. Para el diseño de requisitos se utilizan los diagramas de casos de uso del lenguaje UML, que muestran una primera aproximación de las operaciones que se deben realizar en relación con las entradas dadas por los usuarios. Los actores (usuarios) del caso de uso principal que se muestra en la figura 5.3 son: el Administrador del componente AC, el Administrador del Componente AR, el Administrador del componente PUB, y el actor PSC, quiénes son los que interactúan con la aplicación.

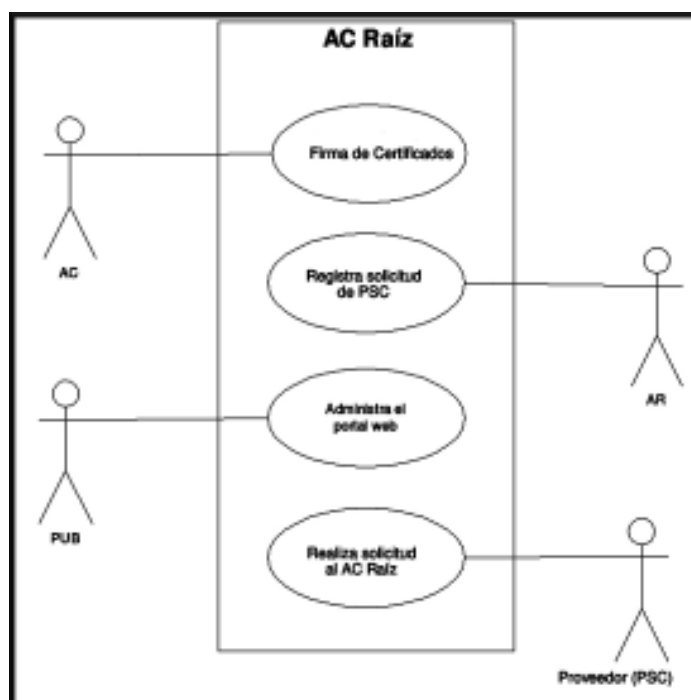
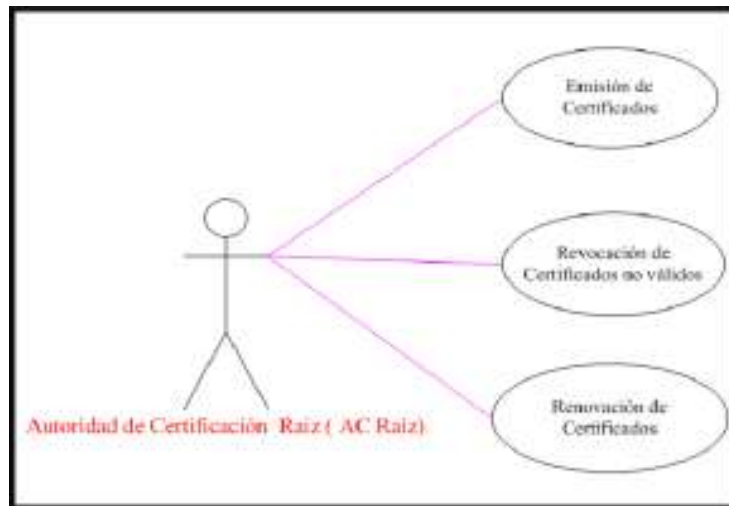


Figura 5.3 Caso de uso principal

Para el resto de la especificación de requisitos se elaboran casos de uso que modelan las funcionalidades con que debe contar la aplicación. Para cada actor, se especifican el correspondiente diagrama de caso de uso. En la figura 5.4 se muestra el caso de uso para el actor del componente AC. Las acciones que realiza este actor son emisión, renovación y revocación de certificados, que conlleva procesos de firma con la clave privada,

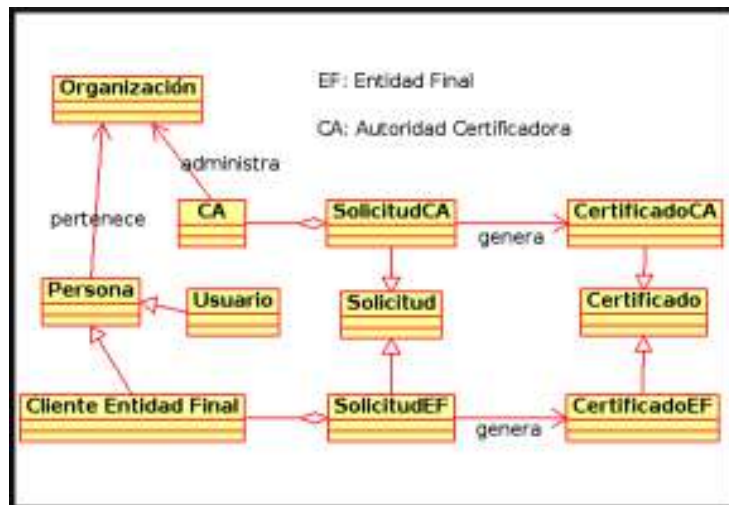


modificación de los periodos de vigencia del certificado y elaboración de listas de certificados revocados respectivamente para cada caso de uso.



**Figura 5.4** Caso de uso para el actor Administrador Autoridad de Certificación

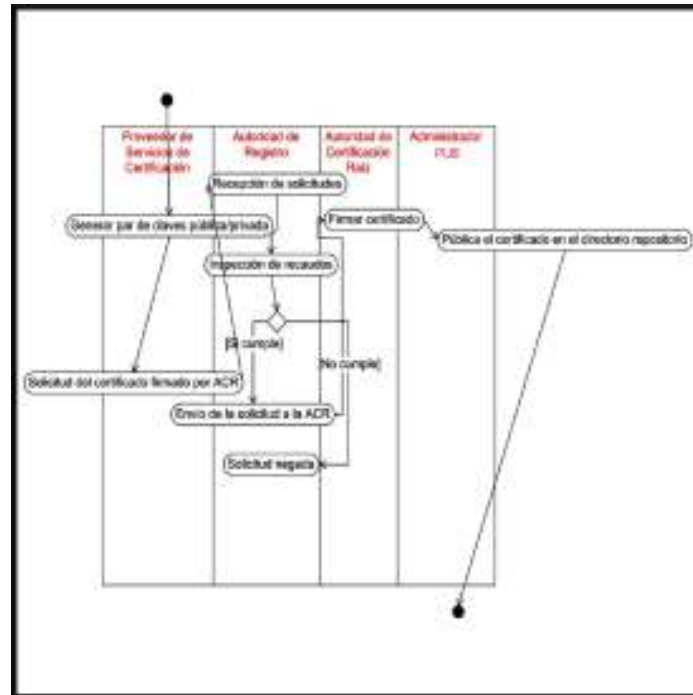
También en esta etapa se construye el modelo de datos de la aplicación. La figura 5.5 muestra de forma parcial, ya que no se incluyen los atributos, el diagrama de clases que explica el modelo de datos. Se consideran como objetos persistentes del sistema a elementos como usuarios, clientes, certificados, autoridades o proveedores de certificación, solicitudes de autoridad de certificación, solicitudes de entidad finales, y sus respectivas relaciones.



**Figura 5.5** Diagrama de clases

Para modelar la secuencia de acciones que se realizan para cada caso de uso se utilizan los diagramas de actividades. La figura 5.6 muestra el diagrama de actividades generales para el caso de uso “Emisión de certificados” del actor Administrador del componente AC. Para este conjunto de actividades participan cuatro (4) actores: Administrador del PSC, quien entrega los recaudos necesarios para que se le firme su solicitud, el Administrador de la AR, quién es el encargado de chequear los recaudos entregados por el PSC, el Adminis-

trador de la AC Raíz y el Administrador PUB, este último encargado de publicar en los diferentes repositorios los certificados (claves públicas) para que sean visibles por el mayor número de usuarios interesados.



**Figura 5.6** Diagrama de actividades para el caso de uso "Emisión de Certificados"

### 5.4.3. Implementación

En esta etapa se utilizan como insumo los diagramas de casos de uso, diagrama de clases y actividades, generados en la etapa de diseño. Se traduce el diagrama de clases al que se hace referencia en la figura 5.6 en un modelo de datos relacional, y se genera un script o guión SQL que genera el mapa de tablas relacional, donde las tablas representan relaciones tales como usuarios, clientes, certificados, y las demás entidades que conforman el modelo de datos.

Se utilizan y validan los diagramas de casos de uso mediante la elaboración de interfaces gráficas de usuarios y funcionalidades de interacción con el usuario. Los diagramas de actividades ayudan en el planteamiento de algoritmos que proveen funcionalidades o características con las cuáles debe contar la aplicación y que deben estar en coordinación con los respuestas y valores esperados.

Haciendo uso de las ventajas que trae el uso de software libre, descritos en 5.2.6, se implementa la aplicación utilizando la mayor cantidad de líneas de códigos disponibles en los repositorios y proyectos de la comunidad, de tal manera que satisfagan los requisitos y funcionalidades planteadas en la etapa de diseño. En este sentido, se utiliza el código fuente del proyecto XCA [11], desarrollado por Christian Hohnstädt, que tiene como objetivo proveer una aplicación escrita en el lenguaje de programación C++[12] y la biblioteca Trolltech Qt[13], que cumpla con el estándar X.509. La aplicación satisface los requisitos básicos para la gestión del componente de gestión de AC Raíz, esto es, los diagramas UML de la etapa de diseño calzan con un gran conjunto de requisitos satisfechos en el proyecto XCA, esto ocurre debido a que este trabajo comparte objetivos con dicho proyecto; por ejemplo, para el caso de uso de la figura 5.4, donde el actor debe ejecutar tres acciones: emitir, renovar y revocar certificados, la aplicación XCA incorpora estas tres actividades, pero se hace necesario adaptar la interfaz de usuario y agregar características en función de los requisitos capturados.

Es importante recalcar, que XCA no satisface todos los requisitos documentados en la etapa de diseño. En respuesta a este hecho, se realiza un proceso de incorporación de funcionalidades. En este sentido, se agregan características a la aplicación acorde con la especificaciones de diseño, entre las cuáles se enumeran:

- La incorporación de un sub-sistema de seguridad para acceso a los activos de información que gestiona la aplicación, que incluya aspectos de autenticación y autorización de usuarios, como lo es la validación de credenciales a través del uso de tarjetas inteligentes, el registro y firma electrónica de las acciones realizadas por los usuarios dentro de la aplicación. En la figura 5.7 se muestra la característica de registro de acciones. La ventana a la derecha muestra los detalles de la acción seleccionada en la lista, se incluyen datos importantes como nombre de la cuenta de usuario, fecha, hora, y otros datos particulares relacionadas con la acción realizada por el correspondiente usuario.



**Figura 5.7** Sistema de registro de acciones

- Estandarización del sistema de gestión de documentos como solicitudes, plantillas de certificados y certificados.
- Conexión a través de una interfaz propia con el hardware donde se resguardan las claves privadas (HSM).

También en esta etapa se seleccionan e integran las tecnologías a utilizar para la codificación y creación de la aplicación de gestión del componente AC Raíz. Los tipos de tecnologías que deben seleccionarse son: bibliotecas para construir la interfaz hombre-máquina (HMI por sus siglas en inglés), motor criptográfico, conexiones con hardware, interfaces con repositorio de datos y algoritmos de cálculo criptográfico más utilizados.

Como criptosistema se utiliza OpenSSL version 0.9.8 [14], que provee un conjunto de funciones criptográficas apegadas al estándar X.509. Para la construcción de interfaces hombre-máquina y uso de algoritmos generales se selecciona la biblioteca Qt. Como interfaz para el uso de tarjetas inteligentes se utilizó el estándar PKCS#11, también conocido como Cryptoki, que especifica una forma para interactuar con este hardware criptográfico[1].

#### 5.4.4. Pruebas

Esta etapa tiene dos objetivos. El primero consiste en asegurar que la aplicación funcione correctamente, es decir, que se generen la menor cantidad de salidas inesperadas o fallas a entradas dadas. En relación al logro de este objetivo se utilizan un conjunto de técnicas aplicadas a lo largo del proceso de desarrollo, entre las cuáles se pueden citar la revisión en parejas [15], que consiste en la programación se realice en equipo de dos programadores por computador, uno de ellos se encarga de escribir los algoritmos en un lenguaje de programación, y el segundo de ellos de revisarlo inmediatamente; después de periodo de unas horas establecido previamente, se intercambian los roles. Otra de las técnicas utilizadas que es importante nombrar son las pruebas unitarias [15], las cuáles consisten en aplicar un número de casos de pruebas a métodos o módulos pequeños de la aplicación (unidades), de tal manera que se asegura que funcionan correctamente de forma independiente. Seguidamente, se realizan pruebas de integración, que consisten en probar módulos más complejos formados por las unidades revisadas en las pruebas unitarias. Las pruebas unitarias y de integración presentan las ventajas que son automatizables, y por lo tanto, se cuenta con herramientas de software para llevarlas a cabo.

El segundo objetivo, es que se satisfagan los requisitos plasmados en la etapa de diseño, y que se extraen de los diagramas UML, es decir, la aplicación debe cumplir con las características necesarias para resolver el problema de gestión de una AC Raíz. En este sentido, se toma una estrategia basada en prototipos con liberaciones periódicas, que permite a los usuarios y desarrolladores de la comunidad chequear el progreso en el proyecto. Los prototipos son chequeados por los usuarios y la modificación de requisitos y notificación de errores son notificados en un sistema web de chequeo y seguimiento [16].

También se habilita un sistema de control de versiones de licencia libre llamado subversion [17], que permite a los programadores involucrados en el proyecto obtener en todo momento y de forma local o remota la última versión de los programas fuentes.

Debido a que la aplicación de gestión de AC Raíz debe ser parte de una infraestructura, es necesario realizar pruebas en condiciones similares a la configuración final de ésta; por ello que se simula la configuración de producción que conlleva pruebas con el sistema operativo y el lugar donde se instala la aplicación, conexión con tarjetas inteligentes y el módulo de seguridad en hardware, controles de acceso físico y lógico, y desconexión de red, ya que la autoridad debe operar fuera de línea.

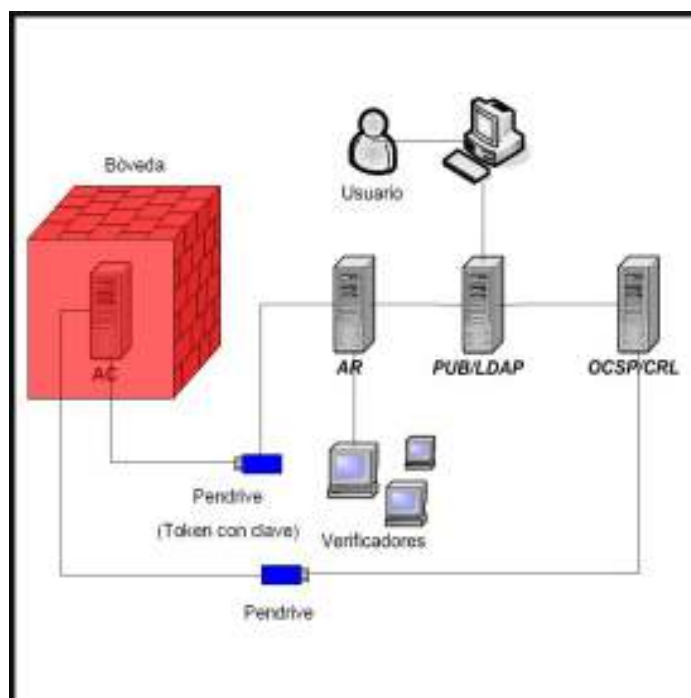
#### 5.4.5. Despliegue y configuración

El despliegue consiste en la instalación en condiciones reales de la aplicación de gestión de AC Raíz dentro de la infraestructura. La figura 5.8 muestra una propuesta para el despliegue de la infraestructura. La aplicación se instala en un computador desconectado de red que debe estar ubicado dentro de un lugar físico seguro, lo que significa que el acceso a personas deber estar restringido por llaves y controles biométricos, y el flujo de información digital hacia adentro y afuera de la bóveda debe ser realizado a través de dispositivos de memoria secundaria con seguridad incorporada, tal como una memoria usb (pendrive) con bloqueo por contraseña, como se muestra en la figura 5.8. También es necesario la habilitación de servidores para la validación de los períodos de vigencia de los certificados a través del protocolo de estado de certificado en línea (OCSP por sus siglas en inglés), y para la generación de solicitudes de firma de certificados, donde las entidades finales o usuarios consignan los recaudos.

Por otro lado, la configuración conlleva el establecimiento de parámetros para el funcionamiento de la aplicación, tales como métodos de control y restricción de acceso, ubicación de archivos y directorios, rutas para importación y exportación de datos, perfiles de usuario, generación y nombres de claves, inicialización de tarjetas inteligentes, inicialización de HSM, y copias de seguridad.

### 5.5. Conclusiones

La puesta en marcha de una AC Raíz supone obligatoriamente contar con una aplicación que gestione este componente de la infraestructura. En este sentido, este trabajo mostró el proceso de desarrollo de una aplicación que respondiera a los requisitos particulares de gestión, determinados por el rol de confianza raíz que debe representar la Autoridad de Certificación. En función de ello, la aplicación tiene un alto grado de



**Figura 5.8** Configuración de los componentes del nodo raíz de una ICP

especialización, ya que cuenta con un mercado relativo de pocos usuarios, si se compara con el mercado de los sistemas de información o aplicaciones de ofimática, y su operación se realiza en condiciones estándares y específicas. A pesar de este hecho, para la construcción de la aplicación se integraron varios proyectos disponibles en los repositorios de software libre, lo que permitió disponer de un criptosistema estándar y suficientemente completo para cumplir con los requisitos descritos en la etapa de diseño. La criptografía se utiliza como herramienta para otorgar las tres propiedades (confidencialidad, integridad y disponibilidad) de la seguridad informática a los datos que gestiona la aplicación, y en virtud de ello el hardware criptográfico utilizado como las tarjetas inteligentes y el módulo de seguridad en hardware configuran un “mundo seguro” que cumple con los estándares aceptados a nivel mundial.

En la etapa de diseño, los diagramas de casos de uso y actividades sirvieron para obtener una visión formal de los requisitos y de los procesos con los que la aplicación debe cumplir. Estos documentos de diseño en el lenguaje UML, permitieron alcanzar de manera más rápida y certera los objetivos que son coincidentes con la gestión real de una AC Raíz.

Al seguir el estándar X.509 se asegura que los certificados, solicitudes y claves gestionados por la aplicación sean compatibles con el esquema de seguridad basado en un tercero de confianza, y aceptado por gran cantidad de aplicaciones y sitios de comercio electrónico y transacciones seguras en la Internet.

Para la tarea de eliminación de fallas las técnicas como la colaboración utilizando herramientas web, la programación en equipos y las pruebas unitarias y de integración sirvieron para los procesos de prevención, notificación, búsqueda y arreglo de errores, permitiendo además guardar una bitácora del progreso a la solución de problemas. La implementación de características específicas en función de los requisitos cada vez más refinados y particulares que surgieron en las iteraciones de prototipos probados con usuarios y condiciones reales.

La combinación de diversos elementos como software, hardware y la configuración de un espacio físico adecuado, esto es, que cumpla determinadas reglas para el control de acceso, conforma la infraestructura necesaria para la operación de una AC, incluso que ésta no sea Raíz, y sea parte de otro nodo de la jerarquía.

Las condiciones de seguridad lógica y física pueden reproducirse exactamente para los nodos intermedios y los nodos Proveedores de Servicios de Certificación de la ICP, tomando en cuenta el escalamiento.

## 5.6. Glosario

*AC*: Autoridad de Certificación; componente de la PKI encargada de guardar de firmar, renovar, revocar las claves de los usuarios o entidades finales.

*AR*: Autoridad de Registro; componente de la PKI encargada de validar los recaudos de un PSC o Entidad Final, es decir, su identidad, y generar la solicitud para una firma de Certificados.

*Entidad Final*: Persona natural o jurídica a la que un PSC le expide un certificado digital.

*PSC*: Proveedor de Servicios de Certificación Digital; Organización que mantiene la infraestructura de nodo de una ICP, y está autorizada a expedir certificados a las personas naturales y jurídicas que soliciten y reúnan los recaudos necesarios para obtener un certificado digital.

*PUB*: Publicador; componente de la PKI encargada de mantener accesibles los certificados digitales emitidos por la PKI en medios como portales Web o directorios.

*PKI*: Public Key Infrastructure, Infraestructura de clave pública; es el conjunto formado por software, hardware, y políticas que asegura en la internet la propiedad de la claves públicas de los usuarios.

*HSM*: Hardware Security Module; módulo de seguridad en hardware, equipo físico computacional que contiene funciones criptográficas, en específico funciona para almacenar con un alto nivel de seguridad claves privadas.

## REFERENCIAS

---

1. R. Nichols and P. C. Lekkas. *Seguridad para comunicaciones inalámbricas*. McGraw-Hill, Mexico, 2003.
2. William Stallings. *Fundamentos de Seguridad de Redes. Aplicaciones y Estándares*. Pearson, Prentice Hall, España, 2 edition, 2003.
3. Andrew Nash, William Duane, Celia Joseph, and Joseph Brink. *PKI: Infraestructura de clave pública*. McGraw-Hill, Mexico, 2002.
4. Vicente Aceituno Canal. *Seguridad de la información*. Noriega Editores, M'xico D.F., M'xico, 2003.
5. Joseph Schmuller. *Aprendiendo UML en 24 horas*. Prentice Hall, México, 2003.
6. Booch G. *UML Lenguaje Unificado de Modelado*. Addison Wesley, 1999.
7. Alain Pierre-Muller. *Modelado de objetos con UML*. Eyrolles, Barcelona, España, 1997.
8. Free software definition. <http://www.fsf.org/licensing/essays/free-sw.html>, 2007.
9. Koretsky Sarwar. *El libro de Linux*. Pearson, Prentice Hall, Madrid, España, 2003.
10. Kurt Wall et al. *Programación en Linux*. Prentice Hall, Madrid, España, 2001.
11. Christian Hohnstädt. XCA, una interfaz gráfica para OpenSSL, Claves públicas y privadas, certificados, solicitudes y listas de revocación. <http://www.hohnstaedt.de/xca.html>, 2003.
12. Bjarne Stroustrup. *El lenguaje de programación C++*. Addison Wesley, Madrid, España, 2002.
13. James Blanchette and Mark Summerfield. *C++ GUI Programming with Qt 4*. Prentice Hall, Massachusetts, USA, 2006.
14. John Viega, Matt Messier, and Pravir Chandra. *Network Security with OpenSSL*. O'Really, 384 edition, 2002.
15. Roger S. Pressman. *Ingeniería del software. Un enfoque práctico*. Mc Graw-Hill, Mexico, 6 edition, 2005.
16. Welcome to the trac project. <http://trac.edgewall.org/>, 2007.
17. C. Michael Pilato, Ben Collins-Sussman, and Brian W. Fitzpatrick. *Version Control with Subversion*. O'Really, 2004.



# PROPUESTA DE ACOPLAMIENTO DE LA FIRMA ELECTRÓNICA AVANZADA EN PROCESOS DE NEGOCIO

---

VÍCTOR BRAVO Y ANTONIO ARAUJO

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

La automatización es el uso de tecnologías de información como un mecanismo directo para el mejoramiento. Sin embargo, existen elementos como la firma autógrafa que ha sido tomada en el área digital, y que en eventos recurrentes de procesos organizacionales son considerados como factor crítico en el flujo de operaciones. Como respuesta a esta situación, se han desarrollado numerosos estándares y tecnologías agrupadas por los conceptos de firmas electrónicas y PKI que han generado nuevas preguntas en este campo, entre ellas aquellas que tienen que ver con los procesos de integración.

En este artículo proponemos un componente de software y un método para conectar sistemas computacionales con la tecnología de firma electrónica avanzada. En este sentido se abordan formatos de documentos, infraestructura de validación y condiciones de seguridad que aseguran su soporte legal. El trabajo describe los problemas de integración bajo el concepto de acoplamiento.

### 6.1. Introducción

La adopción de la tecnología de firma electrónica aún no está suficientemente extendida. Ésta se utiliza en distintas áreas y en muchas instituciones o empresas alrededor del mundo pero no ha llegado a ser equivalente a



la firma autógrafa en un sentido amplio. Vinculado a este hecho, surge la pregunta ¿Pueden converger estas dos tecnologías en un futuro próximo? Con la finalidad de responder esta interrogante, se puede decir que la firma electrónica debe tener por lo menos tres características comunes a la autógrafa: identificar a la persona que la realiza; declarar la asunción u obligatoriedad de cumplimiento (contrato) del contenido de lo que se firma y por último, servir como prueba de autenticidad o no repudio del firmante. El modelo de firma electrónica basado en una infraestructura de clave pública (PKI por sus siglas en inglés), ha sido jurídicamente aceptado en muchos países, lo que equivale a decir que en estos casos se cumple con las características antes mencionadas.

La firma manuscrita se percibe como un elemento tecnológico desacoplado, esto es, no dependiente de otra tecnología o factor (solo se necesita papel y lápiz) que puede usarse casi en cualquier lugar y con aceptación universal. En cambio la firma electrónica requiere de elementos de software (manejadores de dispositivos, clientes de firma, etc.) y hardware (lector de tarjetas, tarjeta inteligente, computador, tableta o móvil), adicionalmente y por lo general se debe contar con una conexión a la Internet para la validación. Otra ventaja importante de la firma manuscrita es la permanencia de factores biométricos que son fundamentales en la realización de auditorías confiables. A pesar de todas estas ventajas, en los últimos años ha crecido el uso de la firma electrónica, gobiernos nacionales y locales de España [1], Alemania [2] y Estonia [3] tienen disponibles plataformas para sus ciudadanos, y la popularización de la tarjeta inteligente (smartcard) como elemento de identificación personal ha apoyado este crecimiento.

En este punto se plantean nuevos problemas vinculados al hecho de introducir o sustituir el elemento físico o autógrafa por el elemento electrónico, entre estos podemos señalar: elección del formato o formatos de archivo de los documentos firmados; ubicuidad y ergonomía de la acción de firma; verificación de los documentos firmados; histórico o archivo de documentos firmados y finalmente la integración de la firma con sistemas de base de datos relacionales, mapeos objetos-relacionales, servicios web, entre otros elementos utilizados en sistemas informáticos actuales.

En este sentido, este trabajo plantea un método para integrar un componente [4] de Firma Electrónica Avanzada denominado ComponenteFEA a procesos de negocio, teniendo presente parámetros de seguridad, rapidez y auditabilidad.

## 6.2. El modelo actual de firma electrónica

Una de las acciones para dar soporte jurídico a la firma electrónica y lograr su equivalencia con la firma manuscrita es fijar unas condiciones iniciales que garanticen integridad y auditabilidad de los documentos firmados, y que puedan ser validados a través de un estándar. Bajo este enfoque, se ha creado el concepto de firma electrónica avanzada, que por definición debe contar con las siguientes propiedades: a) estar vinculada al firmante de manera única; b) permitir la identificación del firmante; c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control y d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable. La formalización de esta idea ha sido llevada a cabo principalmente por el Parlamento Europeo, y se describe en la directiva 1999/93/EC [5].

Existen dos grandes dominios tecnológicos para el uso de la Firma Electrónica Avanzada: uno es el que tiene que ver con los procesos de identificación, registro, emisión y validación de certificados electrónicos. De este dominio se ocupan las organizaciones que están bajo el esquema PKI, que funcionan como terceros de confianza. Cada certificado brinda identidad a una persona o empresa en la Internet, y se le otorga al ente bajo la aceptación de un contrato que especifica condiciones de uso. El certificado es un documento -un archivo- que autentifica la clave vinculada al ente. La clave secreta/privada se distribuye en una tarjeta inteligente o token criptográfico que funciona como un elemento de control de acceso de nivel 2. Los certificados electrónicos contienen información especificada bajo el formato X.509 versión 3 [6], el cual incluye campos como fecha de expedición y vencimiento del certificado, Nombre único del propietario (conocido como Nombre Común), datos del Proveedor del certificado, datos criptográficos del certificado y datos del servidor de validación que utiliza el protocolo de estado de certificados en línea (OCSP por sus siglas en inglés).

El segundo dominio corresponde a las aplicaciones que usa el propietario del certificado para aplicar la firma electrónica, y que generan valor agregado. Las aplicaciones de este tipo más utilizadas cuentan con una interfaz basada en bibliotecas dinámicas (.dll o .so) para este fin, así como también tienen un archivo de

certificados de autoridades de certificación para validar la vigencia y correcta conformación del certificado del firmante. Esta interfaz es básica, solo permite generar un archivo de firma en formato PKCS#7 [7] separado del documento firmado, lo que conlleva a que las tareas de almacenamiento, validación y auditoría deben ser provistas adicionalmente a través de un programa o complemento de software. Las aplicaciones de este tipo más utilizadas son navegadores web y clientes de correo electrónico.

Por otro lado, se han especificado diferentes formatos estándares de archivo con firma autocontenida. Por ejemplo el formato PDF dada sus características de solo lectura y visualización en pantalla como documento impreso es uno de los más utilizados para este fin. El estándar PADES [8] basado en PDF es un ejemplo de ello, también existe el formato PDF nativo, y que es verificable por los visores más populares como el de *Adobe Reader*®.

También existen estándares para archivos con firma electrónica basados en XML. La ventaja de estos formatos es que pueden integrar metadatos como la fecha y lugar de la(s) firma(s), y permiten incluir diferentes tipos de archivos como fotos, videos, documentos de texto u ofimáticos. Entre los estándares XML más conocidos está el XMLDsig [9]. Este estándar cuenta con diferentes implementaciones y extensiones, entre ellas el formato creado por las repúblicas bálticas llamado BDOC [10], que sigue a su vez el popular estándar OpenDocument, utilizado por el paquete ofimático OpenOffice como formato principal para sus archivos.

### 6.3. Antecedentes

La inclusión de la firma electrónica en un proceso de negocio tiene varios aspectos asociados. Se pueden señalar como los más relevantes la ergonomía de la firma (facilidad de uso), los formatos y visualización de documentos, la integración con plataformas de software y la arquitectura de la solución.

En relación con el tema de la ergonomía Xyzmo SIGNificant<sup>1</sup> es una novedosa propuesta. Xyzmo es una aplicación comercial de código fuente propietario, que introduce elementos innovadores en el área de ergonomía y adaptación al cambio: no obliga a aprender una nueva técnica de firma sino que ofrece a los usuarios de esta tecnología el uso de la firma manuscrita a través de una tableta electrónica o teléfono con interfaz multitouch (multitouch) bajo sistemas operativos Android® y iOS®, esto sin desvincularse del esquema PKI. Este modelo proporciona al usuario la metáfora de la firma manuscrita mostrando el documento tal cual como si fuese impreso, habilitando la firma electrónica avanzada a través del uso de los dedos o de un lápiz para pantalla táctiles. Para el proceso de validación se utilizan parámetros biométricos tales como ritmo, velocidad o características del trazo, y también técnicas criptográficas estandarizadas vinculadas al esquema PKI.

Existen diferentes implementaciones de software para la gestión y visualización de los dos tipos de formatos principales: PDF y XML. Para el caso del formato PDF la visualización está automáticamente disponible ya que existen numerosos lectores para este tipo de archivo, por ejemplo, el Adobe Reader® que visualiza la firma electrónica o digital como un sello (imagen) dentro del documento, y muestra también su contenido con características de forma (encabezado, líneas, tablas, logos, etc.) que pueden ser parte o no del documento firmado, pero que en muchos casos son necesarias para la elaboración de documentos formales o legales. En el caso de los formatos XML la visualización no es automática, por lo tanto si se requiere visualizar el contenido con elementos de forma se debe disponer de un software visualizador que formatee el contenido. En [11] se muestra una propuesta para documentos XML que necesitan por disposiciones legales o formales de gobierno aplicar forma a documentos firmados electrónicamente.

Una de las potencialidades de la firma electrónica es su integración con sistemas informáticos para la mejora de procesos mediante la eliminación de puntos lentos. Es por ello que los temas de integración y arquitectura juegan un papel preponderante. En esta tendencia se inscribe el proyecto *@firma*: una solución desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, que se plantea como una plataforma de firma electrónica orientada a brindar servicios de gobierno electrónico, y que está integrada con el sistema de identificación Español. Cuenta con una aplicación de escritorio que puede usarse en diversos sistemas operativos, y un *applet* [12] para usar la firma a través de la web. Estas características habilitan a *@firma*

<sup>1</sup>Para ver información completa sobre Xyzmo Significant visitar la dirección web: <http://www.xyzmo.com>

para el desarrollo de aplicaciones de gobierno electrónico, así como también para la integración con sistemas empresariales.

#### 6.4. Acoplamiento de la firma electrónica avanzada

La conexión entre un componente (software) y el sistema informático se denomina acoplamiento. Este procedimiento debe cumplir con un conjunto de requisitos que tienen que ver con características tales como reutilización, cohesión y la exportación de una interfaz definida. A continuación se describen los elementos desarrollados en este trabajo.

##### 6.4.1. Componente de firma electrónica avanzada

Se desarrolló un componente que permite realizar diferentes operaciones asociadas con la firma electrónica: subir un documento desde el computador cliente; realizar la firma utilizando una tarjeta inteligente con PIN (contraseña) desde el computador cliente y entregar un archivo firmado en formato XAdES[13] al programa servidor. El componente se ha denominado de firma electrónica avanzada (ComponenteFEA), ya que cumple con las condiciones citadas en la sección 6.2 sobre este tipo de firma.

Las funcionalidades que implementa el ComponenteFEA son las siguientes:

1. Firmar electrónicamente (para este caso se asume que lo electrónico está asociado a un dispositivo en hardware como una tarjeta inteligente, y en relación a ello debe connotar vinculación jurídica, lo digital sólo a una clave en software) un documento de tipo de archivo definido por especificación MIME [14].
2. Firmar digitalmente (usando un archivo PKCS#12 [15]) un documento de tipo de archivo definido por especificación MIME .
3. Verificar un archivo firmado electrónicamente usando o no validación OCSP.
4. Verificar un archivo firmado digitalmente usando o no validación OCSP.
5. Mostrar propiedades como algoritmos utilizados, fecha y lugar de la firma de un archivo firmado
6. Firmar electrónicamente utilizando un componente para el navegador un documento de tipo de archivo definido por especificación MIME.

```
class BDocDocument : QObject {
// *** Métodos para firma electrónica
    BDocDocument();
    void init();
    void create( const QString file );
    bool openBDocContainer(const QString path);
    void saveBDocContainer(const QString path);
    bool signWithP12(const QString profile,...);
    void addDocument(const QString path);

// ** Métodos de firma por navegador web
    bool presignWeb(const QString profile, ...);
    bool postsignWeb(const QString profile, ...);

// ** Métodos para validación
    QString signatureAlgorithm(int index );
```

```

bool validateOffline() const ;

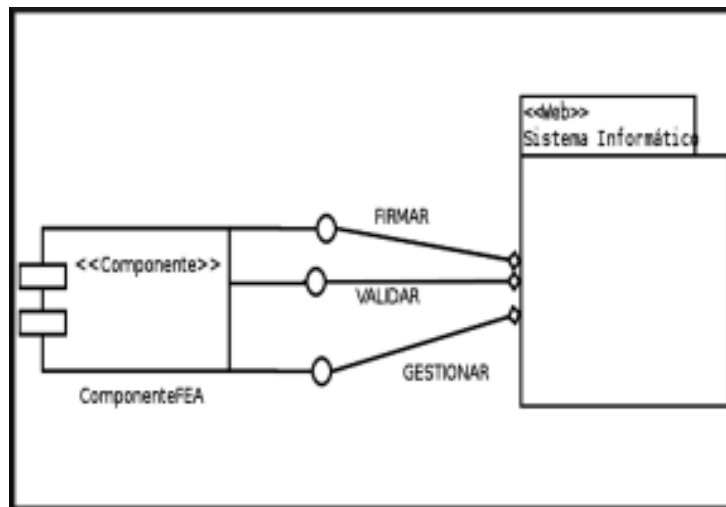
// ** Métodos para Gestión de archivos
QString signatureFormat(int index );
QString signatureDateTime(int index );
QStringList signatureLocation(int index );
QString signatureRol(int index );
QString signatureDigestMethod(int index );
QString subjectCertificateCommonName(int i);
QString documentName(int docId);
int documentCount();
int signatureCount();
void saveDocument(int docId...);

}

```

**Listado 1.** API del ComponenteFEA en C++ accesible desde *Python*

Bajo esta perspectiva se propone tratar las funcionalidades asociadas a la firma electrónica avanzada, es decir, empaquetar las funcionalidades exportando una interfaz de programación de aplicaciones (API por su siglas en inglés) que puede ser utilizada de forma encapsulada y separada por una aplicación anfitrión, escrita teóricamente en cualquier lenguaje de programación. Una de las aplicaciones que trabaja bajo este esquema de complementos o componentes es el navegador web, este diseño ha permitido contar con grandes repositorios que extienden las funcionalidades del navegador casi para cualquier uso.



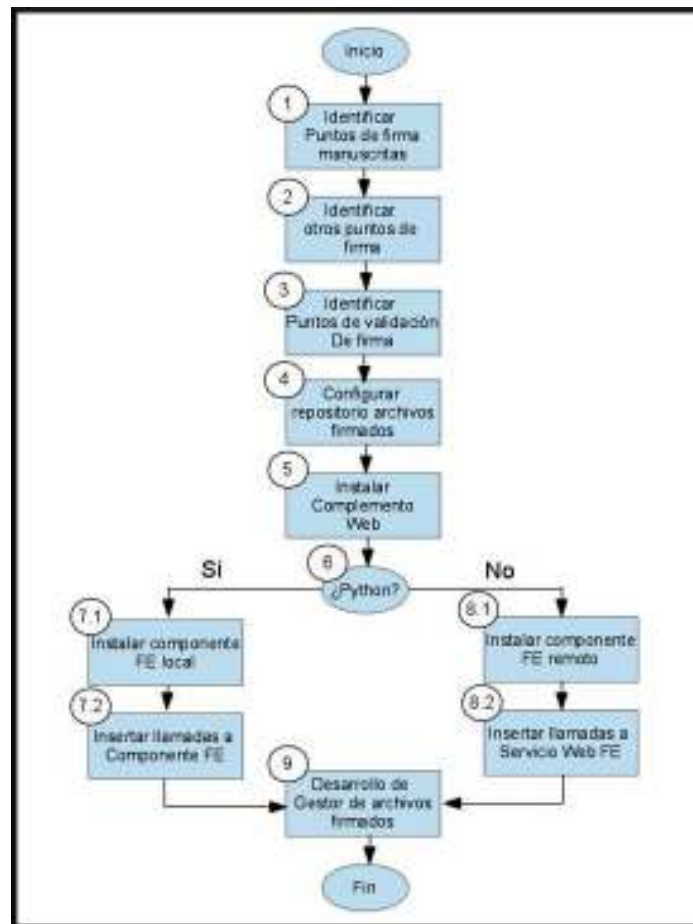
**Figura 6.1** Diagrama UML de acoplamiento

La figura 6.1 muestra un diagrama en lenguaje UML del componente y su conexión con un sistema informático. Existen tres tipos de funcionalidades que exporta el ComponenteFEA: “Firmar”, interfaces para firma electrónica y digital; “Validar”, interfaces para validación fuera de línea y en línea de certificados electrónicos; y “Gestionar”, interfaces para el almacenamiento y búsqueda de archivos firmados.

A nivel de lenguaje de programación se provee un paquete o *package* para *Python* que está construido envolviendo una librería de firma electrónica avanzada escrita en lenguaje C/C++. El listado 1 muestra los métodos que son accesibles desde *Python*.

#### 6.4.2. Método de conexión

El diagrama de flujo de la figura 6.2 muestra los pasos a seguir para incorporar el ComponenteFEA dentro de un proceso de una organización. Los primeros dos pasos de este diagrama corresponden a la identificación de los puntos de firma y validación dentro del proceso de negocio, para luego conectar los métodos (mensajes) correspondientes del ComponenteFEA en dichos puntos.



**Figura 6.2** Diagrama de flujo para el acoplamiento del ComponenteFEA

En un siguiente paso y dependiendo del tipo de proceso a automatizar se adoptará un esquema de conexión para el servidor. En esta fase se establecen algunos aspectos importantes relativos al sistema informático a colocar en funcionamiento, entre estos están la existencia de un sistema automatizado, el tipo de lenguaje de programación y sistemas operativos a utilizar, el soporte de la PKI, la asignación de las tarjetas inteligentes, entre otros.

En este punto el desarrollador tiene la libertad de utilizar el componente de firma según su criterio, sin embargo, puede seguir algunas pautas relacionadas con el proceso a automatizar. Si el proceso no se encuentra automatizado se recomienda seleccionar para el desarrollo de software el lenguaje *Python*. Para el caso anterior o si el sistema se implementó utilizando este lenguaje se sigue el paso 7.1 de la figura 6.2 que corresponde con la instalación del componente "servidor" para la firma electrónica avanzada.

En el caso de que los procesos de negocio se encuentren automatizados bajo un lenguaje diferente a *Python*, se utiliza la interfaz de servicios web<sup>2</sup> que provee el ComponenteFEA (Paso 8.1 de la figura 6.2).

Un tema a tomar en cuenta es el relativo al tipo de repositorio donde se almacenan los archivos firmados. El ComponenteFEA genera archivos tipo XAdES con extensión *.bdoc*. Para este fin puede utilizarse un directorio en el sistema de archivos o un gestor de base de datos relacional. En este punto también hay que trabajar sobre el esquema de nombres, es decir la forma como se identifican unívocamente los archivos para que puedan ser encontrados. Para ello se puede utilizar la vinculación de metadatos en los registros de las tablas de la base de datos relacional, o simplemente asignar un nombre como clave única a los archivos firmados.

Como último paso se debe habilitar un módulo para gestionar los archivos firmados (paso 9 de la figura 6.2), es decir, proveer una interfaz de usuario para las acciones de visualización de propiedades de archivos, validación de firmas electrónica, búsqueda, entre otras. Estas funcionalidades las provee el ComponenteFEA mediante los métodos que se nombran en la sección "Métodos para Gestión de archivos" del Listado 1, y pueden ser extendidas utilizando algunas de las funcionalidades del gestor de datos que se utilice.

## 6.5. Casos de estudio

A continuación se muestran tres casos de integración utilizando un mismo proceso con diversos sistemas informáticos. El proceso tratado es el conocido como "Orden de compra", el cual está presente en muchas organizaciones. Consiste en realizar un proceso de negocio con la finalidad de obtener un conjunto de productos o servicios necesarios para la organización a través de una búsqueda y evaluación de un cierto número de cotizaciones y que siguen una serie de criterios, como por ejemplo, las características de calidad y precio. El proceso en pasos se puede describir así:

1. Generar una requisición o documento de solicitud para el conjunto de productos o servicios
  - Firma del solicitante
2. Obtener por los menos  $n$  ( $n \geq 2$ ) cotizaciones para el conjunto de productos o servicios
3. Seleccionar una cotización y generar un acta
  - Firma del analista de compras
4. Generar una orden de compra
  - Firma del gerente del departamento

Generalmente este proceso se lleva a cabo utilizando firmas manuscritas en coordinación con un sistema informático: se imprime desde el sistema el documento (requisición, acta u orden de compra), se firma, y luego se actualiza la información en el sistema informático.

Para el caso de estudio planteado se puede sustituir la primera, la segunda o las tres firmas manuscritas por sus respectivas firmas electrónicas. También es posible agregar firmas electrónicas en puntos donde no existen firmas manuscritas.

La segunda funcionalidad a conectar del ComponenteFEA es la validación de los documentos firmados electrónicamente. Para ello se identifican los puntos donde se actualiza la información sobre la firma manuscrita. Una tercera funcionalidad es la que tiene que ver con la visualización de los atributos de los documentos firmados electrónicamente.

Después del proceso de identificación, para cada punto que se determinó en la fase anterior, se incorporan los métodos del ComponenteFEA con llamadas locales o remotas según sea el caso. A continuación se presentan tres implementaciones del proceso "Orden de compra" para tres sistemas informáticos diferentes.

<sup>2</sup>La interfaz de servicios web está disponible en: <http://bazaar.launchpad.net/~signature/esignature/bdoc/files/head:/server/>

### 6.5.1. Caso OpenERP

OpenERP<sup>3</sup> es un software de Planificación de Recursos Empresariales (ERP, por sus siglas en inglés), software libre, que tiene un gran número de instalaciones. En su base incluye el proceso de "Orden de compra". Para realizar el acoplamiento se creó un nuevo módulo de OpenERP. Se identificaron los puntos de firma y validación y se sustituyeron por las llamadas respectivas al ComponenteFEA. Como elemento agregado se creó un nuevo módulo basado en bandejas de documentos -archivos generados por OpenERP- (similar a las usadas en los clientes de correo electrónico) asociadas a los documentos a ser firmados electrónicamente.

La figura 6.3 muestra la interfaz de usuario para gestionar los archivos firmados electrónicamente. Los usuarios autorizados pueden utilizar una tarjeta inteligente para firmar los documentos correspondientes al proceso de "Orden de compra", teniendo la misma validez legal (especificado por las políticas de la PKI y la legislación del país) que la firma manuscrita. Primero el solicitante firma la requisición, y este documento se envía a la bandeja del analista de compra, quién busca las cotizaciones correspondientes y selecciona el conjunto de productos a comprar. Se generan los documentos "Acta" y "Orden de compra", este último es enviado a la bandeja del gerente quién lo firma para aprobar la compra del conjunto de productos o servicios seleccionados.

OpenERP provee al desarrollador patrones Modelo-Vista-Controlador (MVC) y un motor de flujo de trabajos o *Workflow* para implementar nuevas funcionalidades. Usando estas herramientas los documentos firmados se vinculan al modelo de datos y las validaciones de firma electrónica se realizan extendiendo el flujo de trabajo relacionado con el proceso "Orden de compra" base de OpenERP.

La última captura de pantalla de la figura 6.3 muestra un cuadro de diálogo que pide un PIN o contraseña al usuario. Esta interfaz forma parte del complemento Web que debe ser instalado en el cliente (navegador) y que tiene interacción con el certificado firmante contenido en una tarjeta inteligente.

### 6.5.2. Caso SAID

SAID<sup>4</sup> es un sistema administrativo que incluye procesos contables y administrativos para instituciones que operen en el sector público venezolano. Entre los procesos que implementa SAID está el de "Orden de compra", que incluye entre sus capacidades la posibilidad de utilizar firmas electrónicas basadas en el formato PKCS#7.

El sistema fue escrito en PHP Versión 4.X, y es de código libre. Los puntos de firma y validación están claramente identificados, ya que son los indicados por las firmas electrónicas, en este caso solo se sustituyen las llamadas a la API del motor criptográfico local, por llamados a los servicios web del ComponenteFEA. El listado 2 muestra las llamadas que se insertaron en el código fuente para extender el sistema de tal manera que funcione con firmas electrónicas avanzadas. El repositorio de archivos firmados a utilizar es PostgreSQL Versión 8.4 (El mismo que utiliza SAID). El listado 2 muestra el código en PHP para validar una firma electrónica y mostrar los firmantes de un documento del proceso de Orden de compra: requisición, acta u orden. Después de realizar la conexión al servidor *localhost* por el puerto 4242, se procede a abrir un archivo firmado con el método "openBDocContainer" a través de una llamada remota, luego se utiliza el método "validateSignature" para validar la firma, y finalmente se listan todos los firmantes utilizando el método "subjectCertificateCommonName".

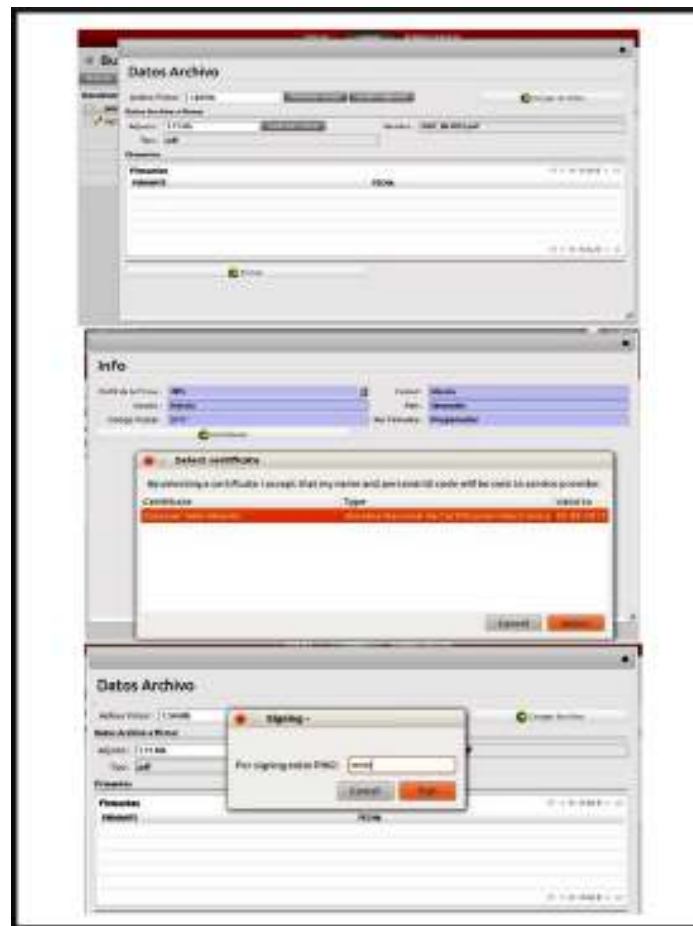
```
<?php

include('xmlrpc.php');

$connec = new XMLRPCClient('localhost:4242');
$idificador = 'prueba1';
$connec->__call('init', array($idificador));
$connec->__call('openBDocContainer',
```

<sup>3</sup> Ver la dirección web: <http://www.openerp.com>

<sup>4</sup> Ver la dirección web: <http://said.cenditel.gob.ve/wiki>



**Figura 6.3** Interfaz de usuario OpenERP para el ComponenteFEA

```

array($identificador,
'detalle_curso.odt.bdoc'));
$resp = $connec->__call('signatureCount',
array($identificador));
$firmanter = Array();
for($pos=0; $pos<$resp; $pos++)
{
    $datos = Array();
    $valida = 'No válido';
    if($connec->__call('validateSignature',
    array($identificador,$pos)))
    {
        $valida = 'Válido';
        $nombre =
        $connec->
        __call('subjectCertificateCommonName',
        array($identificador,$pos));
        $firmanter[] = array('nombre'=> $nombre,
        'valida'=>$valida);
    }
}

```



```

}
}

for($i=0;$i<count($firmantes);$i++)
{
echo "{$firmantes[$i]['nombre']}"
{$firmantes[$i]['valida']}\n";
}
?>

```

### Listado 2. Conexión mediante servicios web-rpc desde SAID al ComponenteFEA

De forma similar al caso OpenERP, se provee un complemento para el navegador de tal manera que los usuarios puedan realizar la firma de forma remota, utilizando una tarjeta inteligente desde su estación de trabajo. Luego el documento se procesa por el sistema SAID, y se almacena en la base de datos del servidor.

#### 6.5.3. Caso Flujos de Trabajo

El proceso especificado en esta sección puede modelarse usando un motor de flujo de trabajo. Los flujos de trabajo son ampliamente utilizados para modelar procesos a través de un lenguaje descriptivo como BPM o BPEL [16]. Para implementar el proceso de “Orden de compra” se utilizó el motor SAFET [17], ya que incorpora el ComponenteFEA nativamente, solo se necesitan especificar los puntos en el proceso donde se requiere la firma electrónica. La validación la realiza el motor de forma automática. Para este caso los pasos 1 y 2 del Diagrama de flujo para el acoplamiento del ComponenteFEA, se realizan sin la necesidad de agregar o modificar código fuente, solo se especifica en el archivo de definición de flujo.

El listado 3 muestra la definición de la acción de firma electrónica en un flujo de trabajo (SAFET). El usuario definido por el *NombreComunUsuario* debe firmar electrónicamente el documento de requisición para pasar a la siguiente actividad que en este caso se denominada *Cotización*. La sentencia *vRequisicion SIGN NombreComunUsuario* indica al motor de flujo de trabajo lo descrito anteriormente.

```

<task id="Requisicion"
  title="Acción de solicitud de bien o servicio" >
<port side="forward" type="split" >
<connection source="Cotización"
query="vRequisicion SIGN NombreComunUsuario"
options="" >
</connection>
</port>
<variable id="vRequisicion" scope="task"
tokenlink=""
documentsource="select id,
nombre,descripcion,
fechageneracion
from requisiciones" >
</variable>
</task>

```

### Listado 3. Tarea de firma de requisición usando SAFET (XML)

## 6.6. Conclusiones

En un mediano plazo la firma electrónica avanzada puede consolidarse como una tecnología fundamental en los procesos de negocio ya que propone la digitalización de un elemento imprescindible en este contexto

como lo es la firma manuscrita. Los retos de la digitalización son diversos y complejos, y tienen que ver con aspectos disímiles como lo son por ejemplo los formatos de archivo de firma electrónica y la ergonomía para el uso de esta tecnología.

En este trabajo se detalla un método para la integración de un componente de software con sistemas informáticos que automatizan procesos de negocio. En la fase de acoplamiento se define la identificación de puntos de firma electrónica, se especifica la validación de los certificados firmantes por una PKI, se muestra la habilitación del navegador web para la firma electrónica (basada en tarjetas inteligentes) a través de un complemento y se discute sobre los parámetros de seguridad de los formatos de firma electrónica. Las tareas como la construcción de un gestor de archivos firmados se proponen como una actividad complementaria.

Con la finalidad de mostrar la aplicación del método propuesto en sistemas en situaciones reales se mostraron tres casos de estudio, cada uno con sus particularidades. El acoplamiento del ComponenteFEA con los sistemas informáticos OpenERP, SAID y SAFET siguen el método descrito en el trabajo, evaluando para todos los casos especialmente el tipo de conexión a utilizar (local o remota), el tipo de almacenamiento y el procedimiento para la conexión en los puntos de firma electrónica y validación.

El análisis de vulnerabilidades es un tema omnipresente en el área de seguridad informática, y está relacionado con este trabajo a través del análisis de los formatos, protocolos y tecnologías utilizados en el proceso de integración.

Existen otros aspectos que no se discuten en este trabajo pero que se consideran importantes para la aprehensión de la tecnología de firma electrónica. Entre ellos se pueden señalar la mejora de la experiencia del usuario y la visualización de los archivos de formato XML firmados electrónicamente.

En el tema específico de integración, en [2] se discute sobre la necesidad de abrir el compás de aplicaciones compatibles con la tecnología de Firma Electrónica Avanzada, y en general, sobre la asunción de un nuevo paradigma en el despliegue de procesos de negocio.

## REFERENCIAS

---

1. Portal del DNI Electrónico Español. <http://www.dnielectronico.es/>, 2012.
2. Andreas Poller, Ulrich Waldmann, Sven Vowe, and Sven Turpe. Electronic identity cards for user authentication promise and practice. *IEEE Security & Privacy*, 10:46–54, 2013.
3. Oficial gateway to Estonia. <http://estonia.eu/about-estonia/economy-a-it/e-estonia.html>, 2013.
4. Campderrich Falgueras. *Ingeniería del Software*. Editorial UOC, Barcelona, España, 2003.
5. Directiva 1999/93/CE del Parlamento Europeo y del Consejo. [http://www.cert.fnmt.es/legsoporte/D\\_1999\\_93\\_CE.pdf](http://www.cert.fnmt.es/legsoporte/D_1999_93_CE.pdf), 1999.
6. D. Cooper, S. Santesson, et al. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Request for Comments (RFC) 5280. <http://www.ietf.org/rfc/rfc5280.txt>, 2013.
7. PKCS#7. Cryptographic Message Syntax. <https://tools.ietf.org/html/rfc2315>, 2013.
8. ETSI. PAdES. PDF Advance Electronic Signatures. <http://www.etsi.org/standards-search>, 2013.
9. M. Bartel, J. Boyer, et al. XML Signature Syntax and Processing (Second Edition). W3C Recommendation 10 June 2008. <http://www.w3.org/TR/xmlsig-core/>, 2013.
10. Formato para firmas electrónicas. <http://www.signature.it/-TOOLS/Bdoc-1.0.pdf>, 2013.
11. T. Neubauer, E. Weippl, and S. Biffl. Digital signatures with familiar appearance for e-government documents: authentic PDF. *Proceedings of the First International Conference on Availability, Reliability and Security*, pages 723–731, 2006.
12. Richardson Clay, Avondolio Donald, et al. *Professional Java, JDK*. Wrox, 2005.
13. J. Cruellas, G. Karlinger, et al. XML Advanced Electronic Signatures (XAdES). <http://www.w3.org/TR/XAdES/>, 2003.
14. J. Galvin, S. Murphy, S. Crocker, and N. Freed. Security Multiparts for MIME. Multipart/Signed and Multipart/Encrypted. <http://tools.ietf.org/html/rfc1847>, 2013.
15. RSA Laboratories. PKCS#12. Personal Information Exchange Syntax Standard. <https://www.rsa.com/rsalabs/node.asp?id=2138>, 2013.
16. Matjaz Juric and Mathew Benny. *Business Process Execution for Web Services BPEL and BPEL4WS*. Packt Publishing, 2006.

17. A. Araujo and V. Bravo. SAFET: Sistema para la generación de aplicaciones de firma electrónica. *Revista Puente*, 6, 2011.



# MODELO DE PROTOCOLO PARA UN SISTEMA ANÓNIMO BASADO EN ESTRATEGIAS BIO-INSPIRADAS

---

RODOLFO SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

## Resumen

En este artículo se propuso utilizar algunas herramientas provistas en el área de la Computación Emergente, específicamente en Inteligencia Artificial Distribuida (IAD), y en particular se utilizaron las Colonias Artificiales de Hormigas para construir sistemas anónimos que tengan la virtud de poseer niveles de anonimato aceptables a un bajo costo. Este costo se refiere a un criterio de rendimiento comúnmente utilizado en los procesos de los sistemas de enrutamiento en telecomunicaciones, tal como son los tiempos de respuesta (latencia), consumo de recursos de la red, entre otros.

## 7.1. Introducción

Para preservar la privacidad de los datos de cada una de las personas que participan en una red de interacción, tal como Internet, se deben utilizar herramientas que sean capaces de proveer protección contra al menos algunos de los ataques típicos. Los ataques en este caso de estudio en particular están orientados, sin autorización, a obtener información privada de los usuarios, incluyendo su propia identidad. Para contrarrestar este tipo de ataques se han propuesto varias ideas que apuntan a establecer cierto nivel de Anonimato, el cual en la

mayoría de los casos tienden a socavar el rendimiento de las comunicaciones. Esto es aun un problema abierto: los sistemas anónimos aún necesitan asegurar el Anonimato a un bajo costo (bajos tiempos de respuesta, bajo consumo de recursos, mayor usabilidad, etc.), y a esto es lo que se le denomina *Anonimato Eficiente*. Este trabajo presente un nuevo enfoque que aplica por primera vez la idea de utilizar la Inteligencia Artificial Distribuida en esta rama de la seguridad en las Tecnologías de Información y Comunicación (TIC), esto quiere decir que se le delega la responsabilidad de alcanzar niveles de Anonimato Eficiente a la Inteligencia Artificial Distribuida, específicamente se propone utilizar las Colonias Artificiales de Hormigas.

## 7.2. Colonias Artificiales de Hormigas en Anonimato

Considerando las ideas propuestas en los sistemas anónimos probabilísticos [1, 2, 3, 4] y las características de los Colonias Artificiales de Hormigas utilizadas en las redes de telecomunicaciones [5, 6, 7], se propone seleccionar las rutas de los mensajes de forma probabilística, utilizando las probabilidades que configuran los agentes móviles adaptativos (las hormigas). Estas rutas, teniendo componentes probabilísticos pueden, dependiendo de los parámetros de configuración, proporcionar ciertos niveles de Anonimato. En este sentido, se podría tener un “control inteligente” sobre los tiempos de respuesta generados y se podría tener un “control inteligente” sobre otros índices que pudiesen ser incorporados, tal como el consumo de recursos (balanceo de cargas).

Se propone mimetizar los mensajes reales con los agentes, esto es, cada mensaje tiene la misma estructura que las hormigas, y la única diferencia entre ellos radica en el contenido del mensaje, estos mensajes mimetizados se encriptan con las claves públicas de los nodos destino. Para hacer similar sus tamaños, se propone utilizar un tamaño único para el envío de mensajes y para cada agente, incluyendo la estructura de datos que almacena la información necesaria para actualizar las tablas de enrutamiento de cada nodo, más un relleno inválido y la clave pública del destino. Si un mensaje se fragmenta para cumplir con el requisito del tamaño único, el mismo es reensamblado en el nodo destino, utilizando un número de secuencia establecido por el nodo emisor. Los fragmentos de los mensajes también tienen la tarea de actualizar las tablas de enrutamiento de los nodos que visitan, de esta manera los atacantes no pueden distinguir entre las hormigas y los mensajes reales. De este modo, se puede comparar los mensajes enviados con hormigas de carga que llevan el alimento a los nidos, y es por esto que se identifican dos tipos de hormigas, las de carga y las exploradoras, sin tener diferencias aparentes.

Se utiliza una estrategia de cifrado por capas, cada nodo que una hormiga visita cifra la información relacionada al nodo anterior con una técnica de cifrado simétrico, e involucra solo la clave del nodo anterior, y para alcanzar cada destino, incluyendo el final, se pueden registrar sólo los nodos previos, y no la ruta completa hacia el origen. Para hacer la ruta de retorno (respuesta del nodo destino), este nodo final envía su respuesta al nodo anterior, y éste descifra la capa que contiene la información del nodo anterior a él, y así hasta llegar al nodo origen (el emisor).

Para optimizar el o los criterios de rendimiento usualmente utilizados en los sistemas de enrutamiento y a su vez incrementar los niveles de Anonimato, se debe configurar apropiadamente la tabla de rutas. Para hacer ésto, cada vez que una hormiga se mueve de un lugar a otro, actualiza la tabla de rutas. Para cambiar las probabilidades de las rutas, se selecciona un mecanismo basado en los criterios de rendimiento.

En los pasos siguientes se muestra el proceso:

- A. Se considera un sistema de  $N$  nodos, formando una red P2P (tal como Gnutella u otra con características similares), junto con sus servidores bootstrap.
- B. Se configuran los valores de los parámetros a utilizar, junto con el índice de uniformidad.
- C. Cada nodo participante solicita a uno o varios servidores una lista de los otros nodos en la red. Esta lista contiene sus claves públicas (certificados electrónicos).
- D. Se inicializan la tablas de rutas con la probabilidad  $1/M$ .  $M$  depende del número de vecinos que cada nodo posea.

- E. El sistema se representa por un grafo el cual forma el espacio de solución por el cual viajarán las hormigas.
- F. El procedimiento siguiente se repite sobre el grafo hasta alcanzar una solución estable:
  1. Se generan  $m$  hormigas exploradoras en cada nodo.
  2. Por cada  $N - 1$  lugares desde cada nodo se envían  $m$  hormigas exploradoras que escogen el salto a nodo vecino utilizando las probabilidades de transición de la tabla de rutas.
  3. Se actualizan las tablas de rutas.
- G. Cuando un nodo envía un mensaje anónimamente, éste lo cifra con la clave pública del nodo receptor y utiliza una estructura de datos similar al de las hormigas exploradoras, es decir, se crea una hormiga de carga. Cada hormiga de carga traslada una parte del mensaje, el cual se fragmenta para que el tamaño de cada fragmento pueda cumplir con el requisito de igualar su tamaño con el de la hormiga exploradora. A cada fragmento del mensaje se le asigna un número de secuencia.
- H. Por cada salto de la hormiga, el nodo intermedio cifra la identidad del nodo anterior con su clave privada.
- I. Cuando una hormiga de carga alcanza el nodo final, y todas las otras hormigas de carga vinculadas a un mensajes también han llegado, es posible reensamblar el mensaje original descifrándolo con su clave privada, y utilizando los números de secuencia correspondientes.
- J. Para enviar un mensaje de respuesta, el nodo final utiliza el camino de retorno cifrado en capas.

### 7.3. Conclusión

Se propuso implementar un sistema distribuido P2P basado en anonimato probabilístico provisto por sistemas de colonias artificiales de hormigas. Para lograr esto se configuran los nodos participantes como potenciales enrutadores de los mensajes anónimos. Las rutas para los mensajes de envío se construyen en base a las estrategias propuestas en los sistemas de telecomunicaciones para optimizar criterios de rendimiento a través del uso de Colonias Artificiales de Hormigas. Una vez que se crean la rutas, el Anonimato se logra al seleccionar probabilísticamente las rutas de los mensajes enviados utilizando cifrado en capas establecido para la ruta de retorno o respuesta.

### Agradecimientos

Se agradece a José Lisandro Aguilar Castro por su revisión, consejos y recomendaciones sobre todo el contenido propuesto.

## REFERENCIAS

---

1. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 4, 1981.
2. G. Danezis, R. Dingledine, and N. Mathewson. Mixminion: Design of a type iii anonymous remailer protocol. *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, 2003.
3. C. Díaz and A. Serjantov. Generalising mixes. *Proceedings of Privacy Enhancing Technologies workshop*, pages 18–31, 2003.
4. R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium*, 2004.
5. G.D. Caro and M. Dorigo. Antnet: Distributed stigmergetic control for communications networks. *Journal of Artificial Intelligence Research*, 1998.
6. T. White and B. Pagurek. Connection management using adaptive mobile agents. *Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications*, pages 802–809, 1998.
7. R. Schoonderwoerd. Ant-based load balancing in telecommunications networks. *Adaptive Behavior*, 5:169–207, 1997.





# SISTEMA DE MEDICIÓN DE ANONIMATO

---

RODOLFO SUMOZA

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

### Resumen

Este trabajo propone el uso de un sistema de medición para anonimato basado en las características de sus propiedades principales: el índice de uniformidad de la distribución de probabilidad y el tamaño del conjunto anónimo. En las propuestas previas, la medida más ampliamente utilizada es la entropía, un índice utilizado y propuesto en la Teoría de la Información, el cual tiene algunos inconvenientes con respecto a la medición del Anonimato según las propiedades mencionadas, en primer lugar dichas propiedades no se representan directa y explícitamente con este índice, y al ser un índice logarítmico, no representa de forma adecuada comportamientos lineales en el Anonimato. Para medir el índice de uniformidad se propone utilizar el criterio del error cuadrático mínimo y como segunda propuesta se plantea utilizar el criterio de divergencia de Jensen-Shannon. Para medir el tamaño del conjunto anónimo se propone utilizar una función de  $N$  (número de entes del conjunto anónimo).

## 8.1. Introducción

Los sistemas de medición utilizados para cuantificar los niveles de Anonimato de los sistemas, mecanismos y herramientas aun se consideran un problema abierto. Se han propuesto algunas alternativas para este propósito, y la que más ampliamente se ha utilizado es la que se basa en una medida utilizada en la Teoría de la Información: la entropía. Sin embargo ésta no representa explícitamente las características fundamentales del Anonimato: el tamaño del conjunto anónimo y el índice de uniformidad de la distribución de probabilidad vinculada al conjunto anónimo. En este trabajo, se propone utilizar como alternativa dos índices para la medición del Anonimato, que explícitamente representen sus principales características. Por un lado el tamaño del conjunto anónimo puede ser representado a través de una función de  $N$  (el número de entes que componen al conjunto) y el índice de uniformidad puede ser representado utilizando uno de los siguientes indicadores: el Error Cuadrático Medio (RMSE por sus siglas en inglés) o el criterio de divergencia de Jensen-Shannon (CDJs por sus siglas en inglés).

En Pfiztmann et al. [1] establecieron una terminología ampliamente utilizada para estandarizar los términos utilizados en el contexto del Anonimato, en la cual ésta establece que un sujeto es anónimo cuando no puede ser diferenciado de los otros sujetos pertenecientes al mismo conjunto, denominado el conjunto anónimo. Describiendo el Anonimato en estos términos, se establece que sus niveles se incrementan si el tamaño del conjunto anónimo crece y cuando la distribución de probabilidad que establece un atacante sobre los miembros de ese conjunto anónimo tiende a ser uniforme. La proximidad de una distribución de probabilidad cualquiera a una distribución uniforme es a lo que se le denomina el índice de uniformidad de la distribución de probabilidad.

En la mayoría de la documentación hasta ahora difundida se utiliza como medida de referencia una obtenida de la Teoría de la Información: la entropía, y puede verse su representación tal como la definió Shannon en [2]. Esta propuesta fue discutida en los trabajos de Díaz et al. [3] y Serjantov et al. [4], y desde entonces ha sido utilizada como base de medición en varios otros trabajos como el de Deng et al. [5], Edman et al. [6] y Gierlichs et al. [7]. Sin embargo, esta medida no representa explícitamente las características que describen al Anonimato y que fueron explicadas previamente, particularmente el índice de uniformidad.

## 8.2. Trabajos Relacionado

Se han hecho varias propuestas para cuantificar el grado o nivel de anonimato provisto por los sistemas anónimos. En [8] definen el grado de Anonimato como  $1 - p$ , donde  $p$  es la probabilidad asignada por el atacante a un sujeto particular. En [9] definen el grado de anonimato como  $A = \log_2(N)$ , donde  $N$  es el número de sujetos (usuarios) del sistema. Este grado solo depende del número de usuarios del sistema, y no toma en cuenta la información que el atacante puede obtener a través de la observación del sistema o por otros medios. En [3] y [4] proponen medir la información que obtiene el atacante, considerando el conjunto completo de usuarios la probabilidad que le asigna, y para ello como medida proponen la entropía utilizada en la Teoría de Información (usan la entropía definida por Shannon en [2]). Ninguna de las propuestas anteriores representa explícitamente el tamaño del conjunto anónimo y el índice de uniformidad. Además en [3] proponen utilizar un grado de anonimato normalizado, pero esta medida puede alcanzar su máximo nivel de anonimato con un  $N = 2$  (tamaño del conjunto anónimo), contradiciendo una de las características fundamentales del Anonimato definida en [1]: Los niveles de Anonimato se incrementan si se incrementa el tamaño del conjunto anónimo y el índice de uniformidad de la distribución de probabilidad. En [5], [6], [7] utilizan la entropía de Shannon con un enfoque diferente pero adoleciendo de los mismos problemas. Cuando utilizan la entropía, están utilizando una función logarítmica, lo que significa que no se tienen grados de medición lineales para comparar los sistemas. Por ejemplo, si se tienen 4 sistemas, y los atacantes no tienen ninguna información de sus usuarios, esto quiere decir, que le asignan una distribución de probabilidad uniforme a cada conjunto anónimo, esto es si el primer sistema tiene  $N = 100$  sujetos, el segundo tiene  $N = 200$  sujetos, el tercero tiene  $N = 400$  sujetos y el cuarto tiene  $N = 800$  sujetos, los grados de Anonimato utilizando la entropía son: 6,6438, 7,6438, 8,6438, 9,6438, respectivamente. Estos escenarios, con la misma distribución de probabilidad y con diferente  $N$  (el doble del conjunto anterior) debería tener el doble del grado de Anonimato comparando

cada uno con el siguiente, pero esto no sucede debido a que la entropía utiliza una función logarítmica y no lineal.

### 8.3. Propuesta

Se propone utilizar dos índices para medir el Anonimato, cada uno para establecer los niveles de cada característica fundamental del Anonimato: Uno para medir el tamaño del conjunto anónimo:  $N$  o  $1/N$ , donde  $N$  es el número de sujetos o elementos, y uno para medir el índice de uniformidad de la función de distribución de probabilidad asignada por el atacante. Para medir el índice de uniformidad se proponen utilizar una de las siguientes dos métricas: La raíz del error cuadrático medio (RSME) o el criterio de divergencia de Jennesen-Shannon (DJS).

#### 8.3.1. Raíz del Error Cuadrático Medio - RSME

Este término se utiliza para estimar el error de la varianza, este es el error residual de la suma de los cuadrados divididos por el grado de libertad. En análisis de regresión, es una cantidad observada dada una muestra en particular, y depende de dicha muestra. Además, este término es referido al error fuera de la muestra: el valor medio de las desviaciones cuadráticas de las predicciones de los valores de verdad, sobre un espacio fuera de la muestra, generado por un modelo estimado sobre un espacio muestral particular. Ésta también es una cantidad observada, y varía según la muestra y según el espacio fuera de la muestra probado.

$$RSME = \frac{\sqrt{(\bar{X} - X)^2}}{n(n-1)} \quad (8.1)$$

En este caso, se propone utilizar  $p_i = \frac{1}{N}$  (probabilidades en una distribución uniforme) para representar  $\bar{X}$ , y  $p_i$ , la probabilidad asignada por el atacante, se representa con  $X$ . Esta medida permite establecer la "distancia" de la distribución de probabilidad del atacante a la distribución uniforme.

$$RSME_a = \frac{\sqrt{\sum_{i=1}^N (\frac{1}{N} - p_i)^2}}{N(N-1)} \quad (8.2)$$

Si un sistema tiene un  $RSME_a \approx 1$ , esto quiere decir que provee un muy bajo nivel de anonimato. Si otro sistema tiene un  $RSME_a \approx 0$ , quiere decir que provee un buen nivel de anonimato. Pero también se debe observar el tamaño del conjunto anónimo para tomar una visión real del sistema.

#### 8.3.2. Divergencia de Jennesen-Shannon

La divergencia de Jensen-Shannon es un método popular para medir la similitud entre dos o más distribuciones de probabilidad. Se basa en la divergencia de Kullback-Leibler, con la notable y útil diferencia que siempre da como resultado un valor finito. La raíz cuadrada de la divergencia de Jensen-Shannon es el índice que se propone para representar el índice de uniformidad en Anonimato.

$$JSD(P_1, P_2) = H\left(\sum_{i=1}^2 \pi_i P_i\right) - \sum_{i=1}^2 \pi_i P_i \quad (8.3)$$

$$JSD_a(P_1, P_2) = \sqrt{JSD(P_1, P_2)} \quad (8.4)$$

donde  $\pi_i$  son los pesos para las distribuciones de probabilidad  $P_1, P_2$ , en este caso  $\pi_i = 1, \forall i = \{1, 2\}$ , y  $H(P)$  es la entropía de Shannon para la distribución  $P$ . En este caso,  $P_1$  es una distribución uniforme y  $P_2$  es la distribución de probabilidad del atacante.

Con este resultado se obtienen dos índices para representar el grado o nivel de Anonimato:

### 8.3.3. Resultados

**Opción 1:** Grado de Anonimato ( $AD$ ) utilizando RMSE para medir el índice de uniformidad de la distribución de probabilidad y  $1/N$  para medir el tamaño del conjunto anónimo.

$$AD = 1/N \pm MSE_a$$

**Opción 2:** Grado de Anonimato ( $AD$ ) utilizando JSD para medir el índice de uniformidad de la distribución de probabilidad y  $1/N$  para medir el tamaño del conjunto anónimo.

$$AD = 1/N \pm JSD_a$$

En ambos casos, el índice de uniformidad y el tamaño son expresados por separado pero no tiene el problema de linealidad de las otras métricas.

## REFERENCIAS

---

1. A. Pfitzmann and M. Hansen. Anonymity, unobservability, and pseudonymity: A consolidated proposal for terminology. [http://dud.inf.tu-dresden.de/Anon\\_Terminology.shtml](http://dud.inf.tu-dresden.de/Anon_Terminology.shtml), 2000.
2. C. Shannon. The mathematical theory for communications. *Bell Systems Technical Journal*, 30:50–64, 1948.
3. C. Díaz, S. Seys, J. Claessens, and B. Preneel. Towards measuring anonymity. *Designing Privacy Enhancing Technologies*, pages 54–68, 2002.
4. A. Serjantov and G. Danezis. Towards an information theoretic metric for anonymity. *Proceedings of Privacy Enhancing Technologies Workshop*, pages 54–68, 2002.
5. Y. Deng, J. Pang, and P. Wu. Measuring anonymity with relative entropy. *Proceedings of the 4th International Workshop on Formal Aspects in Security and Trust*, pages 65–79, 2007.
6. M. Edman, F. Sivrikaya, and B. Yener. A combinatorial approach to measuring anonymity. *Intelligence and Security Informatics*, pages 356–363, 2007.
7. B. Gierlichs, C. Troncoso, C. Diaz, B. Preneel, and I. Verbauwhede. Revisiting a combinatorial approach toward measuring anonymity. *Workshop on Privacy in the Electronic Society*, pages 111–116, 2008.
8. M. Reiter and A. Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1, 1998.
9. O. Berthold, A. Pfitzmann, and R. Standtke. The disadvantages of free mix routes and how to overcome them. *Proceedings of Privacy Enhancing Technologies Workshop*, pages 30–45, 2001.



# APORTES ESTRATÉGICO-POLÍTICOS EN IDENTIDAD DIGITAL

---



## EXPLORANDO EL SENTIDO DE LA IDENTIDAD DIGITAL PARA LA VENEZUELA DEL SIGLO XXI

---

JOSÉ J. CONTRERAS

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

### 9.1. ¿Identidad? ¿Identidad Digital?

Hace doscientos años, en 1818, Mary Shelley, publicó su archiconocida novela gótica “Frankenstein o el moderno Prometeo” bastante leída todavía en estos días. En ella, el Dr. Víctor Frankenstein toma retazos de cadáveres, los arma en un cuerpo, le aplica electricidad y logra darle vida. Se ha dicho mucho que la criatura del Dr. Frankenstein causaba miedo por su fealdad. Ciertamente. Sin embargo, se debería también decir que el terror que causa la criatura —la cual es siempre llamada como monstruo, animal o simplemente criatura— es precisamente su falta de nombre, su falta de identidad.

“Aquello que no puede ser nombrado no existe” dice Ramalle [1]. Pero esa *criatura* existía, era vista, sí era fea seguro, pero lo que más resaltaba de su monstruosidad era precisamente su carencia de nombre. No era un animal, no era un ser humano, se dudaría en decir hasta que era una cosa. La *criatura* de Frankenstein era completa otredad. Cuando logra comunicarse con su creador, le solicita que le haga una mujer. Necesitaba de vida social. Allí, en la vida social, surgiría el nombre y la identidad. Frankenstein no la hace... Y se desencadena

el drama de la obra. Al final de la novela, la creatura se humaniza al echar el cuento de su vida. Popularmente la gente llamó al monstruo “Frankenstein”, el apellido de su creador, a quién él veía como su padre.

Llama mucho la atención que a mediados de la segunda década del siglo XIX estuviese Shelley en Suiza escribiendo una novela en que la falta de identidad aparecía como una monstruosidad. Llama mucho la atención porque en 1819 estaba por estos lares del Trópico Simón Bolívar en el proceso de independencia americana. En su famoso discurso de Angostura, Bolívar caía en cuenta de que el proceso de independencia americana era un asunto muy particular. No se podía calcar otros modelos y otras leyes. No sólo porque operativamente no funcionasen, sino porque el pueblo venezolano era *otro* pueblo. Decía Bolívar que el pueblo venezolano “no es el europeo, ni el americano del Norte, que más bien es un compuesto de África y de América, que una emanación de la Europa; pues que hasta la España misma deja de ser europea por su sangre africana, por sus instituciones y por su carácter. Es imposible asignar con propiedad a qué familia humana pertenecemos” [2]. Para aquel momento puede verse cómo Bolívar había ya caído en cuenta que el problema de la independencia era un problema de identidad. *En qué familia nos clasificamos, quiénes somos... En ello somos venezolanos, somos colombianos, somos americanos.*

Venezuela nace como pueblo en la búsqueda por tener identidad en una época en la que la carencia de identidad resuena como monstruosidad.

Este cuento sobre el nacimiento de la nación venezolana contrasta mucho con la versión de Benedict Anderson sobre el nacimiento de las naciones, dominante en nuestros días. Según Anderson [3], las naciones surgen en la confluencia de tres grandes fenómenos: la caída de las grandes sociedades monárquicas, el declive de las lenguas sagradas (y privilegiadas) como el latín en favor de las lenguas vernáculos y la aparición de la prensa impresa capitalista. ¿Por qué? porque la prensa impresa capitalista facilitó y potenció que se reuniese una comunidad conformada alrededor de una misma lengua vernácula y de un mercado común que emergía a partir de la cercanía geográfica.

Pues bien, el caso venezolano no se adapta a estos patrones que narra Anderson. Venezuela nace como nación, sí, a partir de un interés mantuano por promover un mercado local que facilitase el intercambio comercial con otras naciones para romper con esa especie de monopsonio impuesto por la metrópoli y que exigía la compra de toda la producción por parte de España. Eso es correcto, y hasta allí compartiría mucho de lo dicho por Anderson. Pero también se debe recordar que, a partir del cambio fundamental que experimenta la revolución después de la caída de la 2<sup>da</sup> República, la epopeya independentista se distancia de la visión mantuana que celebraría la teoría de Anderson. Como bien lo dice Bolívar, citado párrafos arriba, la independencia venezolana se convirtió en un proceso de lucha por una identidad y construcción de la misma.

A partir de aquí fue posible la construcción colectiva de un imaginario de “nación” limitado por lo que anteriormente era una provincia del Reino de España a la que llamaban Capitanía General de Venezuela. Fue allí donde se reveló un pueblo que buscaba ser soberano, es decir, independizarse de la corona española y de su orden jerárquico y en el que apareció un profundo igualitarismo entre sus miembros. Igualitarismo conformado a partir de una fraternidad y confianza compartida de fondo. Esta utopía de fondo posibilitó la epopeya independentista que liberó un territorio dos veces más grande que el conquistado por Alejandro Magno y tres veces el de Napoleón Bonaparte. En el tiempo, esta epopeya terminaría posibilitando el surgimiento de seis naciones.

¿Qué tiene que ver esta dispersión con respecto a la Identidad Digital en nuestra época?... Respuesta: ¡Todo!.

Venezuela entró a la década de los noventa del siglo veinte viviendo un proceso de *globalización* en el que se pretendía homogeneizar a todas las naciones del mundo en una gran sociedad de mercado. Con la globalización, las naciones tendían a vivir un profundo proceso de transformación en el que, se esperaba, su sentido de identificación popular como *un* pueblo conformado a partir de un devenir común en función de un proyecto nacional, desaparecía para dar paso así a una sociedad de individuos asociados alrededor de un mercado común que los reunía. De la nación se pasaba a la sociedad de mercado.

Ahora bien, cuando parecía que este proceso ocurría como una posibilidad “inevitable” empieza a cobrar fuerza en Venezuela un movimiento de reacción popular, nacionalista y bolivariano. De esta manera, las elecciones presidenciales del año 1998 se vieron signadas por el interesante fenómeno de contar con dos contrincantes que simbolizaban de buena manera la lucha a la que se está aludiendo. Por una parte, se encontraba a Henrique Salas Römer, economista egresado de la Universidad de Yale, fiel expresión de la clase mantuana,



con un discurso apegado a las corrientes dominantes de la sociedad global de mercado. Del lado contrario se encontraba a Hugo Chávez Frías, comandante militar del ejército, fiel expresión de la mezcla racial venezolana con dominancia del indio y del negro y con un discurso nacionalista que evocaba a Bolívar, la independencia y nuestra identidad patria. En aquel diciembre de 1998 ganó Chávez y siguió ganando hasta el momento de su muerte en 2013.

El punto al que queremos aludir aquí es que Venezuela entra al siglo XXI en un conflicto de identidad cuya remembranza lleva a principios del siglo XIX. Venezuela comenzó el siglo XXI viviendo y sufriendo (quizá pariendo) un proceso constituyente de refundación en el que se llegó hasta a decidir, en plebiscito, cambiar el nombre de la nación al de “República Bolivariana de Venezuela”. Es en este contexto en el que aparece la pregunta por la “identidad digital” en Venezuela. La pregunta por la identidad en tiempos de revolución bolivariana.

## 9.2. El surgimiento de la Identidad

Hoy día en el que se tienen múltiples números de identificación, identificación biométrica, nombre y apellido, varios seudónimos en aplicaciones web, etcétera, parece casi inconcebible imaginar pueblos en los que la identidad surgiese como una sin mayor problema. MacIntyre [4] presenta un contexto interesante y que de alguna manera aparece como entraño en su extrañeza. MacIntyre [4] habla de las sociedades heroicas o sociedades homéricas.

El punto clave de estas sociedades heroicas<sup>1</sup> es que en ellas todo ser humano tenía su lugar predeterminado, sus privilegios y también sus deberes. Dice MacIntyre que en estas sociedades la estructura social y la moralidad eran una misma cosa. Es por ello que en las sociedades heroicas, Homero habla de “conocimiento” a la hora de saber qué hacer y cómo juzgar una situación. Solo en casos muy excepcionales un personaje hallaba difícil responder la pregunta “¿qué hacer?” puesto que su lugar en el orden social predeterminaba claramente “qué debía hacer”.

Las reglas ya brindadas que asignan a los hombres su lugar en el orden social y con él su **identidad**, también prescriben su deber y lo que les es debido, y cómo han de ser tratados y considerados si fallan, y cómo tratar y considerar a los otros si los otros fallan.<sup>2</sup> [4]<sup>3</sup>

La identidad proviene del orden social y ella no sólo hace referencia a un ser que se distingue de los otros, sino que en ella se determina todo lo que se es y se debe ser. Sin ese orden social, un ser humano no podría ser reconocido y no podría reconocerse a sí mismo. No tendría identidad. Aunque ello prácticamente no ocurría. Lo más parecido que encuentra MacIntyre a una situación de este tipo es el encuentro de Odiseo con los cíclopes quienes, simplemente, no reconocían la identidad humana<sup>4</sup>.

En la sociedad homérica “Yo debo hacer lo que debo hacer hasta mi muerte”. No hay posibilidad de separarse de su posición particular o incluso de cuestionarla. La identidad aquí no era problemática.

Pero luego empieza a tener lugar una separación en esa aparente unidad de mundo. Una separación en la que se presentan dos dominios: el público y el privado.

El dominio público refiere al espacio de la *polis*, refiere a la organización política. El dominio privado refiere al espacio de la casa y la familia. El dominio público refiere al espacio al que se accede como “igual”. El dominio privado es el espacio de la desigualdad. Mientras en el público se debate y persuade con argumentos, en el dominio privado se comanda y se ordena. El primero es espacio de escrutinio a la luz, el segundo se oculta en las entrañas oscuras del hogar.

El dominio privado refiere a la vida. El dominio público refiere al mundo. La casa atiende a las necesidades de la vida. Las actividades de la casa refieren al cuidado de los niños, al cultivo y la industria. Del dominio

<sup>1</sup> Si estas sociedades existieron realmente o no, no es asunto de este escrito. En cualquier caso, ellas aparecen como originarias de ese mundo occidental del cual somos también herederos.

<sup>2</sup> Énfasis del autor.

<sup>3</sup> A menos que se indique lo contrario, ésta y todas las traducciones realizadas en las citas fueron realizadas por el autor.

<sup>4</sup> Odiseo le dice a Polifermo: *preguntaste, cíclope, cuál era mi nombre glorioso y a decirte voy. Ese nombre es nadie. Nadie mi padre y mi madre me llamaron de siempre y también mis amigos.*

privado es la familia, la propiedad, los esclavos. El dominio público refiere al mundo en el sentido de ese segundo mundo artificial que construyen los seres humanos, que los separa de la naturaleza y en el cual se es efectivamente humano.

En la concepción de los griegos antiguos, el dominio público era de una jerarquía superior al dominio privado. Para acceder al dominio público debían tenerse cubiertas las necesidades básicas de la vida. Sólo si ello ocurría era posible trascender del dominio privado hacia el público. Las actividades de las mujeres y los esclavos eran propias de la casa, por ello no podían trascender al dominio público. Las actividades propias del artesano y del agricultor (la industria), también eran hogareñas, por eso ellas no podían trascender al dominio público.

Arendt [5] plantea que esta concepción de la superioridad del dominio público sobre el privado se basaba en la presunción de que la vida con otros seres humanos no era lo que podía llamarse fundamentalmente humano. La necesidad de la vida con otros era un asunto compartido con otros animales gregarios. Lo que era fundamentalmente humano era la organización política, que brindaba junto a la vida privada una suerte de segunda vida: la vida política. Por eso se consideraba al dominio público como de una estatura superior al dominio privado. El dominio público refería a lo que era fundamentalmente humano; el dominio privado refería a las necesidades biológicas de la vida. Cuando un individuo no podía trascender al dominio público, se consideraba un individuo “privado”, en el sentido que aún resuena un poco de persona de “menor rango”.

Sin embargo, eso no quiere decir que el dominio privado fuese de poca importancia. Si bien el dominio privado guardaba el sentido de “privativo”, y vivir enteramente en el dominio del hogar privaba de cosas esenciales a una verdadera vida humana (al punto que la felicidad era prácticamente imposible para los esclavos, mujeres, campesinos o artesanos), el dominio privado era concebido también como algo sagrado.

En los tiempos de la antigua Grecia los entes eran considerados como una aparición que provenían de lo oculto. Todo lo que *era*, era una revelación. De hecho, la verdad, *aletheia*, era un acto de revelación en el que se buscaba dar cuenta de cómo los entes llegaban a ser viniendo desde lo oculto hacia lo claro [6]. Este proceso de revelación era sagrado. “La sacralidad de esta privacidad era como la sacralidad de lo oculto, dígame, del nacimiento y de la muerte, del origen y del fin de los mortales quienes, como toda las criaturas vivientes, aparecen desde —y retornan a— la oscuridad del inframundo... [El hogar] es oculto porque el hombre no sabe de dónde proviene cuando nace y a dónde va cuando muere” ([5] Pp. 62, 63).

Las cosas propiamente humanas podían llegar a revelarse en el dominio público porque provenían del oscuro dominio privado. Mientras al dominio público se accedía en igualdad, el dominio privado era de dominación tiránica. Mientras en el dominio público se ejercía la persuasión de la verdad a través del debate y el diálogo, en el dominio privado se ejercía la dominación por la fuerza. Para poder acceder al dominio público debía dominarse la vida con propiedad. Mientras que ser político significaba alcanzar la mayor posibilidad de la existencia humana, el no tener propiedad de un lugar privado (como en el caso de los esclavos) significaba no llegar a ser apropiadamente humano.

Es a partir de esta cercanía entre el dominio privado y la propiedad de la casa, del cultivo, de la tierra, de los esclavos que tiene lugar esa concepción todavía actual de la “propiedad” en términos de “propiedad privada” e incluso de una cierta sacralidad todavía existente en el término mismo en tiempos tan no teístas como los contemporáneos y en los que la “propiedad” está prácticamente desapareciendo.

En ninguna época anterior, tanto de las épocas antiguas como en las medievales, podría concebirse al ser humano como un individuo a priori. Todo individuo se identificaba en su papel como miembro de una familia, de un linaje, de una ciudad, de una nación, de un reino. Es en este orden de ideas que aparecen los nombres que identificaban a una persona con un nombre particular y luego con algún tipo de antroponímico relacionado casi siempre con algún oficio o con algún lugar y siempre denominando no sólo a un individuo sino a una familia. La identidad designaba la individualidad a partir de quien se es en su familia, su oficio, su residencia, su orden social. La identidad cobraba sentido dentro del orden social. Insinuaba la revelación desde el dominio privado de la familia en el papel social del oficio y cercano siempre al lugar, a la ciudad, en la que se es y en la que es posible, para algunos, desplegar la humanidad en el dominio público.

Este modo de entender la identidad —desde el linaje, la ciudad y el oficio a partir del orden social— queda muy bien expresado por Mary Shelley en el primer párrafo del Capítulo 1 de la obra de *Marras* y en la que el Dr. Víctor Frankenstein se presenta a sí mismo:

Soy ginebrino de nacimiento, y mi familia es una de las más distinguidas de esa república. Durante muchos años mis antepasados habían sido consejeros y jueces, y mi padre había ocupado con gran honor y buena reputación diversos cargos públicos. Todos los que lo conocían lo respetaban por su integridad e infatigable dedicación. Pasó su juventud dedicado por completo a los asuntos del país, y sólo al final de su vida pensó en el matrimonio y así dar al Estado unos hijos que pudieran perpetuar su nombre y sus virtudes. [7]<sup>5</sup>.

En el transcurrir de la Modernidad esta situación cambia fundamentalmente y el orden social a partir del cual tiene lugar la identidad se resquebraja por completo. Pero, antes de entrar en esta aún nuestra época es pertinente que se haga un paréntesis para acercarse a entender mejor las distinciones entre “vida” y “mundo” por una parte, y entre “labor” y “trabajo” por la otra, y cuyo trastoque abrirá espacio para un desplazamiento fundamental en la noción de identidad.

### 9.3. “Vida” y “Mundo”; “Labor” y “Trabajo”

Arendt [5] hace una distinción que es útil para entender algunos asuntos que hoy aparecen como incuestionables. Arendt refiere a la labor como aquella actividad dirigida a atender las necesidades de la vida. Estas actividades no finalizan en una obra. La labor produce y aquello que se produce se consume. El producto de la siembra se consume y la labor del hogar se desvanece. El producto de la industria se usa y se gasta.

El trabajo, de manera contraria, es la actividad que se corresponde con la existencia humana como algo no-natural. Mientras el producto de la labor se consume en el ciclo de la vida, la obra del trabajo permanece hacia la eternidad. Mientras la labor se remite al ámbito hogareño, la obra del trabajo procura trascender por siempre. “La condición humana de la labor es la vida en sí misma... La condición humana del trabajo es la mundanidad”[5].

El dominio privado es claramente el ámbito de la vida y la labor. El hombre libre no labora. El hombre libre obra mundo: trabaja. El hombre libre domina el hogar y obra en el dominio público. La obra del hombre libre permanece. El esclavo, el artesano o el campesino laboran y producen objetos necesarios para la vida que se consumen y se gastan. Se labora desde el dominio privado, se trabaja para el dominio público.

El espacio público por excelencia es el ágora. El ágora es la plaza en la que tienen lugar los debates y los concursos públicos. Espacio en el que compete y gana el mejor. A menos claro está que la fortuna dictamine otro desenlace, en el ágora se revela el mejor argumento político y se distingue la mejor obra. En el ágora se revela la obra que hace mundo permanente.

El mercado es un espacio —quizá intermedio— en el que se intercambian públicamente productos de la labor. En el mercado se puja por el precio justo. El precio justo es producto del debate público, pero el producto intercambiado es de consumo perecedero. Del mismo modo lo es el proceso de intercambio el cual se agota con su realización. En esto, el mercado se diferencia del concurso y el debate público. El concurso, el debate, va revelando la mejora progresiva de las prácticas que en sus obras van realizando el mundo del dominio público que trascienden hacia la eternidad.

Pero como se decía anteriormente, en la Modernidad se trastoca fundamentalmente esta concepción del mundo y, con ello, se produce un cambio fundamental de la identidad.

### 9.4. El trastoque de la modernidad

En la modernidad tienen lugar dos desplazamientos de importancia cardinal: un cambio en la concepción fundamental del ser humano y una alienación del mundo. Se comenzará por este último.

En la modernidad lo que se hace común, lo que tiene lugar propiamente en el dominio público, es el cuidado por la propiedad. La propiedad deja de ser del dominio privado. Lo que domina ahora en el dominio público es la vida. En las épocas antiguas si un propietario hubiese escogido aumentar su propiedad como un fin en sí mismo en vez de hacer uso de ella como un medio para fortalecer su vida política, sería como si voluntariamente sacrificara la libertad para hacerse esclavo de las necesidades.

<sup>5</sup>El traductor en esta edición no aparece especificado en la obra

Es en esta época moderna que aparece el término “sociedad” en el sentido que se le da aún en nuestro tiempo. La palabra “sociedad” anteriormente refería a un grupo de personas que se asociaban en función de un objetivo concreto. Pero en la modernidad el término “sociedad” refiere a una organización de propietarios quienes, en vez de demandar acceso al dominio público gracias a su riqueza generada en el dominio privado, acudían al dominio público para demandar mayor protección de la sociedad con miras a una mayor acumulación de riqueza.

Un punto importante a hacer alusión es que en la modernidad ocurre también un desplazamiento del sentido de “propiedad” en el que el término deja de ser algo fijo que ocupa un lugar físico para pasar a tener su origen en el ser humano mismo. Es aquí cuando aparece el concepto marxista que veía al laborador proletario como un ser humano que de lo único que era dueño era de su propio cuerpo el cual ponía a disposición para ser explotado en retribución por un salario.

Se pierde así la diferencia entre los dominios público y privado. El mundo público común —que era el mundo real— y para el que obraba el hombre libre desaparece. La producción industrial que antiguamente estaba confinada al ámbito hogareño, en una revolución que logró alcanzar hasta los últimos confines del planeta, se convirtió en el motor que reunió al pueblo en nación. Así, lo que llega a ser común es la llamada riqueza común de la nación. Pero la riqueza común no aporta a la construcción de un mundo trascendente. La riqueza común está conformada por medios de consumo que se gastan y no permanecen. No es extraño que se haya llegado a llamar nuestro mundo: la “sociedad de consumo”.

Arendt critica a Marx y propone que la principal alienación de la época moderna no es la de la propiedad del producto del asalariado, sino que la principal alienación moderna es la enajenación del mundo. Se pierde esa relación esencial y recursiva entre un dominio privado oculto dirigido a satisfacer las necesidades de la vida para, a partir de allí, revelarse hacia el dominio público en la construcción de un mundo común. La política se enfoca a los intereses de propietarios privados que quieren riqueza para generar mayor riqueza. Esta hipertrofia del dominio privado no trae consigo mayor privacidad, sino precisamente todo lo contrario, el sinsentido de un espacio oculto que posibilite la revelación en el dominio público. Pierde sentido la relación recursiva esencial entre “vida ↔ mundo” ; “labor ↔ trabajo”.

Si la identidad de la antigüedad dependía del orden social, del oficio, de la familia, ya en la Modernidad este orden se resquebraja. En su defecto empieza a aparecer una identidad cambiante que como en un perchero se van colgando diversos ropajes que se visten transitoriamente dependiendo de la circunstancia y la coyuntura. Si en las sociedades heroicas el personaje sabía de antemano qué hacer dependiendo de su posición dentro del orden social, en nuestra actualidad la pregunta por el qué hacer no puede obtener respuesta moral definitiva y resolutoria.

MacIntyre [4] dice que este yo moderno “pareciese tener un cierto carácter abstracto y fantasmagórico”. En este cambio fundamental de la concepción del ser humano se revela con cardinal importancia una característica clave de la identidad contemporánea. Desde los tiempos antiguos y hasta el medioevo, la identidad referenciaba a esa persona que ocupaba un lugar fijo en la sociedad cumpliendo sus deberes. En nuestros tiempos ocurre una especie de “privatización” de la identidad. La identidad ya no depende del orden social sino que depende del papel ejercido circunstancialmente, el individuo escoge la identidad que porta en el momento particular. Es por ello que la identidad en nuestros tiempos se identifica más con un seudónimo que un nombre. Se usan seudónimos para ropajes particulares. La identidad puede ser un número, o un símbolo, o un correo electrónico, o un seudónimo cualquiera, incluso un símbolo impronunciable.

En nuestra época no entra en juego ni el oficio, ni el linaje, ni el lugar de procedencia, ni nada de eso, no como en otras épocas en la que la familia de los descendientes de la puebla de Bolívar eran los “Bolívar”, o en la que los descendientes de la familia de carpinteros eran los “Carpintero” o “Labrador”, “Coronel”, “Guerrero” según fuese el caso, en la que los descendientes de “Pedro” y “Gonzalo” eran los “Pérez” y los “González” o en la que los “Manco” son la familia del manco. En nuestro tiempo, sólo se necesita un identificador que permita, en el momento, poder distinguir un nodo particular de una red.

## 9.5. La Identidad en la sociedad digital

Nuestra época se caracteriza porque gran parte de la interacción entre los seres humanos viene mediada por las tecnologías de información y comunicación. Desde el correo electrónico, las llamadas redes sociales, el televisor digital o el teléfono inteligente hasta los juegos, noticias y cursos. Incluso actividades de vieja data como escuchar música o ejecutar un instrumento, leer un libro o hacer un café cada vez más vienen mediadas por redes electrónicas. Se puede decir que en nuestros tiempos vivimos inmersos en una sociedad de corte digital con redes que determinan el modo y tipo de interacción entre los seres humanos.

En el Capítulo 1 de este libro, Araujo, Bravo y Sumoza presentan varias propuestas de definición de la identidad en este contexto de la Sociedad Digital. En este capítulo se hará énfasis en algunas de ellas:

4. La identidad es un conjunto de atributos pertenecientes a un individuo que permiten diferenciarlo del resto de individuos que forman parte de un conjunto determinado. Por esta razón no existe una identidad única y universal, sino que pueden existir varias para un mismo individuo, según el conjunto y contexto al que se haga referencia. Incluso los valores de los atributos y los atributos mismos pueden cambiar en el tiempo.

Se puede ver aquí aparecer el “yo” fantasmagórico del que hablaba MacIntyre anteriormente. El “yo” aparece según el conjunto o contexto de referencia. Ya no se trata de un linaje o de un oficio fijo el cual marca una identidad basada en el deber desde el nacimiento hasta la muerte. Se trata de conjuntos que van cambiando según el contexto y que en ello determinan temporalmente y parcialmente la identidad.

Es por ello que hace falta incorporar el concepto de “identidad parcial”. Una “identidad parcial” permite que un sujeto pueda ser identificado en el contexto y el momento particular. Esta identificación no tiene por qué ser necesariamente fija ni definitiva. Si un usuario está leyendo una página web con información general y pública posiblemente la red solo necesite el identificador “ip” que indica en que nodo de la red se encuentra. Este *mismo* usuario puede utilizar un seudónimo particular para participar en una plataforma de juegos en red, varios seudónimos para el mismo o distintos servicios de correo electrónico y redes sociales (laborales, familiares, hobbies), mientras que utiliza otros seudónimos para actividades de orden religioso o político. Estos identificadores son distintos a los que utiliza para servicios de infogobierno como los de “pago de impuesto” (nacional, municipal o estatal), “identificación nacional”, “tránsito terrestre”, “seguridad social”. Otros seudónimos distintos los podría utilizar para los servicios de banca y comercio electrónico, videoconferencias, cursos en línea y un largo etcétera.

Se hace evidente aquí que en la sociedad digital la fluidez de la identidad es muy marcada. La identidad se consume y se gasta, surge y desaparece fugazmente dependiendo de la actividad y del papel que se esté jugando en algún momento. Algunas identidades, muy pocas, se mantienen en el tiempo, pero éstas son la excepción. La gran mayoría de las “identidades parciales” aparecen y desaparecen.

Es hora de volver sobre las definiciones de “identidad digital” que se mostraban en el Capítulo 1 y ver otras dos de las propuestas.

1. Es el conjunto de datos que describen y representan a un sujeto: persona, grupo de personas o cosas de manera única. Puede contener información sobre gustos, creencias, relaciones, tendencias, ideologías, y cualquier otro descriptor vinculado al sujeto.
2. Es la suma de toda la información disponible en formato digital de un sujeto (persona, grupo de personas, cosas).

En la definición número 4 y que se vió anteriormente, el énfasis parecía estar en las “identidades parciales”, en las propuestas 1 y 2 el énfasis se encuentra en la identidad como una totalidad que es resultado de la suma de todos los datos y de toda la información. El “yo” aquí podría concebirse como la suma de las “identidades parciales” surgidas en los distintos contextos y tiempos. La identidad es ese hilo conductor que traza una cierta continuidad entre las distintas “identidades parciales” que conforman un mismo sujeto.

En todo lo que se ha dicho hay un presupuesto que es necesario terminar de revelar y hacer explícito. La identidad es necesaria porque los seres humanos convivimos unos con otros. Si los seres humanos fuéramos unos seres que no necesitasen de vivir con los otros, no hiciese falta la identidad. Pero no se trata exclusivamente de una relación instrumental en la que se necesita identificar al otro porque se necesitan mutuamente para sobrevivir. Se trata, como dice Matthews, de que “nuestras identidades se conforman, al menos parcialmente, en función de la manera en la que nos presentamos ante los otros”. [8]

Aquí la cosa empieza a ponerse peliaguda porque de ceñirse a la propuesta 1 de definición de “identidad digital” entonces en la identidad no se amerita de indagar si se trata de una persona, un grupo de personas o unas cosas. Esto es de particular importancia porque al recordar que en la sociedad digital en la que toda la interrelación social está mediada por la tecnología y las redes de datos, entonces cualquier comunicación entre personas tendrá lugar siempre sobre la base de la tecnología digital. De modo tal que, de fondo, se comunican máquinas. En muchos casos estas comunicaciones no tienen a un operario humano, sino que son programas automáticos los que toman las decisiones con supervisión humana esporádica. Es por ello que en la sociedad digital la identidad identifica un nodo de la red.

Sin embargo, de quedarse limitado a la comunicación entre máquinas en red, la identidad quedaría reducida al intercambio de datos. Entre máquinas pierde sentido hablar de contextos en los cuales la identidad cambia dependiendo del papel que se ejerce. Es cuando incorporamos a las personas que se comunican en la sociedad digital que estos contextos se hacen complejos y pletóricos de significado. Aún más, Matthews [8] incorpora un ámbito adicional y es que la identidad debe incluir tanto la comunicación con los otros como la auto-reflexión.

“El modo en que me veo a mí mismo depende mucho de la manera en que me veo a mí mismo a través de la interpretación de los otros. Es decir, de la manera que ellos me ven. De tal suerte que al afectar las tecnologías de información el modo en que los otros me ven, especialmente en virtud de las maneras en que se alteran los distintos modos de comunicación social, se afectará la manera en que me veo a mí mismo”. [8]

Nótese que cuando un usuario se encuentra en línea pero no se encuentra navegando en la web y no necesita identificarse con algún seudónimo particular es porque va a mantener poca o ninguna interacción con otros usuarios. Sin embargo, si un usuario necesita interactuar de manera sostenida ameritará de la utilización de algún seudónimo. ¿Por qué? Porque es en la interacción con otros usuarios que se necesita la distinción que permite su diferenciación de entre los demás. Y para que la interacción logre mantenerse en el tiempo y permitir espacios de intercambio, por ejemplo comercial, deberá posibilitarse la identificación.

El caso del “intercambio comercial” revela la necesidad de poder “contar con” el usuario, tanto en el caso del comprador como del vendedor. Los modos de pago —a través de tarjetas de crédito o débito, depósitos o transferencias de dinero, o tarjetas prepago— permiten al vendedor asegurar el pago por la mercancía. Por su parte, el comprador puede revisar la “reputación” que ha venido logrando el vendedor a través de las plataformas de comercio electrónico y así poder esperar —contar con— una transacción exitosa.

Mientras la transacción comercial transcurre a satisfacción de las partes, no hay problema. Pero ¿qué ocurre cuando la transacción no es satisfactoria para ambas partes? ¿qué ocurre cuando una persona no honra sus deudas? ¿Cómo se pueden hacer cumplir las leyes y los acuerdos comerciales en la sociedad digital?

Aquí aparece la necesidad de poder relacionar, sin lugar a dudas, la identidad digital con la persona de carne y hueso que se vincula con el seudónimo. Debe posibilitarse esto de tal suerte que no pueda haber repudio de la transacción (a menos claro que se encuentre en presencia de algún tipo de fraude electrónico). Esto mismo aplica para situaciones criminales como acoso, prostitución infantil, tráfico, contrabando, entre tantas otras en las que es necesario poder relacionar el o los seudónimos digitales con la persona de carne y hueso que los opera. Nótese que, hasta lo que hemos visto aquí de no haber situación criminal, esta necesidad de relacionar seudónimos y operario físico es prácticamente inútil.

Etzioni [9] propone el uso de identificadores biométricos para reducir los costos en el seguimiento y persecución de fugitivos criminales, ofensores sexuales y abusadores de infantes, evasores de impuestos, compradores ilegales de armas, estafadores, inmigrantes ilegales, y hasta padres que se niegan a dar la mesada para la manutención de sus hijos. Sin embargo, Naím [10] comenta que en el año 2004 un club nocturno en Barcelona comenzó la utilización de identificadores tipo Dispositivos de Identificación por Radiofrecuencia (RFID) implantados en el cuerpo de sus mejores clientes quienes podían ir al local y consumir sin necesidad de llevar ningún tipo de forma de pago. Por supuesto que cada consumo se les cobraba posteriormente solo que con el RFID se facilitaba la transacción. Propuestas de implantación corporal de dispositivos tipo RFID han sido realizadas con el objetivo de facilitar las transacciones comerciales, control de presidiarios, personas con enfermedades mentales, infantes, etcétera.

Es importante ahora que se indague sobre dos puntos que se han venido ya asomando. La identidad es condicionada por la relación con los otros. Pero para que ella sea duradera, para que pueda mantenerse en el tiempo y con ella se construya un mundo que pueda llamarse apropiadamente “humano”, se hace necesario el cultivo de la “confianza”. Este punto será revisado en la próxima sección.

## 9.6. La identidad digital y la diferencia entre el “contar con” y la “confianza”

Pettit [11] trae a la palestra la discusión en torno a las relaciones de confianza entre personas. La Internet es una herramienta que potencia, y mucho, el poder “contar con” otras personas. A través de la Internet se puede *contar con* otros para el desarrollo de transacciones diversas de comercio electrónico. Desde la Internet se puede *contar con* un servicio de correos que permite enviar información alrededor del mundo en cuestión de segundos. A través de la Internet se puede *contar con* otros para compartir información y así, un largo etcétera.

Sin embargo, Pettit [11] es más cauto cuando pasa de un poder *contar con* otros a establecer relaciones de *confianza*. Se puede *contar con* otros en la sociedad, de una manera bastante similar a como se puede contar con la red y sus servidores. Están allí, como sin estarlo, disponibles para su uso. Tan disponibles están que ni se cae en cuenta de que están. Pero si se habla de una relación de confianza ya es otra cosa. La relación de confianza va más allá de poder *contar con* para establecerse sobre la base de ser de *confianza*. Y la confianza implica que las relaciones se vayan conformando en el tiempo.

Según Pettit [11] la gente no sólo busca bienes que pueda intercambiar. La gente valora bienes que “dependen de la actitud”. Algunos de estos bienes son: “ser amado”, “ser agradable”, “ser apreciado y reconocido”, “ser respetado”, “ser admirado”, entre otros. La “estima” es un bien de importancia en el establecimiento de relaciones de confianza. Se puede *contar con* otra persona sin necesidad de estimarla, pero no se puede *confiar* en otra persona si no se le tiene buena estima.

Pettit [11] vé tres problemas con el establecimiento de relaciones de confianza en la internet. El primero lo llama la “evidencia del rostro” y es que una relación de confianza se establece a partir de gestos, palabras, compostura y la expresión. En la relación mediada por Internet se pierde muchos de estos componentes básicos para la generación de confianza. Se encuentra también la “evidencia del marco”. Con esta expresión se refiere a cómo la persona se relaciona con otras personas y con quién se relaciona. La tercera es la “evidencia histórica” y refiere al devenir de la relación conjunta y de su comportamiento tanto conmigo como con otros y otras. Para Pettit la relación mediada por la internet empobrece las evidencias de rostro, marco e histórica y por eso, si bien facilita el poder “contar con” alguien, dificulta el establecimiento de relaciones propiamente de confianza.

Sin embargo, es importante manifestar al menos cuatro asuntos que se contraponen a la conclusión de Pettit. En primer lugar, el autor se refiere principalmente a interacciones sociales en la sociedad digital basadas en texto (tipo chat y correo electrónico). Se han desarrollado nuevas tecnologías como las redes sociales las cuales pudiesen propiciar la revelación de evidencias de “cuadro”. Asimismo, el creciente uso de videoconferencias personales (también conocidas como “videollamadas”) que han venido revolucionando el uso de las salas de “chat” posibilitan marcadamente las evidencias de “rostro” en la Internet. Si además de lo anterior puede verse que cada vez más las relaciones sociales están entrelazadas con herramientas de la sociedad digital es obvio afirmar que de manera cada vez más creciente se irán afianzando las evidencias de carácter “histórico” en las interacciones entre las personas.

En segundo lugar, es también importante resaltar que muchas de las interacciones que se realizan a través de herramientas de la sociedad digital, por ejemplo las redes sociales, entremezclan las relaciones virtuales y no virtuales. Posiblemente en la mayoría de los casos, al menos hasta el momento, no se trata de relaciones excluyentes (virtual o no) sino que la misma gente que interactúa en la internet luego se encuentra (o se ha encontrado) en la escuela, la universidad, el trabajo, la comunidad, la organización social. Incluso en muchas ocasiones se propician el encuentro no virtual de personas que se han conocido vía virtual y estas relaciones han venido mediadas por personas que han establecido lazos de confianza en la interacción cotidiana, no necesariamente virtual.

En tercer lugar, se debe traer aquí nuevamente el asunto de “la estima”. El uso de las “redes sociales” y otras herramientas de la internet no eliminan los bienes que “dependen de la actitud” quizá incluso los potencian. Ahora bien, para poder cultivar la estima es necesaria la interacción en el tiempo, la evidencia histórica, así como las evidencias de marco y también, cuando es posible, las de “rostro”. De aquí que, si un usuario cada vez que entra a interactuar en la red cambia su seudónimo no podrá cultivar el ser estimado por los demás. Para cultivar estima (“reputación”) es necesario revelarse en evidencias históricas en las que se muestre el “rostro” en el “cuadro”.

Nótese que si se llegase al momento en el que el uso de herramientas tecnológicas como los “certificados de seguridad” o “firma electrónica” fueran de uso masivo y asegurasen la transacción digital con la persona

de carne y hueso que opera el usuario, entonces podría potenciarse aún más el *contar con* esas evidencias que posibilitan la *confianza*. De modo tal que, se puede concluir —de modo contrario a Pettit [11]— que las herramientas de tele-presencia no sólo potencian el poder *contar con* sino también la posibilidad de la **confianza**.

Se ha visto aquí una marcada discontinuidad entre la “identidad” como aparece hoy día y cómo ella aparecía en épocas antiguas. La identidad antigua refería al linaje, al oficio y de allí se desprendía el deber y el quehacer práctico moral de toda la existencia. La identidad provenía del orden social al cual cada persona se debía hasta su muerte. Pero tampoco se puede confundir la identidad de nuestra época con los identificadores propios del estado moderno. Éste procura identificar a un ciudadano dentro de la comunidad nacional. Para ello comúnmente le asigna un número de identificación al cual en Venezuela se denomina “cédula de identidad” (en otros países es el número de “seguridad social” o el del pasaporte). Pero esta identificación es una entre otras, correspondiente a una de las comunidades de las que se forma parte, la nacional. No hay ninguna razón para creer que esta es la única o que es la verdadera identidad.

La identidad moderna aparece así fundamentalmente fragmentada, aparece incluso como un asunto de escogencia. El individuo escoge su papel. En la mayoría de los casos el individuo escoge su seudónimo dentro de un grupo. En el grupo, puede entrar y salir cuando quiera. Si necesita mantener continuamente una identidad en el tiempo, en muchos casos, es por un asunto de acrecentar estima.

Cabe preguntarse entonces que si la identidad antigua referenciaba ese espacio privado, familiar, de la propiedad, a partir del cual era posible provenir para participar libremente en el espacio público de la ciudad, si se ha perdido la identidad antigua que precisamente indicaba el espacio privado del linaje y el oficio, ¿qué ha pasado con los dominios privado y público en esta época de identidades fugaces y consumibles? ¿Qué ocurre con lo público y lo privado en esta época de privatización de la identidad? Este asunto se intentará abordar en la próxima sección.

## 9.7. La resignificación de los dominios público y privado

Ya se había adelantado anteriormente que en la modernidad las nociones de dominio “público” y “privado” cambiaban radicalmente al punto de desaparecer en el sentido de su noción antigua. Tanto Etzioni [9] como Sandel [12] hacen un recuento que puede ayudar a revelar el cambio de fondo que tiene lugar con la noción de “privacidad”. Si bien ambos se enfocan en el caso de la legislación estadounidense, su trabajo ayuda a mostrar un cambio ocurrido en la visión que de estos dominios mantenía buena parte del mundo occidental.

Etzioni [9] dice que antes de 1890 la noción de privacidad en Los Estados Unidos de América era bastante vaga y estaba muy relacionada con la propiedad privada. “Por ejemplo, [dice el autor], se consideraba que debe ser legalmente reparable el daño a la reputación que pudiese haberse hecho a una persona mediante el revelamiento de detalles que le son privados, porque se pensaba que se había hecho un daño a algo que uno poseía (p.e. la reputación de uno) más que por haber sido una invasión a la privacidad”.

En consonancia con la visión de los antiguos, para los estadounidenses la *propiedad privada* aparecía con un halo semisagrado. Cosa que resuena con la sacralidad del dominio privado de la que hablaba Arendt a principios de este opúsculo. Sin embargo, ya a finales del decimonónico empieza a concebirse que el derecho a la privacidad era algo conceptualmente distinto a la propiedad privada. Particularmente empieza a aparecer el derecho que tiene toda persona de poder estar sola en su casa. Pero aún más, no se trata sólo del derecho a la soledad en casa, sino que —cosa curiosa— este derecho es visto como principio de *autonomía y libertad*. Nótese el marcado contraste con la noción antigua de libertad. La libertad ya no aparece como vinculada a la deliberación política en el espacio público sino como algo ligado a la soledad en el dominio privado de la casa.

Pero entre los años sesenta y setenta del siglo XX termina por ocurrir un profundo desplazamiento en la noción de privacidad. En los años sesenta tienen lugar dos famosos casos en la Corte Suprema de los EE.UU. relacionadas con la prohibición de venta de anticonceptivos. Para el momento, los anticonceptivos estaban prohibidos, el problema (decían algunos juristas) era que para hacer cumplir esta prohibición debería llegar el momento en que los oficiales y funcionarios entrasen a las habitaciones maritales para inspeccionar si se estaba utilizando o no anticonceptivos y esto sería una invasión de la privacidad. El importante giro que tiene



lugar es que se deja de discutir sobre la moralidad del acto sexual como tal y se lleva la discusión al ámbito del derecho a la privacidad marital<sup>6</sup>.

Un segundo giro llega en los años setenta. Se confronta nuevamente la prohibición de venta de anticonceptivos pero ahora se confronta la prohibición de venta a personas no casadas. La eliminación de esta prohibición se logra con base al *derecho de la privacidad*. Pero ya no se trata de la alusión a la privacidad de la casa o de la habitación marital. Ahora se alude que los anticonceptivos pueden ser adquiridos por cualquier persona independientemente de su estado civil *como parte de su privacidad*. La privacidad pasa a entenderse como un derecho del individuo como individuo<sup>7</sup>. Dice Sandel [12]:

“Distinto a concebir la privacidad como la libertad de no estar bajo vigilancia o de tener que divulgar asuntos íntimos, la Corte descubrió el derecho a la privacidad en términos de estar protegido para participar libremente en ciertas actividades sin restricción gubernamental alguna”.

[9] dice al respecto:

“[Con esta nueva concepción de la privacidad] una persona portaba este **derecho** a cualquier parte; derecho que era ahora una libertad que no podría confinarse nuevamente a la habitación o a la casa”.

Es así como se hizo posible que se haya llegado a concebir como sinónimos a la privacidad, la autonomía y la libertad. La privacidad ahora alude al derecho a que un individuo pueda escoger libremente según sus preferencias los bienes y la vida buena que desee. El dominio público se transforma en un espacio común para el sostenimiento del derecho a la privacidad de los individuos.

Pero ya en este momento la privacidad ha perdido ese halo de sacralidad que tenía en la antigüedad. Ya el dominio privado no es la oscuridad que permite el revelamiento del hombre libre y, por el contrario, se transforma en el espacio propio de la libertad de escogencia. Con este desplazamiento se entiende que la “privacidad” pierda ese halo sagrado y oscuro de la antigüedad. Es cierto que se mantiene uno que otro espacio de intimidad, en los que todavía resuenan la privacidad y relacionados con las necesidades de la vida<sup>8</sup>, pero esos espacios son cada vez los menos. De hecho, pareciese que esos antiguos espacios de la “privacidad” se han convertido en una mina de explotación de recursos para promover y dinamizar la “sociedad de consumo”.

## 9.8. La Identidad preciosa

En una época en que los entes aparecen como seres a disposición para ser consumidos, la identidad se revela como un metal precioso que puede descubrirse a partir de un proceso de minería. En efecto, se podría aventurar que en la contemporaneidad los datos personales son a la sociedad digital lo que los metales preciosos eran al Renacimiento en los inicios del capitalismo.

De acuerdo con los datos que presenta Etzioni [9] ya a mediados de la década de los noventa tres compañías contaban con archivos de información de más del 90 % de los ciudadanos estadounidenses. Su objetivo era el de hacer diversos perfilamientos con miras a dirigir las operaciones de mercadeo hacia clientes más específicos. O’harrow [13] muestra un ejemplo de cómo funciona el asunto. Una señora de 50 años compra un antidepresivo por prescripción en una franquicia de una conocida red de farmacias, los datos de su compra son transmitidos a una empresa que maneja datos. En el ejemplo que narra O’harrow la empresa se llama PCS Health Systems y lo que hace es reunir información de miles o millones de personas sobre los medicamentos que adquieren regularmente. Con esta información el sistema inscribe directamente a la paciente en un programa psicológico anti-depresión y que le enviará material educativo para atender esta enfermedad. Además, el sistema permite sugerir el uso de otros medicamentos, más económicos, que tengan los mismos componentes farmacéuticos para la atención de la enfermedad. El objetivo de este programa es reducir los costos en compra de medicinas para con ello reducir la tasa de siniestralidad del seguro colectivo de la empresa donde trabaja

<sup>6</sup>A los casos que nos estamos aquí refiriendo son: Poe vs. Ullman, 367 U.S. 497 y Griswold vs. Connecticut, 381 U.S. 479.

<sup>7</sup>En este momento se hace referencia a Eisenstadt vs. Baird, 405 U.S. 438

<sup>8</sup>Arendt llama la atención de ese espacio privado del baño —tan relacionado aún con la privacidad— como un último reducto en el que se mantiene algo de la visión antigua de la “privacidad”.

la señora y con ello reducir el costo de la póliza de seguros laboral. Según decían los representantes de la industria, expresa O'harrow, las empresas ahorraron millardos de dólares gracias a este sistema.

Pues resulta que la paciente arriba mencionada, y que estaba tomando antidepresivos, estaba pasando por la menopausia. No estaba deprimida como resultado de una enfermedad psicológica. Así que, por una parte, ni el programa antidepresión, ni el material educativo que le enviaría la empresa le servirían para atender su problema de salud. Pero lo que más le molestaba a la señora arriba mencionada era que este manejo de datos había sido una invasión a su privacidad puesto que los registros médicos son privados por derecho. La paciente se preguntaba si podía ocurrir que una promoción laboral no la obtuviese debido a su supuesta “enfermedad mental”...

Ya para mediados de la década del 2000 estaban disponibles —para quien quisiese y pudiese pagarlos— los datos crediticios sobre todos los habitantes de varios de los países del mundo. Aún más, ya en 2002 se había hecho público un proyecto cuyo objetivo era guardar información personal sobre todos los habitantes del planeta en la supuesta cacería de terroristas. Decía el líder del proyecto, el Almirante Poindexter de la armada estadounidense, que el gobierno necesitaba “romper las paredes que separaban los distintos compartimentos de las bases de datos comerciales y gubernamentales, para así permitir a los equipos de las agencias de inteligencia la caza de patrones de actividad ocultos a través del uso de poderosas computadoras”. [14]. El sistema se basaría en un conjunto de técnicas conocidas como “minería de datos” utilizadas en mercadeo para buscar posibles clientes y que ahora serían utilizadas también por los equipos de inteligencia para indagar en los patrones de comportamiento de los habitantes de todo el planeta, incluyendo por supuesto los mismos habitantes de los EE.UU. con cuyos impuestos se pagan los salarios del personal de las agencias.

Una década más tarde se pudo conocer la magnitud del sistema desarrollado, gracias especialmente a las filtraciones que realizó uno de sus agentes, el Sr. Edward Snowden. En resumen, el sistema busca recolectar los datos que cruzan la red de telefonía y la Internet. En el caso de la red de telefonía es conocido que la empresa Verizon, que es una de las compañías que más presta servicios de telefonía en EE.UU., pasa los metadatos de todas las llamadas de sus clientes diariamente a la Agencia de Seguridad Nacional (NSA, por sus siglas en inglés). Los metadatos que se entregan son de información general de cada llamada: número de origen y número de terminación, duración de la llamada, centrales y troncales de la red, número de suscriptor internacional, ruta de la comunicación, entre otras (ver [15]). El conocimiento de los metadatos de un usuario particular brinda mucha información sobre su persona. Se puede conocer su red de amistades, familiares más cercanos, intereses y hobbies, enfermedades, tendencias sexuales, activismo político, lugares que frecuenta en qué horario, etc. No es necesario conocer el detalle de las comunicaciones para realizar el perfil del usuario y con ello tener un acercamiento bastante cercano al modo de ser de la persona de carne y hueso.

Dice Greenwald [16] que “los metadatos son matemáticos: limpios, precisos que pueden ser fácilmente analizados”. El procesamiento de tantos millones de datos amerita de sistemas de procesamiento automatizados. Por ello, los sistemas realizan automáticamente las conexiones y realizan las inferencias que puedan realizarse. Por ejemplo, si una persona ha llamado a su psiquiatra tres veces entre las 9:00pm y 11:30pm se puede inferir con alta probabilidad una crisis, sin necesidad de conocer el detalle de la llamada. Sin necesidad incluso de conocer el idioma y los detalles locales de los dialectos.

El sistema no se queda allí. Snowden da cuenta del programa PRISM mediante el cual la NSA recolecta las comunicaciones de las principales compañías de Internet en el planeta. Según los documentos filtrados, la NSA tiene asociaciones estratégicas con *Microsoft* (*Hotmail*, *Outlook*, *Skydrive*, *Skype*, *Bing*, etc.), *Google* (*Gmail*, el motor de búsqueda de igual nombre, *Youtube*, *Drive*, *Docs*, etc.), *Yahoo*, *Facebook*, *Apple*, *Intel*, *Oracle*, *HP*, *Cisco*, *Motorola*, *IBM*, *AT&T*, entre otras. A través del programa PRISM, la NSA puede tener acceso a los correos electrónicos, chats (tanto de texto, como voz y vídeo), fotografías, vídeos, datos guardados en servicios de almacenamiento en línea, transferencia de archivos, telefonía vía IP, videoconferencias, logins, redes sociales en línea, etcétera.

Como puede verse el asunto aquí va mucho más allá de los metadatos. Según narra Gellman y Soltani [17] a partir de los documentos filtrados por Snowden, la NSA en conjunto con la agencia británica de inteligencia conocida como GCHQ ha logrado copiar flujos enteros de información a través de la intersección de los cables de fibra óptica en la comunicación entre distintos centros de datos de Yahoo y Google ubicados tanto en los EE.UU. como en otras partes del mundo.

Si bien los voceros de las distintas compañías involucradas negaron su participación en los procesos de recolección de datos, sus declaraciones “fueron parafraseadas de modos evasivos y legalistas, ofuscando la mayoría de las veces más que clarificando. Por ejemplo, Facebook expuso no proveer un ‘acceso directo’ mientras que Google negó haber creado una ‘puerta trasera’ para la NSA”[16]. La respuesta pública de las empresas ante el supuesto espionaje gubernamental fue la de cifrar sus redes privadas para de esta manera evitar que los flujos de datos, aunque fuesen interceptados, pudiesen ser interpretados.

Sin embargo, ello no parece ser mayor impedimento. Greenwald [16] comenta que *Microsoft* en un momento promocionó ante el público aumentar los niveles de cifrado de su sistema de correo y chat “*Outlook*”. Sin embargo, Microsoft y la NSA se reunieron y acordaron métodos para eludir las protecciones de cifrado de “*Outlook*” para la NSA. Por otro lado, Gellman y Soltani [17] dicen haber visto una diapositiva —de las filtradas por Snowden— en la que un funcionario de la NSA aseguraba que habían burlado el sistema de cifrado de Google logrando tener acceso —a través de la red pública— al “lugar” preciso en el que se cifra y descifra en la nube de la empresa.

Otra mina de datos importantes son las redes sociales en línea. A través de las redes sociales es posible detectar información como detalles personales (direcciones, teléfonos, correos), patrones del día a día, conexiones y redes, información sobre localización y viajes, vídeos, fotografías, etcétera (ver [16]). Otras redes sociales en línea como *MySpace* y *Twitter* también aparecen como fuentes de información y de señales de inteligencia y que son monitorizadas a través del programa PRISM. No importa que usted maneje las opciones de privacidad de la red, si usted sube la información, la NSA la tiene.

Otros muchos elementos son también recolectados. Un dato importante es el de las direcciones IP que visita un usuario mientras navega, lo cual dice cuáles páginas web visita y suele visitar. Si bien, algunos usuarios suelen utilizar sistemas de anonimato que buscan ocultar su identidad ya la NSA ha infiltrado el sistema de anonimato más conocido, llamado *TOR* (The Onion Router). También se almacenan los mensajes SMS y los del sistema de mensajería instantánea PIN de *BlackBerry*. Hace poco *Facebook* compró *Whatsapp* así que la conclusión lógica es que ya están siendo almacenados los datos (sino es que lo estaban siendo antes).

También existen referencias a infiltración de sistemas operativos y de aplicaciones particulares. Se interceptan incluso las compras de servidores y enrutadores (en su envío a destino) los cuales son manipulados y modificados incorporándoles hardware que facilita la recolección de información de las redes internas hasta en el caso en el que ellas no estén necesariamente conectadas a la Internet [16].

¿Para qué recolectar todos los datos? ¿Para la consabida lucha contra el terrorismo?. Sí, seguramente habrá algo de eso. Pero también es cierto que se recolecta información de otros gobiernos “amigos” y de una multitud de fuentes de las que no se puede sospechar de terrorismo. ¿Será entonces que es para obtener ventajas diplomáticas? Sí, también por eso. Los documentos de Snowden muestran cómo mucha de la información colectada está relacionada con reuniones diplomáticas entre representantes de América, Europa y África. La información colectada permite conocer de antemano estrategias de negociación, de diplomacia y otros detalles que le facilitan la preparación adecuada para lograr sus objetivos preestablecidos.

¿Será también que todos estos datos sirven para obtener ventajas económicas? Sí, también. Llama la atención que entre los Departamentos del Gobierno de EE.UU. que aparecen como “clientes” de la NSA se encuentran los Departamentos del Comercio, del Tesoro, Agricultura y Energía, cuyo principal énfasis es, posiblemente, económico. Como bien dice Greenwald [16]:

“Los documentos no dejan lugar a dudas de que la NSA estaba involucrada igualmente en espionaje económico, espionaje diplomático y vigilancia dirigida a poblaciones enteras de las que no se tenía sospecha alguna”.

Y es que también es cierto que la información de la identidad ha llegado a ser apreciada como un bien en sí misma que no necesita ser medio para lograr otra cosa. Es por eso que el eslogan de la NSA para estos días (y que aparece por doquier en los documentos filtrados por Snowden) reza “¡Coléctenlo todo!”. No se trata de almacenar una que otra información que parezca importante como medio para alcanzar algún fin militar, policial, diplomático o económico. No, toda información es valiosa; el perfilamiento de todos los habitantes del planeta es bueno; almacenar todo el tesoro de la información que circula en las redes es precioso.

Toda esta información almacenada, lista para ser procesada y consultada al clic del ratón del PC:

“Sentado en mi escritorio, podía espiar las comunicaciones de cualquiera, desde usted o su contador hasta un juez federal o incluso el presidente, con sólo conocer su correo personal”.<sup>9</sup>

## 9.9. Identidad Digital a tiempo de revolución bolivariana

Desde la particularidad venezolana (y también suramericana) la identidad digital y la acumulación de almacenes de información con los datos de todas las transacciones digitales es un serio serio problema. En esta sección, este problema se abordará en dos niveles: el primero (más superficial), el político estratégico, el segundo (más profundo), el político filosófico. Se comenzará por el primero.

Para el año 2014, la población venezolana se estima en 30.206.307 habitantes (datos del INE), con 30.325.373 líneas de teléfonos móviles activas. Esto significa que muchos de los usuarios de telefonía móvil tienen mas de una línea activa. A nivel de telefonía fija, 93 % de los hogares venezolanos cuentan con este tipo de servicio. Según los datos de la Comisión Nacional de Telecomunicaciones de Venezuela (CONATEL) viene aumentando sostenidamente el uso de voz por telefonía móvil alcanzando para el segundo trimestre de 2014 los 11.991 millones de minutos con 28.662 millones de mensajes de texto SMS enviados. Al mismo tiempo, el tráfico de voz originado por telefonía fija ha venido disminuyendo. Hasta donde se sabe, las empresas que prestan el servicio telefónico en Venezuela no están entregando los metadatos a la NSA, pero la verdad es que los organismos de inteligencia tanto de EE.UU. como de sus aliados (Israel, Canadá, Reino Unido, Nueva Zelanda y Australia) no necesitan de la entrega voluntaria de los datos por parte de las empresas telefónicas para colectarlos. Lo que sí se sabe es que si se quiere perfilar a todos los venezolanos, un bueno modo de hacerlo sería con los metadatos de los sistemas de telefonía dada su alta penetración en la población.

En el caso del uso de la Internet los datos son más que interesantes. Según los datos de CONATEL, para el segundo trimestre de 2014 el número de usuarios de la Internet ha llegado a la cifra de 13.300.000 con una penetración de 44 % de usuarios frecuentes y estables. En este momento 32 % de los hogares tienen acceso a la Internet desde su casa. Y todos estos hogares y usuarios están utilizando frecuentemente correos electrónicos de *Microsoft* (*Hotmail* o *Outlook*) y de *Google* (*Gmail*). Están también haciendo búsquedas en la red a través de los motores de *Google*, *Microsoft* (*Bing*) y *Yahoo*. Están voluntariamente entrando e interactuando en redes sociales en línea como *Facebook* y *Twitter* dejando datos personales y subiendo fotos y vídeos etiquetados. Están haciendo uso de servicios como *Skype* y de almacenamiento masivo en la nube (a través de *Drive*, *Dropbox* u otros). En la mayoría de los casos se está utilizando el sistema de operación *Windows* de *Microsoft* y viene creciendo con fuerza el uso del *Android* de *Google*. También se sabe que buena parte de la infraestructura de red utiliza servidores de tecnología *Intel* con enrutadores *Cisco* y que buena parte de los Computadores Personales que se tienen en Venezuela (incluso los ensamblados nacionalmente) tienen al frente una calcomanía que dice “*Intel Inside*” (por cierto, más llamativa que la marca misma del computador). También se sabe que actualmente está en crecimiento el uso del servicio de “mensajería instantánea” a través del uso del *PIN* de *Blackberry* y del *WhatsApp* de *Facebook* y que hacen uso de toda esta infraestructura de datos arriba mencionada.

Incluso si se quisiera no hacer uso de ninguno de los servicios mencionados, administrados por las transnacionales de la era digital, y se quisiera utilizar un correo nacional (como *Cantv.net*) para acceder a servicios nacionales de infogobierno, esta comunicación probablemente pasé primero por Miami, Atlanta o Washington antes de llegar al servidor de la institución nacional ubicada en Caracas. Y si hace uso de *Cantv.net* es bueno saber que, al menos hasta el momento que se está escribiendo este libro, la comunicación es transportada de manera no cifrada, incluyendo tanto la cuenta de usuario como la contraseña.

Las filtraciones del Sr. Snowden dan algunas luces de la importancia estratégica de Venezuela dentro de la visión del “¡Coléctenlo Todo!” de la NSA y sus aliados. A través del programa PRISM se ha colado que se espía a Venezuela principalmente en los temas relacionados con “petróleo” y “procura militar” (ver [16]). Se ha filtrado también que constantemente se están realizando copias completas de los discos duros de los computadores ubicados en las embajadas de Venezuela en Washington y Nueva York ([16]). Y también logró filtrarse

<sup>9</sup>Edward Snowden citado por [16].

un oficio en el que, en el marco de la 5<sup>ta</sup> Cumbre de Las Américas, el Secretario Asistente de Estado Thoman Shannon agradecía al general Keith Alexander de la NSA por los más de:

“100 reportes recibidos de parte de la NSA que nos dieron una visión profunda en los planes e intenciones de otros participantes de la Cumbre y aseguró que nuestros diplomáticos estuviesen bien preparados para aconsejar al Presidente Obama y a la Secretaria Clinton sobre cómo lidiar con asuntos conflictivos, como el de Cuba, y la interacción con contrapartes difíciles, tal y como lo es el Presidente Venezolano Chávez”.<sup>10</sup>

Uno de los documentos filtrados y publicado por el periódico *New York Times* muestra además que para enero de 2007 Venezuela contaba con un lugar privilegiado dentro de los objetivos de vigilancia de la NSA en conjunto con China, Corea del Norte, Irak, Irán y Rusia. El objetivo era el de prevenir que Venezuela lograra su liderazgo regional y que pudiese impactar negativamente sobre los intereses estadounidenses. Para ello, la NSA se comprometía a proveer de una perspectiva holística con señales de inteligencia permanentes sobre las tendencias y los desarrollos regionales. Para muestra, este extracto del documento con algunas de las tareas sobre Venezuela:

“Evaluar las tendencias de la política internacional de Venezuela y las intenciones de liderazgo que impacten los intereses de los EE.UU. Evaluar el progreso de Chávez en sus iniciativas por alcanzar objetivos de poder regional en las arenas política, económica, energética e ideológica”. [18]

Si bien Venezuela tiene un lugar privilegiado en las prioridades de espionaje no se encuentra allí sola. Brasil es también uno de los países que más llama la atención de los esfuerzos de inteligencia. Uno de los documentos filtrados muestra que en uno de los programas de la NSA, el *Boundless Informant*, en un período de un mes se colectaron 2,3 millardos de metadatos del Brasil y 13,5 millardos de la India [16]. Asimismo se muestra que la empresa petrolera Petrobras y el ministerio de Energía y Minas de Brasil se encuentran como objetivos privilegiados de vigilancia y que también existen objetivos prioritarios tanto en México como en Argentina. Por último, llama la atención el énfasis en ganar mayor entendimiento de los métodos de comunicación y de selección de asociados de la actual presidenta de Brasil, Dilma Rousseff y también del actual presidente de México, Enrique Peña Nieto. Uno de los documentos de la NSA en el que se atiende este asunto se intitula “Identificando los desafíos: tendencias geopolíticas para el 2014 – 2019” y el subtítulo de la sección en la que se listan a México y Brasil reza “¿Amigos, Enemigos o Problemas?”<sup>11</sup> [16]. Aparecen también interceptadas las embajadas de Brasil en Washington y Nueva York, la agregaduría de negocios de la embajada colombiana en Nueva York y también la embajada mexicana en la misma ciudad ([16]. Pp. 144,145).

No es sólo que colecten todos los datos de la región, es que además Suramérica aparece entre las principales prioridades de investigación y espionaje.

Obviamente se ha trastocado por completo ese respeto y/o sacralidad del dominio privado y con ello, también, del dominio público. La privacidad como un derecho aparece ya como una noción hasta inocente. Van den Hoven [19] asoma la propuesta de dejar de preocuparse por la “privacidad” puesto que hay tanta información disponible sobre la gente que se puede saber casi todo sobre una persona con poco esfuerzo. Del otro extremo se encuentra la tendencia completamente contraria, la libertaria, que busca proteger todos los datos (cifrándolos), esconder toda identidad convertirse en un completo fantasma, un anónimo, en la web. En esta tendencia, el dominio privado se sobreexpande tanto que casi desaparece el dominio público en la masa de usuarios sin identificación.

La revolución que ha venido viviendo Venezuela a inicios de este siglo XXI es una que ha buscado una refundación, una resignificación, del sentido de patria. La mayoría de la población ha venido manifestando claramente su intención de reconstituir una patria basada en el sentido de identidad. Como pueblo, se ha tratado de una nación que ha provenido de una historia común que la identifica, que la distingue y que le permite lanzarse, proyectarse, hacia un futuro con sentido patrio. Esto se ha venido viendo en ya más de dos décadas de revolución bolivariana y con especial énfasis desde el proceso constituyente de 1999.

Pues de ser así, Venezuela se encuentra con un problema grave en la llamada sociedad digital. La Internet no es neutra. La Internet plantea un espacio posible para la interacción social. Sí, como se ha visto ya, en los tiempos de la Identidad Digital gran parte de la identidad tiene lugar en términos de identidades fragmentadas

<sup>10</sup>citado por [16]

<sup>11</sup>Traducción propia.

y que pueden ser perfiladas tanto por poderosas empresas transnacionales como por agencias de inteligencia, entonces no pareciera haber posibilidad para una actuación libre en el dominio público. Así de claro.

Sería temerario en este momento adelantar cómo será el dominio público y privado para la nueva época. No, no se pretende plantear algo tan complejo. Sin embargo, si se puede aventurar algunos bosquejos, so riesgo de equivocarse, que aparecen como mas apropiados para propiciar esos nuevos dominios propios para la Venezuela del siglo XXI.

Se puede adelantar que se necesita posibilitar espacios públicos para la discusión política en el ciberespacio. Existen actualmente muchas páginas, redes sociales, blogs, en los que tiene lugar comentarios políticos. Eso está bien y debe mantenerse. Sin embargo, no existen espacios públicos —o al menos existen pocos— que posibiliten, faciliten y propicien el foro o debate. Este espacio digital debería venir complementado con herramientas tipo encuestas, web semántica, minería de datos, etc. que ayuden a procesar los datos de participación en foros masivos para facilitar la toma de decisión política.

Uno de los primeros pasos para propiciar el dominio público en el ciberespacio es un Identificador Digital Nacional (IDN) (o Suramericano, IDS). Se necesita de un IDN que permita asegurar en los casos que sea necesario que un usuario se corresponde con un ciudadano de carne y hueso. En los casos en que esto no sea necesario, no hará falta. Pero si un usuario está realizando un trámite o participando en el dominio público deberá autenticarse con su IDN de modo tal de propiciar, exigir y resguardar la responsabilidad propia de un ciudadano libre en el dominio público.

Es en este contexto que se debe trabajar más en espacios de construcción plural. Por ejemplo, espacios para la escritura colaborativa de legislaciones que terminen en proyectos que se presenten a los Concejos Municipales, Consejos Legislativos, la Asamblea Nacional u otros espacios de acción política. Sistemas para la administración de peticiones a diversas instancias de gobierno que faciliten su procesamiento, veracidad y verificación mientras que, al mismo tiempo, cuiden y resguarden la privacidad de los datos en los casos en que sea necesario hacerlo (p.e. denuncias, solicitudes de referendos, solicitudes masivas de políticas, etc.).

Se necesita también de herramientas de comunicación que faciliten la interacción entre los entes gubernamentales y la ciudadanía. Esto incluiría sistemas de Alerta Temprana que hagan uso de servicios de mensajería instantánea, SMS y llamadas telefónicas que permitan la atención oportuna de las diferentes situaciones que se presenten. Esta herramienta debe ser mucho más que una cuenta en la transnacional estadounidense “*twitter*”, visitada de cuando en cuando por algún funcionario. Se trata de todo un sistema que permita recibir las solicitudes y las alertas tempranas para procesarlas y evaluar su atención por parte del organismo asignado. El sistema debe permitir mantener un registro de los tiempos de atención que permitan su evaluación no sólo por las autoridades de la institución, sino también por organismos de supervisión y también por la “Defensoría del Pueblo”.

Se debe contar con servicios públicos para la sociedad digital. Por ejemplo, se necesita de un servicio público de correo electrónico nacional que le permita al ciudadano no tener que abrir necesariamente una cuenta en una empresa privada transnacional. Un servicio público de este tipo estaría apegado a las leyes nacionales en la que el Estado podrá proteger y salvaguardar la identidad y los datos privados del ciudadano. ¿Por qué si casi todos los países del mundo cuentan con sistemas de correos y telégrafos públicos no ocurre lo mismo con el correo electrónico?

Es también pertinente evaluar la implantación de un sistema público de anonimato que permita poder navegar en la web sin dejar rastros. El primer tipo de usuario de este servicio, que sería indiscutible, sería el de funcionarios públicos en cargos sensibles que puedan estar siendo monitorizados en todo su quehacer por parte de agencias de inteligencia internacionales: qué noticias leen, qué páginas visitan, qué tuits revisan, qué perfiles ven en las redes sociales, qué productos compran en servicios de comercio electrónico, etc. Si se utiliza un sistema de anonimato para telefonía móvil, esto pudiera ayudar incluso a esconder la localización de funcionarios sensibles para el gobierno nacional y que, actualmente, están completamente expuestos.

Se pudiese tener también un servicio de anonimato de uso público para ciudadanos nacionales que les permitan navegar sin dejar rastros en la web. Esto le permitiría al usuario navegar sin que lo perfilen las transnacionales y las agencias de inteligencia. Sin embargo, este servicio exigiría la autenticación del usuario con su identificador nacional. De esta manera, el usuario sabe que esta haciendo uso de un sistema público que si bien lo protege del espionaje global, no lo encubre necesariamente a la hora de cometer algún delito.

Otros servicios públicos que pudiésem ser brindados son los de contraloría social, almacenamiento masivo de datos, sistemas públicos de videoconferencia, etc. Todos podrían estar a la disposición de la ciudadanía para su uso con el compromiso legal y público de salvaguardar su identidad y sus derechos ciudadanos.

No debe precipitarse la suposición de que se prohibirá el uso de estos mismos servicios por parte de las transnacionales privadas de la sociedad digital. No, eso no es lo que se ha dicho en este escrito. Lo que se está proponiendo es que hayan alternativas públicas sometidas a leyes nacionales y en la que los ciudadanos nacionales puedan sentirse protegidos. Muchas de las diversas tramitaciones públicas deberán necesariamente hacer uso del identificador nacional y del correo electrónico público nacional que permita validar al usuario que se autentica con el ciudadano de carne y hueso. Otros servicios podrían estar abiertos a la completa disposición del usuario sin necesidad de uso del identificador nacional tal y como ocurre actualmente con los servicios de información.

Ahora bien, para poder proteger efectivamente los datos de de los ciudadanos es necesario promover, por lo menos, las siguientes medidas:

- Asegurar que los diversos sistemas de dominio público exijan el uso del IDN y del correo electrónico público nacional. Nada se podrá adelantar si se sigue enviando el usuario y la contraseña de los ciudadanos nacionales a servicios de correos afiliados al programa PRISM.
- Promover redes de transmisión y la legislación adecuada que permitan y forcen a que las transmisiones de datos de todos los usuarios nacionales, en el momento que vayan a hacer uso de los servicios públicos digitales, no salgan del territorio nacional.
- Si un ciudadano nacional se encuentra fuera de la región y/o necesita acceder a redes extranjeras para poder hacer uso de algún servicio público regional deberá habilitarse un servicio de puente que le permita una comunicación suficientemente cifrada desde el extranjero con la red nacional o regional.
- Esto lleva a que se debe investigar algoritmos de cifrado y llevar a cabo desarrollos nacionales o regionales que permitan cifrar las comunicaciones y contenidos. Actualmente, los desarrollos nacionales hacen uso de funciones de cifrado desarrolladas en otras latitudes y que se desconocen a fondo. Se sabe ya que existen alianzas entre las agencias de inteligencia y las transnacionales de la era digital para burlar estas funciones de cifrado. Se hace necesario, imperioso e impostergable proceder a realizar desarrollos regionales para el cifrado de la información.

Se trata, como puede verse, de sistemas que respondan al dominio público y también que protejan el dominio privado de los ciudadanos para, a partir de allí, promover la libertad en el marco de la democracia participativa y protagónica expresada en nuestra Constitución Bolivariana.

## 9.10. Palabras finales: el recuento

En otras épocas, la identidad referenciaba a la diversidad en el orden social. La identidad referenciaba al oficio, al linaje, al pueblo o al lugar de procedencia. La identidad digital, por el contrario, homogeneiza a todos. Tras las múltiples identidades parciales que puede utilizar un mismo operario, se encuentra siempre la homogeneidad del nodo de la red. Por eso es que no hay mayor diferencia entre un usuario operado por un ser humano y un autómeta.

La propuesta que aquí se adelanta propone el ejercicio de la ciudadanía libre y responsable, con espacios de participación pública y salvaguarda de la privacidad en la sociedad digital. La propuesta es de carácter político y revolucionario; busca revelar la homogeneidad escondida tras los velos de la llamada “neutralidad”; busca posibilitar la diversidad desde la inacabable y constante definición de *quiénes somos*.

La identidad no puede reducirse a un nodo de la red como si esa fuera la naturaleza homogénea de todos los habitantes del planeta. Como no se puede ser reducido a un nodo de la red, como los seres humanos no conformamos una masa homogénea, la pregunta por la identidad no puede enmarcarse en un “qué somos”. Rorty [20] acertadamente propone que la pregunta más pertinente que debe hacerse es “¿quiénes somos?”:

“... la pregunta por el ‘quién’ es política. Esta pregunta la realiza quien quiere separar a unos seres humanos de otros porque son más apropiados para un propósito particular, y así conformarlos en una comunidad auto-consciente: es decir, una comunidad reunida por la confianza recíproca y la voluntad de atender a sus compañeros cuando lo necesiten. Las respuestas a las preguntas por el ‘¿quién?’ son intentos por forjar, o refundar, una identidad moral”.

Venezuela es una comunidad con identidad moral conformada en la confianza recíproca forjada desde una historia en un proyecto de patria (quizá de patria grande visualizada hacia Suramérica). Para ello, hace falta que se trabaje en conjunto para posibilitar el sostenimiento de nuevos y resignificados dominios público y privado que sean apropiados a esta nueva época.

Ahora bien, fundamentar la identidad amerita poder hacer inteligible, brindar coherencia, dar cuenta unitaria, hacer sentido, de la vida. Sea esta vida la de un individuo o la de un pueblo o una patria. Es por eso que hace ya un rato se había adelantado que la identidad era un asunto de auto-reflexión. La identidad amerita de una narrativa a partir de la cual ella tenga sentido. La identidad no se reduce sólo a la posibilidad de generar y sostener cierto nivel de confianza. Se trata también de que esa confianza es posible sobre la base de mostrar coherencia y unidad histórica. Como bien lo dice Matthews [8]:

“Nuestro control sobre **quiénes somos** es algo que obramos mediante la construcción de un ‘yo’ el cual, esperamos, no esté tan embrutecido por la tecnología que mine el sentido de que nuestras vidas entrelazan sus manos en una narrativa simple”.<sup>12</sup>.

Obviamente, Matthews es bastante pesimista sobre el poder de la tecnología para la construcción de identidad. Sin embargo, la Sociedad Digital abre importantes oportunidades para la construcción de nuevas identidades si se logra construir un tipo de tecnología que no sólo asegure el poder “contar con el otro” sino también, y más importante, sembrar confianza a partir de la cuenta de una historia que pueda ser considerada “nuestra”.

“Es posible interpretar que el monstruo intenta a lo largo de la novela convertirse en humano y que finalmente lo consigue, cuando cuenta su historia a Walton. Es entonces, cuando logra contar la historia de su vida, cuando se hace humano... Así, el monstruo puede salir del ámbito de lo privado, de su sola compañía y hablar en público... No es de extrañar, pues, que en el mito resultante, y en el habla popular, el **nombre de Frankenstein** suele transferirse del creador a la criatura. El monstruo recibe a la larga una identidad social...” [1]

En este sentido, “¿quiénes somos?” implica responder “¿cómo hemos llegado a ser quiénes somos?”. Una tecnología que promueva atender esta pregunta no es evidente. Nótese que no se trata solamente de contenidos nacionales e históricos, se trata también de un modo tecnológico de interacción que promueva la reflexión en torno a esa pregunta... Sin embargo, esto es algo que deberemos atender en otro momento.

<sup>12</sup>Sección: “Character Identity”. Pág: 8.



## REFERENCIAS

---

1. E. Ramalle Gómara. Frankenstein, un espejo de la identidad humana. *Berceo*, 153:81–96, 2007.
2. S. Bolívar. Discurso ante el Congreso de Angostura el 15 de Febrero de 1819. <http://es.wikisource.org/>, 1819.
3. B. Anderson. *Imagined Communities. Reflections on the Origin and Spread of Nationalism*. Verso, New York, 1998.
4. A MacIntyre. *After Virtue. A Study in Moral Theory*. University of Notre Dame Press, Indiana, 1984.
5. H. Arendt. *The Human Condition*. The University of Chicago Press, 1998.
6. R. Fuenmayor. The roots of reductionism: a counter-ontoepistemology for a systems approach. *Systems Practice*, 4, 1991.
7. M. Shelley. Frankenstein o el moderno prometeo, 2004.
8. S. Matthews. *Identity and Information Technology. En Information Technology and Moral Philosophy*. Cambridge, 2006.
9. A. Etzioni. *The Limits of Privacy*. Basic Book, 2006.
10. M. Naím. *Ilícito. Cómo traficantes, contrabandistas y piratas están cambiando el mundo*. Debate, 2006.
11. P. Pettit. *Trust, reliance and the internet. En Information Technology and Moral Philosophy*. Cambridge, 2008.
12. M. Sandel. Moral argument and liberal toleration: Abortion and homosexuality. *California Law Review*, 77, 1989.
13. R. O'harrow. Health plans' access to pharmacy data raises concerns about privacy. *The Seattle Times*, 1998.
14. J. Markoff. Pentagon plans a computer systems that would peek at personal data of americans. *The New York Times*, 2002.
15. G. Greenwald. Nsa collecting phone records of millions of verizon customers daily. *The Guardian*, 2013.
16. G. Greenwald. *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*. Penguin Books Ltd., 2014.
17. A. Gellman, B. y Soltani. Nsa infiltrates links to yahoo, google data centers worldwide, snowden documents say. *The Washington Post*, 2013.
18. New York Times. Documents show n.s.a. efforts to spy both enemies and allies. *New York Times*, 2013.
19. J. Van den Hoven. *Information Technology, privacy, and the protection of personal data. En Information Technology and Moral Philosophy*. Cambridge, 2008.
20. R. Rorty. Who are we? moral universalism and economic triage. *Segundo Foro de Filosofía de la Unesco*, 1996.



# EL ESCENARIO REGIONAL ANTE LA CIBERGUERRA Y LA CONSTRUCCIÓN DE UNA IDENTIDAD DIGITAL SURAMERICANA IDS COMO FACTOR CONTRIBUYENTE A UNA DEFENSA CIBERNÉTICA EN LA UNASUR

---

DANIEL QUINTERO

Fundación Centro Nacional de Desarrollo e Investigación en Tecnologías Libres

## 10.1. Introducción

En el presente capítulo se extraerán principios del pensamiento estratégico clásico y moderno, para establecer las redefiniciones que en los ámbitos de defensa han producido el ingrediente tecnológico, puntualizándose sobre ese contexto mundial en temas cibernéticos, que muestra cómo un grupo de potencias militares y actores estatales han desarrollado conceptos como: ciberestrategia, y ciberpoder, que les han permitido desplegar capacidades superiores a la mayoría de los Estados. Asimismo, se deliberará sobre la ciberguerra, exponiendo su naturaleza como medio para obtener fines políticos, explicándose aspectos propios de su construcción teórica/jurídica/militar, para entrar en el escenario suramericano, y reflexionar sobre la pertinencia del concepto de Identidad Digital Suramericana **IDS**, como complemento a una propuesta de Defensa Cibernética en la Unión de Naciones Suramericanas (UNASUR), analizándose tres marcos referenciales; Primero: la propuesta primigenia sobre ciberdefensa enmarcada en el literal 1.f de los Planes de Acción 2012/2013 del Consejo de Defensa Suramericano (CDS); Segundo: la decisión de la creación del mega anillo de fibra óptica para la

región suramericana; y Tercero: el pronunciamiento presidencial de Paramaribo y su directriz para la defensa cibernética subcontinental.

## 10.2. La Cibernética y el Ciberespacio, contextualización de las definiciones

Para comprender el fondo conceptual de la ciberguerra, es importante entender semánticamente su significado compuesto, para visualizar concretamente qué contiene y qué descarta esta novedosa perspectiva. Primeramente, hay que indagar sobre el término cibernética, el diccionario de la lengua española en su vigésima segunda edición, expone que el origen etimológico de la palabra se vincula al término griego *κυβερνητική* (arte de gobernar una nave), pero el significado más general referenciado en el mismo texto alude al:

“Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas; y en particular, el de las aplicaciones de los mecanismos de regulación biológica a la tecnología” [1].

Esta reseña, conduce a escrutar sobre los pensadores que originaron esta corriente, estando los antecedentes en las primeras décadas del siglo XX, cuando escritores como Norbert Wiener fueron precursores de los estudios que inquirían explicar los relacionamientos y diferenciaciones entre seres vivos y estructuras creadas artificialmente por el hombre, sugiriendo en [2], que la finalidad de la cibernética era el desarrollo del lenguaje y técnicas tendientes al abordaje de los problemas generales del control y la comunicación, en la búsqueda de hallar un amplio repertorio de ideas y métodos para catalogar a sus expresiones particulares en concepciones determinadas. Hay que destacar que Wiener tuvo sus primeras incursiones teóricas de la mano de Arturo Rosenblueth Stearns, siendo este estudioso de origen azteca uno de los estructuradores de los basamentos cibernéticos, sobresaliendo:

“La influencia enorme para la formación de ideas de Wiener acerca del problema de la interacción “hombre-máquina”” [3].

Estas pinceladas iniciales del pensamiento cibernético, que implicaba explicaciones biológicas y físicas, posteriormente tuvieron en Ross Ashby uno de los artífices de las reflexiones actuales, previsualizando lo vasto y conexo del tema, apuntando en [4], que esta rama de pensamiento tendería a desvelar un buen número de llamativas correlaciones entre las máquinas, el cerebro humano y la sociedad, estando en la capacidad de proveer un lenguaje común, en donde las revelaciones en un ámbito pueden aprovecharse en otros. Esos tres factores de estudio (máquina/individuo/sociedad), coinciden en una interoperabilidad que funge como eje transversal, conllevando a la generación de toda una nueva gama de procesos, relaciones, y lenguajes sociales.

Esa complejidad que encarnan todos aquellos vocablos que anteponen el prefijo ciber, se manifiesta también en el uso de la palabra ciberespacio, que contradictoriamente no se asocia inicialmente a las teorías de control o sistemas que moldearon la cibernética disciplinariamente, sino que varios autores lo remontan al año 1984 en la obra literaria de William Gibson, quien por primera vez hace uso de la expresión ciberespacio, detallándola en uno de sus pasajes ficticios como:

“Una alucinación consensual experimentada diariamente por billones de legítimos operadores, en todas las naciones, por niños a quienes se enseña altos conceptos matemáticos... Una representación gráfica de la información abstraída de los bancos de todos los ordenadores del sistema humano. Una complejidad inimaginable” [5].

A pesar de lo novelesco de esta propuesta, lo expuesto por Gibson, da un abreboca de lo que ciertamente unas décadas después sería el escenario digital interconectado, que reúne concordancias con lo sugerido en *Neuromante* [5]. Entrando en un campo más teórico, Cicognani intenta irrumpir en las profundidades terminológicas del ciberespacio, señalando en [6], que en la expresión ciber+espacio, el espacio es tomado por su connotación física, por su parte ciber corresponde a las particularidades de la inmaterialidad. Aunque pareciera simple deducir esta dualidad, el unificar lo físico y virtual, no ha sido sencillo, y ha necesitado un hondo ejercicio analítico, para ampliar y derrumbar viejos paradigmas que hacían imperioso lo material para asumirlo como real, no estando exento de un intenso debate<sup>1</sup>, sobre cómo se debe valorar el espacio cibernético.

<sup>1</sup>De hecho, las interpretaciones teóricas del ciberespacio cuentan con dos grandes vertientes conocidas como los Excepcionalistas (*The Exceptionalists*) y los No Exceptionalistas (*The Unexceptionalists*), estando los primeros enmarcados en el establecimiento de regulacio-

Es así que Post en [7] reflexiona, acerca de una interrogante recurrente ¿es acaso el ciberespacio un lugar en realidad?, resultando la pregunta una curiosidad en sí misma, equivaliendo a inquirir si la existencia terrestre es “igual a” o “disímil a” la vida acuática, concluyendo que la contestación correcta, es que paralelamente, ambos escenarios son ciertos. El hombre ha tendido históricamente a delimitar y definir su hábitat, orientándose para ello en referencias físicas, o en la costumbre transmitida por sus antepasados, y esta tendencia se ha reproducido ante una creación antrópica como el ciberespacio, proponiendo Anders en [8], que aunque se puede identificar el espacio cibernético como la referencia manejada en los medios de comunicación electrónicos para ubicarlo espacialmente, en el fondo se vincula a la necesidad de explicar el espacio donde se interactúa socialmente, lo que es fruto de la complejidad mental humana. Lo manifestado por Peter Anders sobre ese complejo proceso mental, muestra cómo los patrones conductuales característicos del ser humano en el espacio físico, pueden ser reproducidos en el espacio cibernético. Cuando en el siglo XV arribaron a tierras americanas los conquistadores europeos, a pesar de estar a miles de kilómetros de sus metrópolis, optaron por replicar su cosmovisión, apoyándose para ello en sus leyes, religión y métodos de guerra, lo que condujo a la aniquilación de las culturas aborígenes. Este mismo proceder viene ocurriendo desde un primer momento en el ciberespacio, donde instancias hegemónicas militares, han extrapolado sus intereses dominadores del espacio material al virtual, percibiendo las potencialidades estratégicas y tácticas que pueden ser aprovechadas para la guerra, apuntando Flores que:

[...]“una definición aprobada respecto a ciberespacio, habría consenso respecto a que las acciones de guerra relacionadas al mismo impactan en los ámbitos terrestres (tierra y mar) y aeroespacial, e interactúan con éstos en forma sinérgica” [9].

Lo subrayado precedentemente, muestra cómo el ciberespacio pasó de una creación literaria a una dimensión técnica, que trascendió paulatinamente las redes, para convertirse en un novedoso proceso social, que ha entrado en la órbita de estudio de potencias mundiales como campo de lucha, exhibiéndose una reducción entre las distancias de lo virtual y físico, que parece evolucionar hacia una simbiosis.

### 10.3. La ciberguerra y sus repercusiones estratégicas

Una vez esbozada la connotación de cibernética y ciberespacio, es preciso adentrarse en su vinculación con la guerra, que ha pasado por un proceso acumulativo de interpretaciones, Fritz en [10] explica que al acrecentarse las investigaciones y propuestas teóricas sobre la guerra cibernética, se ha producido un aumento sostenido en las conceptualizaciones en la materia. Esta multiplicidad de aportes, y la necesidad de tomar medidas cibernéticas en defensa, colocó a muchos estrategas y gobernantes en la encrucijada de tener que asumir una delimitación entre el antiguo y nuevo campo de batalla, que era inadvertido en el pasado, tal como lo exponen Winterfeld y Andress en [11], el contraste esencial entre cinético (el mundo material)<sup>2</sup> y el no-cinético (el mundo virtual) son las técnicas bélicas, las armas versus los software que ellos usan. Esta presencia inmaterial generó inmediatamente un controvertido giro, que pasaba de la convencionalidad militar entre Estados, a un escenario centrado en la virtualidad informática, en el cual los límites y acciones se hacen dudosos, pese a que la capacidad de infringir daño puede ser la misma, advirtiendo McGraw en [12], que la ciberguerra demanda un firme impacto en el plano físico, que los especialistas castrenses denominan consecuencia “cinética”, siendo primordial para recibir la calificación de guerra cibernética, que los medios sean informáticos, pero la secuela debe ser física. No obstante, la virtualidad y materialidad de la guerra, tienen un punto de confluencia importante, y es la motivación política que origina los ataques, que históricamente ha sido el activador de la maquinaria bélica de los países, reflejando Kostyuk y Alí en [13], que la guerra en su percepción clásica y la cibernética son análogas en el objetivo que persiguen, que no es otro que alcanzar una preeminencia respecto a un Estado-nación, impidiendo que el mismo logre aventajarle de cualquier manera.

nes e interpretaciones que asumen la especificidad que personifica el ciberespacio. Mientras que los segundos, pregonan que la legislación existente en el espacio cinético se puede proyectar en el ciberespacio.

<sup>2</sup>Cuando en el presente capítulo se hace uso de la palabra cinética o en inglés *kinetic*, se refiere a la afectación física en el mundo material, en el caso militar, explicaría las consecuencias que puede producir un arma convencional o informática (muerte, daño infraestructura, etc.).

Por tanto, el factor político, empieza a relucir como el propiciador de la acción cibernética, apuntando Lewis en [14], que la guerra convencional consistiría en la utilización de componentes militares para que un país destruya o averíe las capacidades de un adversario, mientras que la ciberguerra involucraría un accionar por parte de otro Estado o agrupación, que por motivaciones políticas lanzan ciberataques para alcanzar sus pretensiones. Lo expuesto por Lewis, es concordante con los principios clausewitzanos<sup>3</sup>, que supeditan lo militar a lo político, siendo la guerra cibernética un medio y no un fin en sí mismo.

Los enfoques que antecedieron, dan luces de lo importante que es la materialización de una estrategia en el área cibernética, que debe desembocar en sus consecuentes aplicaciones operativas, con equipos capacitados técnicamente, y que estén bajo la subordinación de los planos político-estratégico, quienes deben orientar la respuesta a los ciberataques recibidos, según los fines que persigue el Estado, como detalla Ferrero:

“Algunas naciones, entre ellas China, Rusia, Corea del norte e Israel, disponen de unidades especializadas con capacidad de llevar a cabo ciberataques, por lo que es necesario disponer de una capacidad de defensa ciberespacial que garantice una protección” [...]. [15].

Sin embargo, lo vertiginoso del escenario informático, ha engendrado una tendencia mundial hacia la militarización a ultranza del ciberespacio, asumiéndose estrategias controladoras y restrictivas, como las emanadas de centros hegemónicos, pero como apunta Kiravuo [16], estratégicamente la defensa cibernética no implica una sujeción al mando militar, siendo pertinente su consideración bajo el direccionamiento civil. Empero, una condición necesaria para el acontecer tecnológico de la guerra actual, pasa por no desligar totalmente a las instancias civiles y militares, para propiciar una respuesta integral en un conflicto informático. Es decir, el debate sobre el carácter militar o civil que se debe imprimir a la ciberestrategia, no puede empantanar la adopción de la misma, ya que la mutación del campo de batalla del siglo XXI, hace impostergable la implementación de medidas para asumir un ataque computacional, que ponga en peligro la integridad del conjunto nacional o supraestatal, referenciando a Sanz y Fojón:

[...]“los adversarios, en cualquiera de sus formas (naciones, grupos criminales o terroristas, facciones extremistas, etc.) tienen acceso y pueden utilizar las mismas tecnologías de un modo completamente innovador y singular” [17].

Tomando en cuenta esta tendencia dicotómica (civil/militar), la mejor manera de sobrellevar una conducción ofensiva, defensiva, o contraofensiva de la ciberguerra, es orientando y perfilando el direccionamiento, que como Rantapelkonen, y Salminen en [18] aclaraban, no tiene que ver con charlas pasajeras o tibios encuentros, precisándose declaraciones, planes y ejecución de acciones cooperativas, para fomentar una visión colaborativa, que promueva un discurso cibernético. Y esa ciberdirección, debe basarse en la comprensión de un concepto que hace acompañamiento teórico a la ciberestrategia, como es el ciberpoder, en vista que ambas definiciones se interrelacionan, y despejan algunas dudas sobre el carácter con que se asume el ciberespacio por los actores. Particularmente el autor Starr, clarifica en [19] el fondo de dichos presupuestos, describiendo el ciberpoder como la utilización de las capacidades propias en el espacio cibernético, para procurar superioridad e influenciar los acontecimientos en otros entornos operativos, con el uso de mecanismos de poder. Mientras que el mismo estudioso, refleja que la ciberestrategia representaría el impulso y utilización de las capacidades operativas en el ciberespacio, integradas y articuladas con diferentes dominios operacionales, para alcanzar o apuntalar el éxito de los objetivos, por intermedio de los elementos del poder nacional. En otros términos, la estrategia cibernética sería el emprendimiento de planes y acciones por un Estado en el ciberespacio, conforme a sus fines políticos, pero no necesariamente contiene un germen dominador, que si puede degenerarse del ciberpoder. Asimismo, Stuart H. Starr explica algunos perfiles profesionales para conformar distintos sectores neurálgicos del área cibernética, señalando que así como las aplicaciones técnicas del ciberespacio deben ser cubiertas por físicos, ingenieros electricistas, informáticos, y de sistemas, en las instancias con competencia para proyectar el ciberpoder de un Estado, se precisan especialistas que apunten planes de dominación (política, diplomática, informática, militar, y económica); y en un sentido parecido, la ciberestrategia debe procurar expertos con conocimiento extenso e interdisciplinario, que abarquen temas gubernamentales, castrenses, financieros, sociales, informáticos y de infraestructura, para que propongan los

<sup>3</sup>El término clausewitzanos es en referencia a Carl von Clausewitz.

pasos a seguir, conforme la coyuntura del contexto interno y externo. Lo formulado, pone en evidencia lo holístico que debe ser la estructuración de una ciberestrategia, que requiere cumplir con una cadena lógica, en que lo estratégico oriente lo táctico, y no a la inversa, siendo Kiravuo bastante puntual en [16], al recalcar que contrariamente a lo que se cree, la ciberdefensa no sostiene su credibilidad sobre el número de servidores, firewalls o técnicos contratados, ya que el agresor puede seleccionar el punto más vulnerable de la infraestructura tecnológica, haciéndose patente que el eje clave no es el técnico sino el estratégico, que afinará sus proyecciones conforme las pretensiones políticas que busca alcanzar el Estado, pormenorizando Olson:

”A pesar de su capacidad demostrada para producir efectos cinéticos, la verdadera importancia de la guerra cibernética radica en su aplicación estratégica” [20].

#### 10.4. Elementos Normativos y Principios de la Ciberguerra

La confrontación entre las naciones ha sido una constante generadora de conflictos durante toda la historia, Vladimir Ilyich Lenin, inspirado en los enunciados de Clausewitz, argüía en [21], que la guerra es un proceso intrínseco al hecho político, debiendo el accionar bélico mantener un hilo conductor con las decisiones que lo originaron, que en definitiva concluirán con la imposición de uno sobre otro. Esa supremacía sobre el oponente, por intermedio del acto de fuerza, se percibe en el campo informático, que es fuente de discordia entre las potencias mundiales en la actualidad, acotando Colom:

“También verá disputada su hegemonía en áreas puntuales como el espacio, el ciberespacio o la información” [22].

Esta lucha en el ciberespacio es ya una realidad, aconteciendo acciones informáticas intrusivas o saboteadoras entre naciones con un largo historial de enemistad, o choque de intereses, pudiendo citarse los casos de Irán/Israel, Corea del Norte/Corea del Sur, pero más allá de las contiendas regionales, hay una nueva bipolaridad mundial en el siglo XXI, que ha tenido a las redes computacionales como punto central de la diatriba, el ex secretario de defensa estadounidense León Panetta, en el año 2012 señaló que la magnitud de la ciberamenaza representaba una preocupación creciente para la nación norteamericana, sugiriendo:

“Los escenarios más destructivos implican que actores cibernéticos lancen varios ataques a nuestra infraestructura crítica de una sola vez, en combinación con un ataque físico en nuestro país. Los atacantes también podrían tratar de desactivar o degradar los sistemas militares críticos y redes de comunicación” [23]<sup>4</sup>.

Este discurso del alto funcionario estadounidense, coloca al ciberespacio en la palestra de la lucha hegemónica por el poder, ya que han sido continuas las acusaciones mutuas por parte de las grandes potencias (China/Estados Unidos) sobre incursiones o sabotajes informáticos, al punto que el diario oficial del Ejército Popular de Liberación de China, ha hecho públicos serios cuestionamientos a las acusaciones de Washington, destacando las del investigador Wang Xinjun, quien expresó:

“A pesar de que es de sentido común que no se puede determinar las fuentes de los ataques cibernéticos sólo a través de las direcciones IP, algunas personas en el Pentágono todavía prefieren creer que son de China, ya que siempre tienen un sentido de la rivalidad” [24]<sup>5</sup>.

Las aseveraciones de ambos gobiernos, describen la tensa relación política, observándose el acrecentamiento de la hostilidad, derivada de los ataques cibernéticos mutuamente imputados, generando una interrogante: ¿Puede un ciberataque constituir un acto de guerra?, razona Stone en [25], que el papel influyente de las herramientas tecnológicas se basa en su potencial mediador, que puede transformar el limitado hecho de pulsar un teclado, en una vorágine violenta con posibilidad de causar destrucción y muerte. Una forma de ejemplificar esta aserción, es explicando los experimentos efectuados en el año 2007, en el Laboratorio Nacional de Idaho (Estados Unidos) [26], en donde se realizaron ataques informáticos sobre una planta de energía, logrando la prueba que el generador perdiera el control, induciendo su autodestrucción, inquietando al gobierno norteamericano, y la industria eléctrica, sobre el alcance de un ataque real a un objetivo mayor. Aunque ya no se

<sup>4</sup>Traducción realizada por el autor del presente capítulo.

<sup>5</sup>Traducción realizada por el autor del presente capítulo.

pone en duda la capacidad destructiva de los cibertataques, la gran disyuntiva, es el ligar la trilogía atacante-arma-objetivo, que en el mundo cinético es menos difusa, Rid en [27] aporta que tanto el acto de guerra o acto de fuerza tradicional, puede comprender fuego de artillería, una aeronave de ataque no tripulada, explosivos caseros situados en una carretera, inclusive un terrorista suicida en un lugar público, pero un acto de guerra cibernética es una acción íntegramente diferente.

El análisis de Rid, que intenta afinar la condición de letalidad, para configurar un acto de guerra, entrevé lo confuso que es aplicar esa tipología al atacante y acto hostil digital, y que la proporcionalidad en la respuesta es aún más entramada, ya que confundir un hecho individual, con un acto de otro Estado, puede ser el desencadenante de una guerra cinética. Sumado a esto último, la relativa libertad de acción cibernética con que actúan algunas fuerzas militares, se traduce en un peligro latente, que puede causar un acto de guerra informático, que no esté autorizado por las jerarquías políticas. Haciendo una comparación sobre los protocolos para el uso de armamento nuclear en la Guerra Fría, que estaban estrictamente delimitados, destaca Junio en [28], la disparidad en el proceder del uso de ciberarmas<sup>6</sup>, que al desvirtuarse su letalidad, se percibe su uso como ampliamente potestativo, pudiendo observarse que los controles para su ejecución son más bajos que otros armamentos, a pesar que el costo de los ataques cibernéticos puede ser superior. En este orden de ideas, Beidleman [29] intenta exponer esa tenue línea entre la guerra y un ataque de menor gravedad, aclarando que más allá del ciberataque y su carácter intrínsecamente hostil, en el espacio cibernético, no todas las acciones inamistosas se equiparan con un ataque armado, pero en algún momento, se cruza el límite, y se asume el evento digital como una agresión bélica. Esta ilustración teórica, aflora lo dubitativo que es canalizar los factores de reconocimiento del acto de guerra informático, siendo ilusorio asegurar que hay un consenso mundial sobre la temática, particularmente porque la brecha tecnológica entre las naciones que tienen mayor desarrollo cibernético, y los países que arrastran problemas sociales estructurales más graves, colocan el debate en diferentes ámbitos de prioridad, dando una ventaja injusta a quienes accionan irrestrictamente en el ciberespacio, al poseer un monopolio tecnológico.

Otra dificultad para detectar la autoría de un acto de guerra informático, recae en la multiplicación de grupos o individualidades, que bien sean a *motu proprio* o bajo el patrocinio de algún Estado, pueden causar severos daños a la infraestructura de una nación, con un sutil mecanismo cibernético. Estos actores no gubernamentales, irregulares, o asimétricos, son una variable que expone a los Estados a agresiones informáticas, siendo referidos por Sánchez:

[...]“Actualmente, existen alrededor de 10.000 sitios web dedicados a la divulgación de material violento y terrorista, lo que indica un crecimiento de la presencia de estos grupos en el ciberespacio” [30].

Lo ininteligible del contendor que atacará, bien sea en la búsqueda por posicionar sus luchas ante la comunidad internacional o hacer visible sus exigencias (políticas, religiosas, ideológicas, reivindicativas, económicas), hacen dificultoso el rastrear el origen de un ataque cibernético, debiendo el Estado o entidad vulnerada dar una respuesta en una fracción de tiempo, discerniendo si se dirigirá hacia un actor estatal o no estatal, asomando Goldsmith en [31], lo arduo e intensivo tanto técnica como económicamente, y en ocasiones inverosímil, el poder delinear de dónde partió un ataque cibernético profesional o de explotación cibernética, siendo un reto menos alcanzable el intentarlo en tiempo real. En resumidas cuentas, de las ideas precedentes, se exteriorizan elementos que colocan lejano el establecimiento del acto de guerra informático bajo un marco regulatorio internacional, acotando Brenner [32], que una secuela del “isomorfismo” de la soberanía/territorio, es que los factores amenazantes contra el orden social son sencillamente reconocibles como internos (crimen/terrorismo) o externos (guerra), pero con la entrada de la comunicación mediada por redes informáticas, se deterioró esta percepción binaria, difuminando la relevancia territorial.

El último conflicto referencial a gran escala que fue la Guerra Fría, tuvo en la estrategia de “Destrucción Mutua Asegurada”, un acuerdo no escrito, que exponía los pasos para evitar una operación militar que conllevara a una confrontación letal, pero en el “teatro de operaciones informático”, las formas para regular el proceder de la guerra computacional no existen a escala global, a pesar que tienen el potencial de trascender y anular perspectivas bélicas como las vividas en la bipolaridad del siglo XX. Esto hace impostergable el

<sup>6</sup>Como ejemplo están las armas informáticas bajo la denominación de *malware*, que abarca los virus, los gusanos, los caballos de Troya, los denominados *rootkit*, las bombas lógicas, entre otros.

establecimiento de normas, que sienten las bases de un Derecho Internacional sobre la materia, que permita fijar límites a los Estados, así como lo hicieron en su momento las convenciones sobre la guerra de Ginebra, según Janczewski y Colarik en [33], es inaplazable una legislación mundial para afrontar la guerra cibernética y el ciberterrorismo, que ameritaran nuevas e innovadoras reglamentaciones, e investigaciones de tecnologías y contramedidas. Este debate necesario sobre la ciberguerra, debería partir de la Organización de las Naciones Unidas (ONU), que es la instancia que puede generar parámetros internacionales para delimitar el accionar bélico en el ciberespacio, conteniendo el propio texto fundacional, principios jurídicos que son aplicables a la lucha virtual, que está empezando a prevalecer entre los países, estableciendo el artículo segundo de la Carta de las Naciones Unidas (1945), en su cuarto numeral que:

“Los Miembros de la Organización, en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los propósitos de las Naciones Unidas” [34].

Sin embargo, para el momento de adopción de este instrumento, no se avizoraba lo poco convencional que sería el panorama bélico medio siglo después, al respecto Hoisington [35] indica, que para especificar aspectos de la guerra cibernética, el sistema internacional debe consensuar la significación de estos actos conforme a la Carta, con mayor atención en el artículo segundo, numeral cuarto sobre la regulación del uso de la fuerza. Los menudos intentos por promover una normativa mundial, han sido relegados paulatinamente, ya que proyectar los basamentos legales de la guerra cinética a la informática es enmarañado, como argumenta Banks [36], el lograr un acuerdo sobre las aplicaciones del Derecho Internacional en la ciberguerra, es complejo por las características únicas del espacio cibernético, específicamente en lo atinente a establecer la intencionalidad de un ataque o la tipificación de las amenazas. Estas “lagunas” normativas sobre la ciberguerra, han desembocado en la estructuración de medidas supraleales, por parte de naciones o instancia de defensa multinacionales, que ante el letargo o despreocupación de la comunidad internacional, han generado un conjunto de doctrinas sobre el ciberespacio, pudiendo mencionarse dos ejemplos palpables, uno sería el llamado *Tallinn Manual on the International Law Applicable to Cyber Warfare*, elaborado por un conjunto de expertos a pedido del Centro de Excelencia en Ciberdefensa Cooperativa de la Organización del Tratado del Atlántico Norte (OTAN) [37], en el año 2013; y por otra parte, la *Presidential Policy Directive 20* [38], que fue emitida en 2012 por la *National Security Agency* (NSA), que representan antecedentes en lo jurídico, estratégico y operativo de la ciberguerra, pero además, muestran los peligros que se avecinan relacionados con la unilateralidad y extraterritorialidad.

#### **10.5. El escenario regional ante la ciberguerra y la construcción de una Identidad Digital suramericana (IDS) como factor contribuyente a una Defensa Cibernética en la UNASUR**

Antes de adentrarnos en aspectos de lo que podría considerarse una IDS, hay que examinar los acontecimientos que fueron configurando ese sentido de identificación multinacional. Durante el período comprendido entre el inicio del siglo XX y la década de los noventa del mismo, las formas de regionalización en Suramérica fueron acompañantes de los modelos económicos nacionales o supranacionales, con un limitado espacio de maniobra en ámbitos estratégicos (políticos, sociales, ambientales o tecnológicos). La institucionalidad suramericana que precedió a la UNASUR, es decir la Comunidad Andina de Naciones (CAN) y el Mercado Común del Sur (MERCOSUR), se manejaron dentro de un ámbito que en gran medida maximizaba lo comercial, encuadrado en una regionalización más que un regionalismo, que los teóricos Bernal-Meza, y Masera intentan deslindar, ya que los conceptos suelen ser usados como pares:

“Si la regionalización es el proceso mediante el cual se conforman áreas regionales de comercio en la economía mundial, el regionalismo es tanto el sistema de ideas que actúa como teoría de la diversificación de los espacios de integración en el escenario internacional, como el criterio normativo que permite la formulación de políticas orientadas a la construcción de esquemas institucionales regionales” [39].

Sólo hasta iniciado el nuevo milenio, la región empezó a establecer procesos que trascendían la regionalización, unificándose esfuerzos para construir un “regionalismo suramericano”, que tuviera un perfilamiento político-estratégico, lográndose una primera experiencia que tomó forma en la Comunidad Sudamericana de Naciones (CSAN), que tuvo en la III Cumbre Presidencial Suramericana celebrada en Perú en 2004 un avance



significativo, quedando establecida en la declaración final, la voluntad colectiva de los mandatarios asistentes para crear una institucionalidad en la región. Las vivencias de la CSAN, sirvieron de fase previa para la maduración de la identidad suramericana, lográndose establecer algunas convergencias de agendas y planteamientos. Empero, la dinámica de interacción suramericana marcaba la necesidad de trascender esta iniciativa, para propiciar un proceso de mayor alcance, que como explica Bizzozero:

“En particular, se fueron esbozando, a partir de los cambios de gobierno que se produjeron en los países de la región: una modificación de las prioridades, centrándolas en lo político y social; una vinculación del regionalismo con el debate estratégico sobre el orden internacional y su estructura” [40].

Esto motorizó la creación de una unidad, que se adaptó a la realidad de los actores regionales, que requerían un espacio de articulación e integración que fuera más allá del “reunionismo”, aconteciendo que en la cumbre energética suramericana, realizada en Venezuela en 2007, se diera nacimiento a la UNASUR. Ratificándose esta decisión, en la reunión con carácter extraordinario citada en Brasilia en el año 2008, donde finalmente se instauró el Tratado Constitutivo, que dejaba expresamente señalado en su artículo segundo:

“La Unión de Naciones Suramericanas tiene como objetivo construir, de manera participativa y consensuada, un espacio de integración y unión en lo cultural, social, económico y político entre sus pueblos, otorgando prioridad al diálogo político, las políticas sociales, la educación, la energía, la infraestructura, el financiamiento y el medio ambiente, entre otros, con miras a eliminar la desigualdad socioeconómica, lograr la inclusión social y la participación ciudadana, fortalecer la democracia y reducir las asimetrías en el marco del fortalecimiento de la soberanía e independencia de los Estados” [41].

Todo este proceso que amalgamó el “regionalismo suramericano”, hizo evidente que existía una serie de atributos, y rasgos que individualizaban a los habitantes de Suramérica, pudiendo hablarse de una “identidad suramericana”, que era palpable en las realidades históricas compartidas, y como lo plasma el tratado constituido, por los aspectos culturales, sociales, económicos, político, educativos, energéticos, financieros, ambientales, que persiguen combatir la desigualdad socioeconómica, para alcanzar la inclusión social y la participación ciudadana, en búsqueda de consolidar valores comunes como la democracia, soberanía e independencia. Los hechos expuestos, hacen patente que la “identidad suramericana” es concreta, y que jugó un papel crucial para acelerar la integración en la UNASUR, asumiéndose a escala regional una tarea de caracterización de esos matices identificativos, que han mostrado un avance interesante en la llamada Identidad en Defensa regional, que podría tener una articulación con la propuesta teórica de IDS que aquí se presenta, pensando en una futura estrategia defensiva del espacio cibernético suramericano ante acciones de ciberguerra. Precisamente, en ese dinamismo político que se desbordó por todo el subcontinente, hubo varios pensadores que empezaron a expresar sus consideraciones sobre la identidad en Defensa, manifestando Nelson Jobim, ex Ministro de Defensa de Brasil:

“Estoy convencido que llegó la hora de que profundicemos nuestra identidad sudamericana también en el campo de la defensa. [...] Debemos articular una nueva visión de defensa en la región fundada en valores y principios comunes, como el respeto a la soberanía, a la autodeterminación, a la integridad territorial de los Estados y a la no intervención en los asuntos internos” [42].

Las palabras de Jobim, revelaban un nivel de maduración subcontinental, ya que históricamente éstos eran temas difíciles de abordar, tras décadas de acumulación de un “sentimiento hostil”<sup>7</sup> azuzado por viejos diferendos limítrofes, significando un avance regional especialmente para debatir temas de defensa, que siempre habían estado ocultos o secretos. Ese mismo criterio fue el plasmado en el “Estatuto” para el CDS, que abogaba por una zona de paz, en donde las naciones sean garantes de la estabilidad democrática y el desarrollo integral, buscando consensuar una cooperación regional en asuntos de defensa, dejando fijado en su artículo cuarto, literal “b”, como uno de sus objetivos:

“Construir una identidad suramericana en materia de defensa, que tome en cuenta las características subregionales y nacionales y que contribuya al fortalecimiento de la unidad de América Latina y el Caribe” [44].

<sup>7</sup>En su momento Clausewitz ilustró cómo el sentimiento hostil puede ser un factor desencadenante del conflicto: “En dos naciones y Estados pueden producirse tales tensiones y tal cúmulo de sentimientos hostiles que un motivo para la guerra, insignificante en sí mismo, puede originar, no obstante, un efecto totalmente desproporcionado con su naturaleza, como es el de una verdadera explosión” [43].

Este planteamiento, resulta concordante con la propuesta del Centro de Estudios Estratégicos de Defensa (CEED) de la UNASUR, que muestra a la defensa como parte esencial del proceso de integración regional, para poder encaminarse a un sistema suramericano de defensa cooperativa, exponiendo a la “identidad suramericana en defensa”, como un conjunto de conceptos que se asemejan y enriquecen entre sí en la diversidad regional, destacando:

“Esta perspectiva estratégica suramericana se sustenta en definiciones comunes de seguridad y defensa que orientan la cooperación y complementariedad en estos campos, en base al diálogo y aproximación de las políticas nacionales” [45].

La importancia de la “identidad suramericana en defensa”, radica en un abordaje en conjunto de las amenazas, ya que las afectaciones son multiestatales, siendo el aislamiento en temas de defensa contraproducentes para los actores regionales, asentando el CEED que para procurar una paz perdurable en Suramérica, es cardinal una cooperación dirigida a erradicar los riesgos y amenazas latentes, en este sentido añade Menezes:

“No pudiendo ser resueltas de forma unilateral, las nuevas amenazas proporcionan el contexto para la cooperación en seguridad, entendiéndolas como un bien público regional” [46].

Asumiendo estos principios generales, y reconduciéndolos a una visión conjunta ante las ciberamenazas<sup>8</sup>, un pilar central podría representarlo una percepción de IDS, en búsqueda de ir enunciando con nitidez cuáles son los bienes jurídicamente protegidos, que pueden ser objeto de una operación maliciosa, e identificar la gama de acciones a emprender. Por tanto, una posible precisión sobre IDS, haría las veces de semilla teórica, generadora de un conglomerado de preceptos estratégicos, que deberían establecerse normativamente, para que se proceda a su resguardo cooperativo, pudiendo usarse como guía inicial uno de los conceptos básicos de Identidad Digital (ID), concebido así:

“Es el conjunto de datos que describen y representan a un sujeto: persona, grupo de personas o cosas de manera única. Puede contener información sobre gustos, o creencias, relaciones, tendencias, ideologías, y cualquier otro descriptor vinculado al sujeto” tal como se definió en la sección 1.1.

Hay que ser incisivo, que cuando se habla de “sujeto”, no se refiere a una singularidad, y puede entenderse como un “grupo”, siendo viable el concebir que en una región pueda haber una ID compartida. La urgencia de conceptualizar estratégicamente temas como la IDS, se refleja en un evento especialmente sensible en temas de defensa suramericano, como lo son las acciones del sistema de vigilancia extensiva manejado por EE.UU, Gran Bretaña, Australia, Nueva Zelanda y Canadá, denominado *Echelon*, que se apoya en una gran cantidad de sistemas informáticos, para controlar parte del subcontinente desde la Isla de Ascensión ubicada en pleno océano Atlántico entre el continente africano y Suramérica:

“La Isla de la Ascensión es de sólo 91 kilómetros cuadrados, y es irrelevante si no estuviera en una posición estratégica a medio camino de los continentes de África y América del Sur [...] su superficie alberga potentes estaciones de interceptación de señales (Sigint)<sup>9</sup>, que destacan como enormes bolas blancas. Integran un sistema de inteligencia avanzada que monitoriza en tiempo real a todas las comunicaciones de Brasil, Argentina, Uruguay, Colombia y Venezuela, y son parte de un proyecto conocido como Echelon” [48]<sup>10</sup>.

Los informes que han hecho público los detalles del *Echelon*, deberían conducir a que la UNASUR acelere las valoraciones y definiciones para dinamizar la delimitación de las amenazas en el entorno tecnológico, entendiendo que las mismas tienen una “virtualidad” e “inmaterialidad” que no debe tergiversarse como “ficticia”. Además de suponer una preocupación, el elemento amenazante pueden ser un catalizador para apresurar la apreciación colectiva, que puede partir de circunscribir el espacio cibernético, como un “interés regional”, que es una noción relevante para vincularla a la comprensión de la amenaza, ya que genera un foco de atención sobre un aspecto puntual, que amerita la protección, para evitar la masificación de la afectación.

<sup>8</sup>Una ciberamenaza es la posibilidad de ocurrencia de incidentes cibernéticos, propiciados por factores externos que pudieran dañar los intereses colectivos físicos ó informáticos a un Estado, nación, organización o sujetos.

<sup>9</sup>*Sigint* (Señales de Inteligencia) implica recolectar inteligencia extranjera de comunicaciones y sistemas de información y proporcionarla a clientes a través del gobierno estadounidense, como altos funcionarios públicos y oficiales militares.[47] Traducción realizada por el autor del presente capítulo.

<sup>10</sup>Traducción realizada por el autor del presente capítulo.

El concretar una concepción suramericana del espacio cibernético, como un “interés regional”, podría apuntalar la adopción de medidas que primeramente deberían estar centradas en una región con soberanía tecnológica, pensando en la disuasión como un pilar estratégico de defensa para el subcontinente. Esta disuasión es un camino complejo, ya que como establece Limnéll [49], un mensaje disuasivo, obedece a un proceso comunicativo efectivo entre el Estado y el ente a disuadir, para lograr persuadir a un posible atacante, debe haber una capacidad real de responder al agresor, correspondiendo la misma lógica al dominio cibernético. En Suramérica, hay claras pruebas que su espacio cibernético está siendo violentado, no sólo por el *Echelon*, sino por sistemas incluso más avanzados como *Prism* y *X-Keyscore*, que interfieren, espían, o manipulan la información de personas o instituciones, con el fin de hacer perfilamientos, para saber sus gustos, creencias, relaciones, tendencias, ideologías, y cualquier otro descriptor vinculado al sujeto, tal como se aclaraba en la cita sobre ID. No obstante, al no tener instituido la UNASUR conceptos como: ciberdefensa, ciberguerra, acto de guerra informático, e IDS, entre otros, se hace distante la adopción de medidas disuasivas, que garanticen una respuesta cooperativa ante la vulneración. Para Clausewitz la disuasión era un punto focal de la guerra, exponiendo que el hecho militar normalmente viene acompañado de una postura que exterioriza fortaleza ante el adversario, con la finalidad de advertirle lo contraproducente que sería iniciar un conflicto, especificando:

“A menudo la guerra no es más que una neutralidad armada o una actitud amenazadora destinada a entablar unas negociaciones, o un intento moderado de ganar alguna ventaja y esperar luego el resultado” [43].

Esta actitud asentada por el prusiano, se logra con un desarrollo del pensamiento estratégico en defensa, ya que la disuasión es una postura colaborativa de todos los componentes de la unidad, y en temas tan puntuales como la ciberguerra, debe haber un acompañamiento monolítico, para que la orquestación defensiva/ofensiva proyecte una credibilidad disuasiva, según se profundiza en [45], al adversario tener certeza que la infraestructura informática es resistente, con capacidad de detectar y prevenir amenazas, junto con el potencial de efectuar contraataques, la acción disuasiva es fuerte. Como reflexionaba Alfredo Fortí, Director del CEED, en la Conferencia “Visiones Hacia una Estrategia Suramericana para el Aprovechamiento de los Recursos Naturales”, celebrada en Caracas:

“la disuasión “hacia fuera”, implica que nuestras capacidades regionales en materia de defensa y militar deben concentrarse y fundirse en una sola cuando de lo que se trata es proteger al interés regional” [...] [50].

En cuanto a las medidas que dentro del proceso institucional de la UNASUR, y el CDS, se han tomado en temas cibernéticos de defensa, hay tres puntos de marcada importancia: los “Planes de Acción 2012/2013”, la decisión de creación del “Mega Anillo de Fibra Óptica”, y el pronunciamiento en 2013 en la cumbre de Paramaribo. En primera instancia, los asuntos cibernéticos pasaron a ser parte de la matriz de análisis del CDS, en su “Plan de Acción 2012”, donde se deja establecido en su punto “1.f” lo siguiente:

“Conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa” [51].

En el documento se asigna la responsabilidad directa a la delegación peruana, y como corresponsables a Venezuela y Uruguay, ampliándose en 2013 con la inclusión de las delegaciones colombiana y brasileña. Dentro de los aportes de este grupo de trabajo, la delegación peruana en 2013, presentó un documento que se titula: “Establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa”, que explicaba tres grandes objetivos: técnicos, formativos, y legislativos. En esta propuesta que tiene elementos importantes y necesarios, no se plasma un tratamiento suramericano de las amenazas cibernéticas en un contexto de ciberguerra, precisándose un bosquejo que refleje capacidades regionales y exteriorice las inferioridades tecnológicas, para determinar esa “base objetiva” que es propiciadora de iniciativas estratégicas, sobre esto reflexionó hondamente Mao:

“La iniciativa es inseparable de la superioridad en la capacidad bélica, en tanto que la pasividad es inseparable de la inferioridad en ese terreno. Tal superioridad o inferioridad constituyen, respectivamente, la base objetiva para la iniciativa o la pasividad” [52].

De lo acotado por el estratega chino, se decanta que una propuesta de IDS podría ser el punto de partida de esa “iniciativa”, que proporcionaría los cimientos para que la UNASUR amalgame una idea central en defensa cibernética. Por tanto, una forma concreta de marcar distancia con la “pasividad”, es con la consecución de

una fundamentación estratégica que no puede ser posterior a decisiones en temas: técnicos, formativos, y legislativos.

Dentro de esa misma perspectiva de asumir decisiones sobre temáticas relacionadas a asuntos cibernéticos, la totalidad de representantes de las carteras ministeriales de ciencia, tecnología y comunicaciones suramericanas, acordaron la creación del “Mega Anillo de Fibra Óptica”. La importancia de este proyecto está íntimamente ligada a salvaguardarse informáticamente como región, en búsqueda de revertir el escenario actual, que muestra a las infraestructuras críticas de Suramérica, estrechamente interrelacionadas con plataformas informáticas extraregionales, como refleja Raúl Zibechi:

“Un mail enviado entre dos ciudades limítrofes de Brasil y Perú, por ejemplo entre Rio Branco, capital de Acre, y Puerto Maldonado, va hasta Brasilia, sale por Fortaleza en cable submarino, ingresa a Estados Unidos por Miami, llega a California para descender por el Pacífico hasta Lima y seguir viaje hasta Puerto Maldonado, a escasos 300 kilómetros de donde partió” [53].

Aunque medidas como el “Mega Anillo de Fibra Óptica”, buscan técnicamente paliar el escenario descrito, el asumir la problemática exclusivamente como un asunto de infraestructura, no haría sino replicar errores cometidos en instancias nacionales, donde se han intentado acciones sin conocer el contexto informático, y obviando un estudio concienzudo de la amenaza. La forma de lograr ese entendimiento, es estableciendo definiciones como la de IDS, que representaría un punto intermedio: contexto/bien o sujeto/amenaza, pudiendo complementarse el eslabón teórico-técnico, para alcanzar una observación macro de la situación, que permita estudiar las vulnerabilidades propias de la “dependencia tecnológica”, y la gravedad del hecho, que parte de la información regional pasa previamente por un actor ajeno a Suramérica, lo que expande la magnitud del problema. Conforme sugiere Huopio en [54], es inexistente una amenaza cibernética separada de la totalidad de escenarios, transformándose en un factor amenazante horizontal, lo que debe ser la mayor preocupación para nuestros países, ya que el atacante que utiliza sistemas para la extracción de información (por ejemplo: *Echelon*), ya ha identificado las vulnerabilidades de la infraestructura atacada, y al tener precisadas estas debilidades, puede proceder posteriormente a acciones que ocasionen un daño no sólo virtual sino físico<sup>11</sup>. La congruencia del “Mega Anillo de Fibra Óptica”, no recae sólo en la infraestructura, sino en la potencialidad para preparar estrategias colaborativas, que permitan afrontar un eventual escenario de ciberguerra, teniendo en consideración que la tecnología es una herramienta que puede amoldarse a cualquier funcionalidad, siendo igualmente provechosa como destructiva, esto lo fundamentan Liang y Xiangsui:

“Mientras que la revolución de la tecnología militar ha permitido que uno sea capaz de seleccionar medidas dentro de una variedad más grande, también se ha hecho para que uno se vea amenazado por estas medidas dentro de la misma gama (esto se debe a que el monopolio de un tipo de tecnología es mucho más difícil que inventar una tecnología). Estas amenazas nunca habían sido como hoy, porque las medidas son diversas e infinitamente cambiantes, y esto realmente le da a uno la sensación de ver al enemigo detrás de cada árbol” [55]<sup>12</sup>.

En medio de la controversia mundial que generaron los informes filtrados, que exhibían las acciones cibernéticas ilegales de un conjunto de gobiernos, la VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la UNASUR, mantuvo una postura cónsona con las gestiones ministeriales acordadas en el Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN), y las entrelazó con los ejes del CDS, procediendo a instruir:

“Al Consejo de Defensa Suramericano (CDS) y al COSIPLAN, evaluar la cooperación con otros consejos ministeriales competentes y avanzar en sus respectivos proyectos sobre defensa cibernética y la interconexión

<sup>11</sup>Es importante explicar, que el ser víctima de sistemas como *Echelon*, *Prism* y *X-Keyscore* no puede ser tomado como un mero “espionaje”, y deben ser valorados como una acción de ciberguerra, ya que estas herramientas extraen información estratégica e identifican las falencias técnicas de los afectados, que pueden ser aprovechadas para efectuar operaciones concretas con consecuencias cinéticas como las *Computer Network Operations (CNO)*, *Computer Network Exploitation (CNE)*, *Computer Network Attack (CNA)*, *Computer Network Defense (CND)*, y las *Information Operations (IO)*. De hecho, en el informe filtrado “*United States SIGINT System January 2007 Strategic Mission List*”, en el punto: “*Enabling Computer Network Attack (CNA): Deliver intelligence, access, and dual-use capabilities in support of U.S. computer network attack objectives*”, se clarifica lo argumentado.

<sup>12</sup>Traducción realizada por el autor del presente capítulo.

de las redes de fibra óptica de nuestros países, con el objetivo de tornar nuestras telecomunicaciones más seguras, fortalecer el desarrollo de tecnologías regionales y promover la inclusión digital” [56].

En referencia a la instrucción efectuada por los primeros mandatarios, es conveniente destacar la integralidad dada al direccionamiento para la defensa cibernética, en búsqueda de no divorciar lo estratégico, político, y operativo, que coincide con lo esbozado en [57] por Kärkkäinen, debiéndose visualizar la complejidad del entorno, no siendo un asunto de proteger y defender aisladamente la información, en vista que la totalidad de la infraestructura de procesamiento informática conserva operativos los ecosistemas económicos, políticos y sociales. En este sentido, la congregación de iniciativas busca contribuir a ampliar el horizonte estratégico, siendo oportuno que se tome en cuenta para la defensa cibernética suramericana, uno de los ejes del CDS, relacionado a: “Industria y Tecnología de la Defensa”, que fue pensado para:

“Elaborar un diagnóstico de la industria de Defensa de los países miembros identificando capacidades y áreas de asociación estratégicas, para promover la complementariedad, la investigación y la transferencia tecnológica” [58].

Esto debe ser concebido como un factor importante para encaminar al subcontinente a una “soberanía tecnológica”, que contribuya a la perspectiva enunciada por Forti de: “cooperación hacia dentro, disuasión hacia afuera”. Empero, la transferencia tecnológica por sí misma no tiene un valor agregado, esto recae en percibir su fondo estratégico y comprender qué se quiere lograr con el conocimiento transferido. Es decir, la “Industria y Tecnología de la Defensa” puede representar el punto de partida de un vasto proyecto regional, pero debe ajustarse a la necesidad de software y hardware bajo estándares libres<sup>13</sup>, que requiera la defensa del ciberespacio suramericano (Particularmente la IDS), siendo ineludible reconfigurar la visión de ciencia y tecnología regional, que aún responden a patrones de dominación. El uso de tecnologías libres, no es un modismo, y todas las argumentaciones estratégicas expuestas serían en vano, si se pretendiera asumir políticas tecnológicas subcontinentales, que sean reproductoras de las visiones privativas o economicista del Complejo Militar Industrial, acotando Julian Assange:

“Es necesario poder mantener la libertad de las comunicaciones, por lo que debemos hacer un cambio al software libre y adaptarnos a su uso, codificarlo y evitar que lean nuestras comunicaciones y revisen nuestros registros y operaciones” [60].

Finalmente, entrando en el ámbito de la conceptualización de la ciberdefensa que se propone desde el plano regional, es significativo hacer algunas apreciaciones teóricas sobre las connotaciones defensiva y ofensiva, para comprender los ataques cibernéticos en toda su dimensión. Pensadores militares desde el siglo XIX han sido propiciadores de enconadas reyertas intelectuales para deslindar las visiones de “defensa” y “ataque”, el propio Clausewitz llamaba la atención de las diferenciaciones que deben ser estudiadas en su justa medida:

“Si sólo existiera una forma de guerra, digamos la que corresponde al ataque del enemigo, no habría defensa; ello es tanto como decir que si hubiera de distinguirse al ataque de la defensa sólo por el motivo positivo que el uno posee y del que la otra carece, si los métodos de lucha fueran siempre invariablemente los mismos, en tal empeño, cualquier ventaja de un bando tendría que representar una desventaja equivalente para el otro, existiendo entonces una verdadera polaridad. Pero la acción militar adopta dos formas distintas, la de ataque y la de defensa, que son muy diferentes y de fuerza desigual” [43].

No es menor esta discusión, que puede contribuir a centrar y precisar las respuestas ante las amenazas cibernéticas subcontinentales, pero de no dirigirse correctamente, podría caer en un marasmo propio de las generalidades, que contribuiría a ensanchar las vulnerabilidades. El propio Mao aleccionaba que los ámbitos de la “defensa” y el “ataque”, deben ser correctamente asumidos por las particularidades que limitan y potencian su accionar, detallando:

“El ataque es el medio principal para destruir las fuerzas enemigas, pero no se puede prescindir de la defensa. El ataque se realiza con el objetivo inmediato de aniquilar las fuerzas del enemigo, pero al mismo tiempo para

<sup>13</sup>Se puede tomar como referencia la conceptualización de tecnologías libres, establecida en la Ley de InfoGobierno venezolana: “Son aquellas tecnologías con estándares abiertos que garantizan el acceso a todo el código fuente y la transferencia del conocimiento asociado para su comprensión; libertad de modificación; libertad de uso en cualquier área, aplicación o propósito y libertad de publicación del código fuente y sus modificaciones” [59]

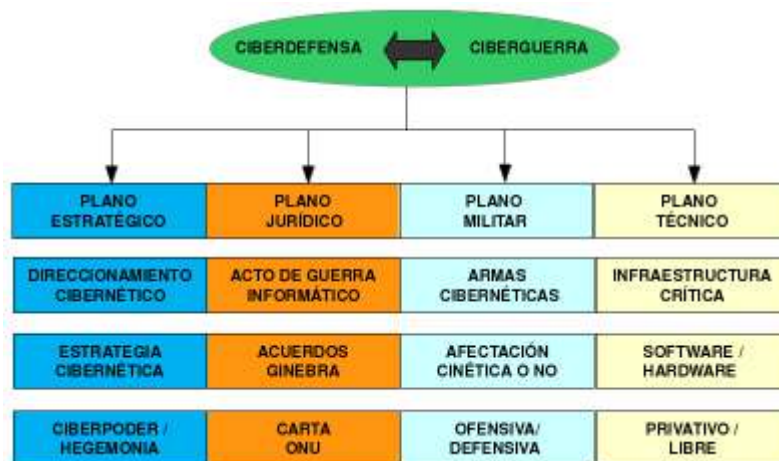
conservar las fuerzas propias, porque si uno no aniquila al enemigo, será aniquilado. La defensa tiene como objetivo inmediato conservar las fuerzas propias, pero al mismo tiempo es un medio de complementar el ataque o de prepararse para pasar a éste” [52].

En el momento que la VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la UNASUR hizo uso del término “Defensa Cibernética”, las diferentes instancias como el CDS, el CEED y las delegaciones que tienen la responsabilidad y corresponsabilidad deben concretar qué incluye y excluye este concepto, y tomar la bidimensionalidad que acusa Clausewitz y Mao, y que complementa Basil Liddell Hart:

“Una verdad más profunda a la que no llegaron plenamente Foch ni los otros discípulos de Clausewitz, es la de que en la guerra todo problema, como todo principio, es necesariamente dual. Tiene dos caras, como una moneda, y de aquí la necesidad de llegar a una componenda bien calculada como medio de conciliación. Esto es consecuencia inevitable del hecho de ser la guerra un juego entre dos bandos e imponer por lo tanto la necesidad de guardarse a la vez que se ataca” [61].

En este diálogo de cierre, relacionado a las apreciaciones sobre “defensa” y “ataque”, se quiere hacer notar que la guerra tradicional o su variable cibernética, deben observarse dualmente, y que la enunciación que se le concede, no es una cuestión sólo de forma, sino que reviste un fondo importante. Una explicación que da un justo equilibrio entre “defensiva” y “ofensiva”, centrándose en la temática informática, es la matizada por Kärkkäinen [57], aportando que la defensa cibernética consiste en las capacidades operativas, defensivas, ofensivas y de inteligencia, en el espacio cibernético. La anterior apreciación ratifica y complementa lo señalado por los otros estrategas, necesitándose para la delimitación de estas capacidades operativas, defensivas, ofensivas y de inteligencia en una escala regional, el aclarar los límites conceptuales de la ciberdefensa para la UNASUR, y que en definitiva logren la concisión de medidas ante acciones de ciberguerra, que resguarden entre otros ámbitos del ciberespacio la IDS.

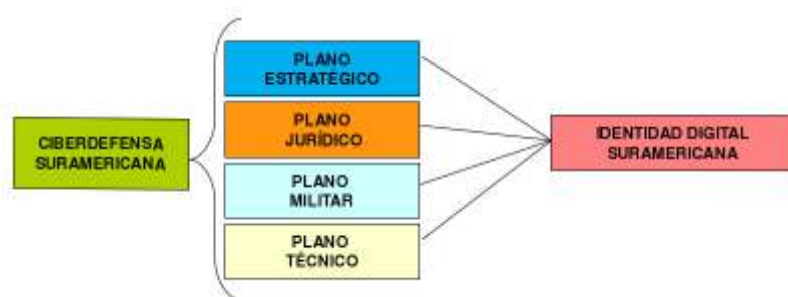
La tarea de formular una propuesta en esta temática, no pasa solamente por demarcar su carácter ofensivo/defensivo, debiendo subrayarse que para pensar en ciberdefensa, también se debe asumir el estudio de la ciberguerra, porque se considera que son conceptos que van al unísono, y sólo con su acoplamiento teórico se podrá alcanzar la profundidad de los planos: estratégico, jurídico, militar y técnico, que se han venido explicando a lo largo de este capítulo. Estos conceptos ciberdefensa-ciberguerra deben desarrollarse paralelamente, y sus diferentes planos enriquecerse mutuamente, para evitar desfases que ocasionen la potenciación de uno en desmedro del otro. En la figura 10.1 se muestran los diferentes planos a considerar en la dualidad señalada.



**Figura 10.1** Ciberdefensa - Ciberguerra: Planos

En relación a lo indicado en la explicación y en el cuadro explicativo, la IDS que se ha venido proponiendo, podría tener la capacidad de hacer converger en la realidad de la UNASUR, la diversidad de planos

detallados. El proponer una IDS pondría en marcha el proceso valorativo del ciberespacio como un interés regional, que es vinculante al plano estratégico, contribuyendo a que desde una mirada regional, se pueda estipular qué está siendo atacado, trayendo como resultado que se sustente sobre bases sólidas los rasgos de un acto de guerra informático para el subcontinente. En esta etapa, un tratamiento militar/civil es ineludible, para trabajar sobre las vulnerabilidades internas y las capacidades de potencias externas, con la finalidad de proponer acciones ofensivas y/o defensivas, que deben estar en sintonía con las proyecciones técnicas que se tengan en la región, que abarca no sólo el hecho de las infraestructuras críticas, sino el debate de lograr soberanía e independencia informática sustentadas en una idea de tecnologías libres y liberadoras. A continuación se presenta una esquema en la figura 10.2 sobre la concentración de los planos en la IDS, en un contexto general de ciberdefensa.



**Figura 10.2** Ciberdefensa y la IDS

## 10.6. Algunas Ideas Finales

En el presente artículo, se buscaba observar la evolución que la temática de la ciberguerra ha tenido en Suramérica, avistándose que hay evidencias del uso de medios informáticos como el *Echelon* contra la región, que no limita las acciones al personal gubernamental o militar específico, sino que toda la población está siendo monitoreada y perfilada. Ante esta realidad, que muestra a determinadas naciones u organizaciones con un uso agresivo, desmedido y belicoso del ciberespacio, se debe sincerar en la UNASUR, el tratamiento ante actos de ciberguerra, que se deslastre de posiciones dubitativas, meramente políticas o diplomáticas, en un frente de batalla que aunque no convencional es real. Enfocar estratégicamente el espacio cibernético de Suramérica, como un “interés regional”, amerita un tratamiento que exteriorice su importancia, acoplándolo con la IDS, que podría relacionarse no sólo a información personal de usuarios, sino a datos de sistemas de defensa, finanzas, energía (Hidroeléctricas, Complejos Petroleros), servicios públicos, telecomunicaciones, entre otros. Si se lograra esta perspectiva, integraríamos dos visiones que contribuirían a clarificar el proceder ante un escenario de ciberguerra: el “interés regional” (ciberespacio), y el “bien jurídico protegido” (IDS), pudiendo trabajarse estratégicamente para evaluar los factores de riesgo externos, representados por las “amenazas” (ataques cibernéticos), y configurar una defensa cibernética con un tono disuasivo en el marco de la UNASUR, que en estos momentos es todavía el principal factor de riesgo interno.

En este escenario variable y en proceso de definición, se puede distinguir que el reconocimiento por parte de los entes decisorios subcontinentales, de una noción de IDS, permitiría contextualizar los riesgos y coadyuvaría a la adopción de medidas en ciberdefensa, que ineludiblemente terminarán por tocar asuntos estructurales, ya que se requiere desarrollar una “Industria y Tecnología de la Defensa”, sostenida sobre estándares libres. A manera de cierre y con la finalidad de contribuir teóricamente en este debate, se presenta la siguiente apreciación sobre lo que debería ser la Identidad Digital Suramericana IDS: es toda aquella información digital que caracteriza individual o colectivamente a personas naturales o jurídicas, que es intercambiada, almacenada, distribuida, o resguardada, en el espacio cibernético de Suramérica, y que es considerada como un bien jurídico protegido por la UNASUR, que garantizará su defensa cooperativa ante un ataque cibernético, que pueda estar vinculado a un delito informático o acción de ciberguerra.

## REFERENCIAS

---

1. Real Academia de la Lengua Española. Diccionario de la lengua española (drae). <http://lema.rae.es/drae/?val=cibernética>, 2001.
2. N. Wiener. *Human use of human beings: Cybernetics and society*. Da Capo Press, 1998.
3. L. Burtseva, V. Tyrsa, B. Ríos, and L. Flores. Norbert wiener: Padre de la cibernética. *Revista UABC*, 4(54):48, 2013.
4. R. Ashby. *An introduction to cybernetics*. Chapman & Hall, 1957.
5. W. Gibson. *Neuromante*. Minotauro, 1984.
6. A. Cicognani. On the linguistic nature of cyberspace and virtual communities. *Virtual reality*, 3(1):20, 1998.
7. D. Post. Against'against cyberanarchy. *Berkeley Technology Law Journal*, 17:10, 2002.
8. P. Andres. Anthropic cyberspace: Defining electronic space from first principles. *Leonardo*, 34(5):405, 2001.
9. H. Flores. Los Ámbitos no terrestres en la guerra futura: Ciberespacio. *Centro Superior de Estudios de la Defensa Nacional Monografías del Ceseden*, (128):18, 2012.
10. J. Fritz. The semantics of cyber warfare. *East Asia Security Symposium and Conference*, 1(7):2, 2013.
11. S. Winterfeld and J. Andress. *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Elsevier Inc., 2012.
12. G. McGraw. Cyber war is inevitable (unless we build security in). *Journal of Strategic Studies*, 36(1):111–112, 2013.
13. Kostyuk N. and Alí M. The cyber dogs of war: Joint efforts of future world leaders in the prevention of cyberwarfare. In The Society of Digital Information and Wireless Communication, editors, *The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013)*, 2013.
14. J. Lewis. The cyber war has not begun. *Center for Strategic and International Studies*, 2010.
15. J. Ferrero. La ciberguerra. génesis y evolución. *Revista General de Marina*, (Enero-Febrero):87, 2013.
16. T. Kiravuo. Offensive cyber-capabilities against critical infrastructure. *Cyber Warfare. National Defence University. Department of Military Technology*, (34):90, 2013.
17. A. Sanz and E. Fojón. Ciberespacio: La nueva dimensión del entorno operativo. *Centro Superior de Estudios de la Defensa Nacional Monografías del Ceseden*, (44):43, 2011.



18. J. Rantapelkonen and M. Salminen. The fog of cyber defence. *National Defence University. Department of Leadership and Military Pedagogy*, (2):11, 2013.
19. S. Starr. Towards an evolving theory of cyberpower. *The Virtual Battlefield: Perspectives on Cyber Warfare*, 3:22–24, 2013.
20. S. Olson. El boxeo con un contrincante imaginario. la guerra cibernética y el ataque económico estratégico. *Military Review*, (Noviembre-Diciembre):67, 2012.
21. Vladímir Lenin. *Vladímir Lenin Obras Tomo XII (1921-1923)*. PROGRESO, MOSCU, 1973.
22. G. Colom. El nuevo concepto estadounidense para el empleo de la fuerza militar. *ARI: Seguridad y Defensa*, (70):2, 2009.
23. L. Panetta. Remarks by secretary panetta on cybersecurity to the business executives for national security. <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136>, 2012.
24. Chinese People's Liberation Army. Pentagon's cyberattack accusations irresponsible: expert. [http://eng.chinamil.com.cn/news-channels/pla-daily-commentary/2013-05/08/content\\_5333521.htm](http://eng.chinamil.com.cn/news-channels/pla-daily-commentary/2013-05/08/content_5333521.htm), 2013.
25. J. Stone. Cyber war will take place! *Journal of Strategic Studies*, 36(1):107, 2013.
26. H. Harrison. *Cyber Warfare and the Laws of War*. Cambridge University Press, 2012.
27. J. Stone. Cyber war will not take place. *Journal of Strategic Studies*, 35(1):9, 2013.
28. T. Junio. How probable is cyber war? bringing ir theory back in to the cyber conflict debate. *Journal of Strategic Studies*, 36(1):130, 2013.
29. S. Beidleman. Defining and deterring cyber war, 2009.
30. G. Sánchez. La nueva estrategia comunicativa de los grupos terroristas. *Revista Enfoques*, VIII(12):203, 2010.
31. J. Goldsmith. The new vulnerability (how cyber changes the laws of war). *The New Republic*, 2010.
32. S. Brenner. "at light speed": Attribution and response to cybercrime/terrorism/warfare. *The Journal of Criminal Law and Criminology*, page 382, 2007.
33. L. Janczewski and A. Colarik. *Cyber warfare and cyber terrorism*. IGI Global, 2008.
34. Organización de las Naciones Unidas. Carta de las naciones unidas. entrada en vigor: 24 de octubre de 1945, de conformidad con el artículo 110, 1945.
35. M. Hoisington. Cyberwarfare and the use of force giving rise to the right of self-defense. *Boston College International and Comparative Law Review*, 32:446, 2009.
36. W. Banks. The role of counterterrorism law in shaping ad bellum norms for cyber war. 89 *INT'L L. STUD.* 157. Available at SSRN 2160078, page 162, 2013.
37. NATO Cooperative Cyber Defence Centre of Excellence Tallinn. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Schmitt, 2013. [www.ccdcoe.org/249.html](http://www.ccdcoe.org/249.html).
38. NSA. *Presidential Policy Directive 20*, 2012. "https://www.hsdl.org/?abstract&did=725668".
39. R. Bernal-Meza. Mercosur ¿regionalismo o globalización? tres aspectos para la decisión de políticas. *Revista Realidad Económica*, (165):2, 1999.
40. Lincoln Bizzozero. América latina a inicios de la segunda década del siglo xxi: entre el regionalismo estratégico y la regionalización fragmentada. *Revista Brasileira de Política Internacional*, 54(1):36, 2011.
41. UNASUR. Tratado constitutivo de la unión de naciones suramericanas, 2008.
42. G. Saint-Pierre, H.; Castro. El consejo sudamericano de defensa. *Boletín RESDAL*, 6(29):1, 2008.
43. C. Clausewitz. *De La Guerra*. Editorial Librodot, 2002.
44. Consejo de Defensa Sudamericano. Objetivos consejo de defensa suramericano unasur. <http://www.unasursg.org/inicio/organizacion/consejos/cds>, 2008.
45. CEED. Informe de avance a diciembre de 2012 sobre conceptos e institucionalidad de seguridad y defensa, amenazas, factores de riesgo y desafíos del consejo sudamericano de defensa, 2012.
46. A. Menezes. Regionalismo y seguridad sudamericana: ¿son relevantes el mercosur y la unasur? Íconos. *Revista de Ciencias Sociales*, (38):41–53, 2010.
47. NSA. Sigint frequently asked questions. <https://www.nsa.gov/sigint/faqs.shtml#sigint1>, 2009.

48. J. Dantas, C. y Jeronimo. Como eles espionam. istoe. [http://www.istoe.com.br/reportagens/paginar/323087\\_COMO+ELES+ESPIONAM/12](http://www.istoe.com.br/reportagens/paginar/323087_COMO+ELES+ESPIONAM/12), 2013.
49. Offensive Cyber Capabilities are Needed Because of Deterrence. Limnell, j. *The Fog of Cyber Defence*, (10):202–205, 2013.
50. A. Forti. El papel de la defensa en una estrategia suramericana para el aprovechamiento de los recursos naturales. conferencia suramericana visiones hacia una estrategia para el aprovechamiento de los recursos naturales, 2013.
51. Consejo de Defensa Sudamericano. Plan de acción 2012 – cds, 2012.
52. M. Zedong. *Problemas de la Guerra y de La Estrategia*. Ediciones En Lenguas Extranjeras Pekín, 1976.
53. R. Zibechi. La silenciosa revolución suramericana. <http://www.jornada.unam.mx/2011/12/02/politica/025a1pol>, 2011.
54. S. Hupio. A rugged nation. *The Fog of Cyber Defence*, (10):127, 2013.
55. W. Liang, Q. y Xiangsui. *Unrestricted Warfare*. PLA Literature and Arts Publishing House, 1999.
56. UNASUR. VII reunión ordinaria del consejo de jefas y jefes de estado y de gobierno de la unión de naciones suramericanas declaración de paramaribo, 2013.
57. A. Kärkkäinen. The origins and the future of cyber security in the finnish defence forces. *The Fog of Cyber Defence*, (10), 2013.
58. UNASUR. Declaración de santiago de chile. primera reunión del consejo de defensa suramericano (cds) de la unión de naciones suramericanas (unasur), 2009.
59. Asamblea Nacional. Ley de infogobierno. Gaceta Oficial de la República Bolivariana de Venezuela Número: 40.274 del 17/10/2013, 2013.
60. J. Assange. No hay elección, tenemos que pasarnos al software libre para nuestra mejor protección. <http://www.telam.com.ar/notas/201409/79058-julian-assan-software-libre-ciberseguridad-espionaje.html>, 2014.
61. B. Liddell. *La Estrategia de Aproximación Indirecta*. Atalaya: Iberia-Joaquín Gil, Editores, S.A., 1946.

## Apéndices

## APÉNDICE A

# CERTIFICADO ELECTRÓNICO X.509 VERSIÓN 3 EN TEXTO PLANO

---

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 5357 (0x14ed)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=VE, ST=Miranda, L=Baruta, O=Sistema Nacional
    de Certificacion Electronica, OU=Fundacion Instituto de
    Ingenieria, CN=PSC Publico del MppCTII para el Estado
    Venezolano/emailAddress=admin-pki@fii.gob.ve
    Validity
      Not Before: Apr  2 10:40:23 2012 GMT
      Not After : Apr  2 10:40:23 2013 GMT
    Subject: C=VE, O=Sistema Nacional de Certificacion
    Electronica, OU=FIISHA256, ST=Merida, L=Alberto Adriani,
    CN=Antonio Araujo Brett/emailAddress=aaraujo@cenditel.gob.ve
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:db:f4:30:58:bc:ce:30:50:9e:44:14:57:d6:eb:
        e9:cd:f6:90:a7:21:ec:bl:0e:73:af:0d:e7:05:1e:
        cd:a6:3b:1e:85:1a:86:1b:12:69:f9:28:28:4c:a0:
        1c:92:09:81:e0:a9:09:40:08:9e:60:89:12:c9:7b:
        96:f3:fd:99:49:52:5f:98:11:41:31:70:60:ca:55:
        de:73:4d:d8:05:c2:ac:d6:1c:9b:9a:2c:74:66:f3:
        e5:fa:ad:48:fc:7d:06:11:72:ed:bc:a4:35:cd:7e:
        50:69:eb:9d:75:01:06:a7:48:e7:58:40:11:0e:41:
        fa:50:03:4f:03:45:67:0d:c7:9a:25:c9:e3:32:86:
        99:64:18:31:d0:19:7d:45:ef:e4:f9:ec:46:12:65:
        7c:61:de:40:2c:c2:4d:2e:ab:dc:27:f2:7b:38:7b:
        81:47:20:ce:4f:6b:3b:a4:be:5b:7a:ef:f7:23:07:
        70:08:c6:6e:7b:4d:a9:6e:a3:c0:5b:0a:09:0d:72:
```

```

ab:1e:cd:a7:f5:28:b4:4f:01:44:63:38:53:96:43:
1e:8d:a8:9c:13:a2:84:30:44:41:a4:56:7c:7d:58:
04:a7:58:a8:46:21:a7:16:64:fb:49:c7:0a:bc:7e:
3a:3d:6a:df:ee:d7:0d:38:00:26:76:44:39:81:20:
b2:7d
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
X509v3 Key Usage:
Digital Signature, Non Repudiation, Key Encipherment
X509v3 Extended Key Usage:
TLS Web Client Authentication, E-mail Protection,
Microsoft Smartcardlogin
X509v3 Subject Key Identifier:
E0:A4:9A:D5:A9:0F:EA:6B:CF:A1:1B:28:74:AD:8E:2A:AE:FD:88:C5
X509v3 Authority Key Identifier:
keyid:AA:94:98:5B:01:C8:17:18:50:28:B5:F6:E1:5F:FB:FC:89:5E:69:AE
DirName:/CN=Autoridad de Certificacion Raiz del
Estado Venezolano/C=VE/L=Caracas/ST=Distrito
Capital/O=Sistema Nacional de Certificacion
Electronica/OU=Superintendencia de Servicios de
Certificacion Electronica/emailAddress=acraiz@suscerte.gob.ve
serial:0D

Authority Information Access:
OCSP - URI:http://publicador-psc.fii.gob.ve:2560/ocsp

X509v3 Certificate Policies:
Policy: 2.16.862.2.6
Policy: 2.16.862.2.7.1
CPS: http://publicador-psc.fii.gob.ve/dpc
CPS: http://publicador-psc.fii.gob.ve/pc

X509v3 Subject Alternative Name:
othername:<unsupported>, othername:<unsupported>,
othername:<unsupported>, othername:<unsupported>
X509v3 Issuer Alternative Name:
DNS:fii.gob.ve, othername:<unsupported>
X509v3 CRL Distribution Points:

Full Name:
URI:https://publicador-psc.fii.gob.ve/crlsha256/cacrl.crl

Signature Algorithm: sha256WithRSAEncryption
22:ca:a7:de:b7:30:27:b6:aa:95:67:c1:68:0a:5b:db:a6:a8:
b5:ee:0b:b4:14:42:39:b7:d8:c5:13:7a:5b:7d:2d:66:49:54:
0d:bc:e4:8a:25:b4:c8:af:87:60:9a:b4:22:a5:92:66:b6:4e:
16:66:26:1d:06:76:1f:2b:af:e1:b0:7f:3f:4c:71:cd:75:99:
66:14:84:01:da:40:18:40:8e:b3:0e:f8:4a:b6:b0:15:53:ef:
40:28:69:1e:e9:dd:30:7d:80:22:c3:84:5f:16:d7:12:cf:a6:
57:67:64:82:9d:b9:9c:43:e3:2b:d2:ed:bd:72:9e:6f:a4:f0:
5b:6d:16:63:d1:9c:0e:68:eb:dd:45:db:57:7c:95:09:a0:53:
d6:08:6b:ea:ae:95:24:8a:d1:eb:c7:99:46:f3:17:93:84:6c:
6b:6b:06:97:3a:77:89:a6:ba:ff:3f:5b:aa:21:d8:55:11:25:
ba:a7:65:a5:8e:9f:7d:f3:f2:7f:14:6a:af:eb:b0:7e:36:31:
93:56:f9:0f:19:2f:27:ed:e7:0d:e4:b2:4f:05:f5:26:ad:76:
c6:b2:b0:0e:4e:9b:e6:7f:5e:65:74:8d:9e:54:4c:6e:4b:aa:
f1:de:85:86:a0:34:bc:bb:5b:7f:a9:1e:cf:ea:6b:a6:e0:66:
3a:e2:48:2d:9e:ae:88:7c:69:da:26:26:bb:37:41:56:9a:5b:
98:78:f6:d2:52:3c:28:9f:dc:5f:01:97:d7:d5:13:b6:00:31:
07:d1:b4:3d:46:49:2c:68:02:4d:b7:fc:ef:b6:0e:7c:b8:19:
4a:91:23:11:38:ea:f2:8a:8a:31:b4:1a:b6:34:ab:c3:d0:3a:
4d:7f:67:ae:ae:04:e1:5e:f4:21:ee:63:83:4e:85:f0:87:13:
9f:5b:f6:77:bc:90:c2:b7:a3:93:d9:75:d6:70:91:b0:94:4b:
7f:2d:d7:d3:e6:ef:31:d8:de:54:62:fe:69:c5:10:95:8f:43:
d6:ce:cf:a9:80:03:9a:87:81:c9:7e:0d:bd:85:2d:3b:11:57:
7b:e1:88:28:b9:3c:ce:55:70:b0:11:59:34:2c:eb:51:de:15:
24:42:2e:1a:e5:0a:30:6d:39:93:54:2d:f3:7b:5e:c6:a9:ca:
b3:3d:13:56:d9:1b:bc:27:31:45:88:3d:e9:b3:40:d2:0e:1b:
c1:3c:5e:4c:da:c6:bb:a3:4f:85:6a:8b:f0:b5:06:e7:2b:31:
68:be:c4:6f:cf:a5:c9:75:79:98:b7:e4:6e:c9:34:b5:a7:c9:
2a:6b:a6:f3:ef:f4:ba:c9:1e:b7:7f:cf:e9:8f:9e:ce:67:fb:
c9:a9:f0:91:c3:33:95:00

```