



# **GUÍA/NORMA DE SEGURIDAD DE LAS TIC (CCN-STIC-400)**

## **MANUAL STIC**

**MAYO 2013**

Edita:



© Centro Criptológico Nacional, 2013

NIPO 002-13-032-6

Fecha de Edición: mayo de 2013

S2 Grupo ha participado en la elaboración y modificación del presente documento y sus anexos.

#### **LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

#### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

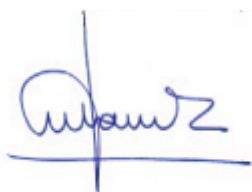
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Mayo de 2013



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

## ÍNDICE

I. INTRODUCCIÓN .....	9
1. ORIENTACIONES DE SEGURIDAD .....	10
1.1. INTRODUCCIÓN.....	10
1.2. MODELO CONCEPTUAL DE LA SEGURIDAD.....	10
1.2.1. SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (STIC).....	13
1.2.2. AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS.....	15
1.2.3. EL FACTOR HUMANO.....	15
1.3. MEDIDAS DE PROTECCIÓN .....	16
1.4. LA ESTRATEGIA DE SEGURIDAD.....	17
II. CIFRADO DE DATOS .....	19
2. INTRODUCCIÓN A LA CRIPTOLOGÍA .....	20
2.1. INTRODUCCIÓN.....	20
2.2. SEGURIDAD CRIPTOGRÁFICA .....	21
2.3. DEFINICIÓN DE CRIPTOSISTEMA .....	22
2.3.1. PRINCIPIOS DE LOS CRIPTOSISTEMAS DE CLAVE SECRETA.....	23
2.3.2. PRINCIPIOS DE LOS CRIPTOSISTEMAS DE CLAVE PÚBLICA .....	24
2.4. TEORÍA DE NÚMEROS .....	25
2.4.1. NÚMEROS PRIMOS.....	25
2.4.2. ARITMÉTICA MODULAR .....	25
2.4.3. EXPONENCIACIÓN Y LOGARITMO DISCRETO .....	26
2.5. TEORÍA DEL SECRETO PERFECTO.....	26
2.5.1. TEORÍA DE LA CONFIDENCIALIDAD PERFECTA .....	27
2.5.2. AUTENTICIDAD PERFECTA EN UN CRIPTOSISTEMA.....	27
2.5.3. ATAQUE DE SUSTITUCIÓN EN UN SISTEMA DE CLAVE PÚBLICA .....	28
2.5.4. IMPLEMENTACIÓN PRÁCTICA DEL SECRETO PERFECTO .....	28
2.6. FUNCIONES RESUMEN .....	29
2.7. CRITERIOS DE DISEÑO DE UN CRIPTOSISTEMA .....	30
2.7.1. ATAQUES A UN CRIPTOSISTEMA.....	30
2.8. ESTEGANOGRAFÍA .....	32
3. CRIPTOSISTEMAS Y MODO DE EMPLEO DE LA CIFRA .....	33
3.1. CLASIFICACIÓN DE LOS CRIPTOSISTEMAS .....	33
3.1.1. INTRODUCCIÓN.....	33
3.1.2. CIFRADO SIMÉTRICO .....	33
3.1.3. CIFRADO ASIMÉTRICO .....	33
3.1.4. CIFRADO EN BLOQUE .....	34
3.1.5. CIFRADO EN SERIE .....	35
3.1.6. SISTEMAS HÍBRIDOS .....	35
3.1.7. COMPONENTES DE UN CRIPTOSISTEMA MODERNO .....	36
3.2. MODOS DE EMPLEO DE LA CIFRA.....	36
3.2.1. CIFRADO LOCAL DE LA INFORMACIÓN .....	36
3.2.2. CIRCUITO CERRADO DE INFORMACIÓN.....	37
3.2.3. CIFRADO DE COMUNICACIONES .....	38
3.2.3.1. COMUNICACIÓN PUNTO A PUNTO .....	39
3.2.3.2. RED EN ESTRELLA CENTRALIZADO .....	39
3.2.3.3. RED COMPLETA DE ENLACE.....	40

3.2.4.	GESTIÓN DE CLAVES .....	40
3.2.4.1.	GENERACIÓN DE CLAVES .....	41
3.2.4.2.	CLAVES ALEATORIAS.....	41
3.2.4.3.	DISTRIBUCIÓN DE CLAVES .....	42
3.2.4.4.	ALMACENAMIENTO Y DESTRUCCIÓN DE CLAVES .....	42
3.2.4.5.	TIPOS DE CLAVES .....	42
3.2.4.6.	PERÍODO DE VIGENCIA DE LAS CLAVES .....	43
3.2.4.7.	OTRAS CONSIDERACIONES FINALES.....	44
4.	INTRODUCCIÓN A LA CRIPTOFONÍA.....	45
4.1.	GENERALIDADES.....	45
4.2.	CRIPTOFONOS ANALÓGICOS Y DIGITALES.....	46
4.2.1.	CONSIDERACIONES GENERALES.....	46
4.2.2.	TIPOS DE CRIPTOFONOS SEGÚN CANAL DE TRANSMISIÓN.....	47
4.2.3.	DIAGRAMA DE BLOQUES DE CIFRADORES ANALÓGICOS Y DIGITALES .....	47
4.3.	BREVE RESEÑA HISTÓRICA DE LA CRIPTOFONÍA.....	49
III.	POLÍTICA Y ORGANIZACIÓN .....	52
5.	POLÍTICA DE SEGURIDAD .....	53
5.1.	POLÍTICAS DE SEGURIDAD .....	53
5.1.1.	POLÍTICA GENERAL O CORPORATIVA .....	54
5.1.2.	POLÍTICAS SOBRE ASPECTOS DE SEGURIDAD.....	54
5.1.3.	POLÍTICAS ESPECÍFICAS .....	54
5.2.	SEGURIDAD DE LOS SISTEMAS.....	54
5.3.	MODOS SEGUROS DE OPERACIÓN .....	55
5.4.	LA PROBLEMÁTICA DE SEGURIDAD .....	56
5.5.	PLANIFICACIÓN DE LA SEGURIDAD.....	57
5.5.1.	SERVICIOS DE SEGURIDAD .....	58
5.5.2.	MECANISMOS DE IMPLEMENTACIÓN .....	58
5.6.	DESARROLLO NORMATIVO .....	60
6.	ORGANIZACIÓN Y GESTIÓN DE SEGURIDAD.....	61
6.1.	INTRODUCCIÓN.....	61
6.2.	ORGANIZACIÓN DE SEGURIDAD .....	61
6.3.	ESTRUCTURA TIC DEL SISTEMA .....	61
6.3.1.	COMITÉ TIC.....	62
6.3.2.	ADMINISTRADORES STIC .....	63
6.3.3.	OPERADORES .....	63
6.3.4.	USUARIOS .....	64
6.4.	ESTRUCTURA STIC DE LA ORGANIZACIÓN.....	65
6.4.1.	ALTA DIRECCIÓN .....	67
6.4.2.	COMITÉ DE SEGURIDAD CORPORATIVA .....	67
6.4.3.	RESPONSABLE DE SEGURIDAD CORPORATIVA .....	68
6.4.4.	COMITÉ STIC .....	68
6.4.5.	RESPONSABLE STIC.....	69
6.4.6.	RESPONSABLES STIC DELEGADOS .....	70
6.5.	ANÁLISIS DE RIESGOS.....	71
6.6.	SEGURIDAD DE LA INFORMACIÓN .....	73
6.7.	DOCUMENTACIÓN DE SEGURIDAD .....	74
6.8.	PROYECTOS.....	74
7.	INSPECCIÓN DE SEGURIDAD DE LAS TIC .....	76
7.1.	INTRODUCCIÓN.....	76
7.2.	INSPECCIONES DE SEGURIDAD .....	76

7.2.1.	ACTIVIDADES A DESARROLLAR .....	77
7.2.2.	TIPOS DE INSPECCIÓN .....	78
7.2.3.	RESPONSABILIDADES .....	79
7.3.	PROCESO DE INSPECCIÓN .....	80
7.3.1.	MEDIOS NECESARIOS .....	81
7.3.2.	REQUISITOS INICIALES .....	81
7.3.3.	ESTIMACIÓN DE TIEMPO .....	82
7.3.4.	INFORME DE RESULTADOS .....	83
7.3.5.	REUNIÓN EN GRUPO .....	84
7.4.	LISTA DE COMPROBACIÓN .....	85
7.5.	HERRAMIENTAS DE SEGURIDAD .....	85
7.6.	PERIODICIDAD.....	86
7.7.	CONCLUSIONES.....	87
8.	ACREDITACIÓN DE SISTEMAS .....	88
8.1.	INTRODUCCIÓN.....	88
8.2.	CONDICIONES PARA LA ACREDITACIÓN.....	88
8.2.1.	DOCUMENTACIÓN DE SEGURIDAD .....	88
8.2.2.	SEGURIDAD DEL PERSONAL.....	89
8.2.3.	SEGURIDAD FÍSICA .....	89
8.2.4.	SEGURIDAD DOCUMENTAL .....	89
8.2.5.	SEGURIDAD DE EMANACIONES.....	89
8.2.6.	SEGURIDAD CRIPTOLÓGICA.....	90
8.2.7.	SEGURIDAD DE LAS TIC (STIC).....	90
8.3.	PROCESO DE ACREDITACIÓN.....	90
8.4.	INTERCONEXIÓN DE SISTEMAS ACREDITADOS .....	92
8.5.	SITUACIONES POSIBLES DE LA ACREDITACIÓN.....	93
8.6.	INSPECCIONES.....	94
8.7.	VALIDEZ DE LA ACREDITACIÓN .....	94
8.7.1.	REACREDITACIÓN .....	94
8.7.2.	INFORMES A REMITIR EN EL PERÍODO ENTRE ACREDITACIONES.....	94
8.7.3.	REGISTRO DE SISTEMAS ACREDITADOS.....	95
9.	GESTIÓN DE INCIDENTES DE SEGURIDAD .....	96
9.1.	INTRODUCCIÓN.....	96
9.2.	DEFINICIONES .....	97
9.3.	GESTIÓN DE INCIDENTES DE SEGURIDAD.....	98
9.3.1.	DETECCIÓN DEL INCIDENTE .....	99
9.3.2.	NOTIFICACIÓN DEL INCIDENTE.....	99
9.3.3.	RESPUESTA AL INCIDENTE .....	100
9.3.4.	PERIODO POSTERIOR .....	101
9.4.	INCIDENTES EN SISTEMAS QUE MANEJAN INFORMACIÓN CLASIFICADA.....	102
9.5.	ACTORES Y RESPONSABILIDADES .....	102
9.5.1.	ACTORES INTERNOS .....	103
9.5.1.1.	Dirección corporativa .....	103
9.5.1.2.	Departamento de Seguridad.....	103
9.5.1.3.	Departamentos TI .....	103
9.5.1.4.	Departamento Jurídico.....	103
9.5.1.5.	Recursos Humanos .....	104
9.5.1.6.	Comunicación.....	104
9.5.2.	ACTORES EXTERNOS .....	104
9.5.2.1.	FFCCSE.....	104
9.5.2.2.	CERT/CSIRT .....	104

9.5.2.3. Fabricantes/proveedores .....	105
IV. SEGURIDAD LÓGICA.....	106
10. SOFTWARE MALICIOSO .....	107
10.1. INTRODUCCIÓN.....	107
10.2. CÓDIGO MALICIOSO O MALWARE.....	108
10.2.1. VIRUS .....	108
10.2.2. CABALLOS DE TROYA .....	109
10.2.3. GUSANOS .....	110
10.2.4. BOMBAS LÓGICAS .....	111
10.2.5. CÓDIGO MÓVIL MALICIOSO .....	111
10.2.6. PUERTAS TRASERAS .....	112
10.2.7. HOAXES .....	112
10.2.8. PHISHING.....	113
10.2.9. ROGUE SOFTWARE .....	114
10.2.10. ADWARE.....	114
10.2.11. OTRO SOFTWARE MALICIOSO.....	115
10.3. SALVAGUARDAS .....	116
10.3.1. ESTRATEGIAS DE PREVENCIÓN.....	116
10.3.2. ESTRATEGIAS DE RESPUESTA.....	118
10.3.3. ESTRATEGIAS DE RECUPERACIÓN .....	118
11. PROTOCOLOS DE RED .....	120
11.1. INTRODUCCIÓN.....	120
11.2. MODELOS OSI Y TCP/IP .....	120
11.3. PROTOCOLOS MÁS COMUNES.....	123
11.3.1. CAPA DE ENLACE DE DATOS.....	123
11.3.1.1. PROTOCOLO ARP .....	123
11.3.1.2. PROTOCOLO RARP.....	123
11.3.1.3. PROTOCOLO PPP.....	124
11.3.1.4. PROTOCOLO L2TP .....	124
11.3.1.5. PROTOCOLO STP .....	124
11.3.2. CAPA DE RED .....	124
11.3.2.1. PROTOCOLO IP V4.....	124
11.3.2.2. Protocolo IP V6 .....	125
11.3.2.3. PROTOCOLO ICMP .....	126
11.3.2.4. PROTOCOLO IGMP .....	126
11.3.2.5. FRAMEWORK IPSEC .....	127
11.3.2.6. PROTOCOLOS DE ENRUTAMIENTO .....	127
11.3.3. CAPA DE TRANSPORTE.....	127
11.3.3.1. PROTOCOLO TCP.....	128
11.3.3.2. PROTOCOLO UDP .....	128
11.3.4. CAPA DE APLICACIÓN .....	129
11.3.4.1. PROTOCOLO SMTP.....	129
11.3.4.2. PROTOCOLO POP .....	129
11.3.4.3. PROTOCOLO IMAP .....	129
11.3.4.4. PROTOCOLO FTP .....	129
11.3.4.5. PROTOCOLO DNS .....	129
11.3.4.6. PROTOCOLO HTTP .....	130
11.3.4.7. PROTOCOLO HTTPS .....	130
11.3.4.8. PROTOCOLO SNMP .....	130
11.3.4.9. PROTOCOLO SIP .....	130
11.3.4.10. PROTOCOLO NTP.....	130
11.3.4.11. PROTOCOLO DHCP.....	131
12. SEGURIDAD PERIMETRAL .....	132

12.1. INTRODUCCIÓN.....	132
12.1.1. IDENTIFICACIÓN DE AMENAZAS .....	132
12.1.2. EVOLUCIÓN .....	133
12.1.3. PUNTOS DÉBILES .....	134
12.2. COMPONENTES DE LA SEGURIDAD PERIMETRAL.....	135
12.2.1. ENRUTADORES Y REGLAS DE FILTRADO .....	135
12.2.2. CORTAFUEGOS .....	138
12.2.3. SISTEMAS VPN.....	139
12.2.4. DISPOSITIVOS DE RED .....	140
12.2.5. SERVIDORES.....	141
12.2.6. SISTEMAS DE USUARIO Y SISTEMAS MÓVILES.....	141
12.2.7. TECNOLOGÍAS INALÁMBRICAS.....	142
13. DETECCIÓN DE INTRUSOS .....	144
13.1. INTRODUCCIÓN.....	144
13.2. CLASIFICACIÓN DE LOS IDS .....	144
13.3. SISTEMAS Y REDES TRAMPA .....	145
13.4. IMPLANTACIÓN EN LA ORGANIZACIÓN .....	146
13.5. AMPLIACIÓN DEL ESQUEMA.....	147
13.6. SISTEMAS DE PREVENCIÓN DE INTRUSIONES .....	148
13.7. ATAQUES .....	148
14. SEGURIDAD EN REDES INALÁMBRICAS .....	150
14.1. INTRODUCCIÓN.....	150
14.2. ESPECTRO ELECTROMAGNÉTICO .....	150
14.3. REDES IEEE 802.11 (WIFI) .....	152
14.3.1. PROPIEDADES DEL ESPECTRO ELECTROMAGNÉTICO .....	152
14.3.2. GRUPOS DE TRABAJO PARA LA NORMA IEEE 802.11.....	153
14.3.3. DISPOSITIVOS .....	154
14.3.4. FUNCIONAMIENTO .....	155
14.3.5. TOPOLOGÍAS DE RED.....	156
14.3.6. AMENAZAS Y RIESGOS PARA ESTÁNDAR 802.11 .....	157
14.3.7. ELEMENTOS DE SEGURIDAD .....	157
14.3.7.1. WEP.....	158
14.3.7.2. WEP DINÁMICO .....	160
14.3.7.3. WPA - 802.11i (WPA2) .....	161
14.3.8. INFRAESTRUCTURA RECOMENDADA.....	162
14.3.8.1. MEDIDAS PROCEDIMENTALES.....	162
14.3.8.2. MEDIDAS TÉCNICAS .....	163
14.3.8.3. CONFIGURACIÓN GENERAL DE LOS PUNTOS DE ACCESO .....	164
14.3.8.4. ESCENARIO ESPECIAL DE DESPLIEGUE: RED WIFI DE CORTESIA.....	166
14.4. BLUETOOTH.....	166
14.4.1. PROPIEDADES DEL ESPECTRO ELECTROMAGNETICO .....	167
14.4.2. ESPECIFICACIONES BLUETOOTH .....	168
14.4.3. DISPOSITIVOS .....	168
14.4.4. TOPOLOGIA DE RED .....	169
14.4.5. ELEMENTOS DE SEGURIDAD .....	170
14.4.6. AMENAZAS Y RIESGOS .....	171
14.4.7. INFRAESTRUCTURA RECOMENDADA.....	173
14.4.7.1. MEDIDAS PROCEDIMENTALES.....	173
14.4.7.2. MEDIDAS TÉCNICAS .....	174
15. HERRAMIENTAS DE SEGURIDAD .....	175
15.1. INTRODUCCIÓN.....	175



15.2. CLASIFICACIÓN DE HERRAMIENTAS DE SEGURIDAD .....	175
15.2.1. ANTIFRAUDE.....	177
15.2.2. ANTIMALWARE .....	177
15.2.3. AUDITORÍA TÉCNICA Y FORENSE .....	178
15.2.4. IDENTIFICACIÓN Y AUTENTICACIÓN.....	179
15.2.5. CONTINGENCIA Y CONTINUIDAD .....	180
15.2.6. CONTROL DE CONTENIDOS .....	180
15.2.7. CONTROL Y MONITORIZACIÓN DE TRÁFICO .....	181
15.2.8. CUMPLIMIENTO LEGAL Y NORMATIVO .....	181
15.2.9. GESTIÓN DE EVENTOS.....	182
15.2.10. HERRAMIENTAS DE CIFRA.....	182
15.3. SELECCIÓN, CONTROL DE LA CONFIGURACIÓN Y USO .....	183
15.3.1. SELECCIÓN .....	183
15.3.2. CONTROL DE LA CONFIGURACIÓN.....	184
15.3.3. USO OPERATIVO.....	184
15.4. RESPONSABILIDADES .....	185
15.4.1. PLANEAMIENTO Y ADQUISICIÓN .....	185
15.4.2. AUTORIDAD RESPONSABLE DEL SISTEMA.....	185
15.4.3. RESPONSABLES DE SEGURIDAD DEL SISTEMA.....	185
V. ANEXOS .....	187
ANEXO A. REFERENCIAS.....	188
ANEXO B. ACRÓNIMOS .....	190

# I. INTRODUCCIÓN

## 1. ORIENTACIONES DE SEGURIDAD

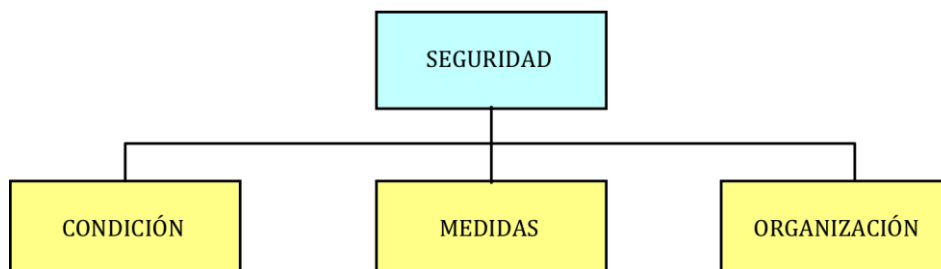
### 1.1. INTRODUCCIÓN

1. Se denomina **activo** a todo aquello que una Organización necesita proteger, desde las personas a las infraestructuras o la información corporativa. Hace años, antes de que los sistemas de información se convirtieran en algo básico para el funcionamiento correcto de cualquier Organización, los principales activos de una Organización solían ser los objetos físicos (maquinaria, mobiliario...), las infraestructuras, la tesorería o las personas. Pero en los últimos tiempos a estos activos –que siguen siendo importantes– se ha añadido uno que en ocasiones es el más crítico por detrás de las personas: la información de la Organización.
2. Por supuesto, la información existe desde que existe la humanidad y el interés por protegerla siempre ha sido alto (como ejemplo, los métodos criptográficos clásicos), pero hoy en día, con el uso masivo de las nuevas tecnologías y la dependencia de éstas, el riesgo es mayor, ya que lo son la probabilidad de materialización de una amenaza y el impacto asociado a la misma. Así, si hace cincuenta años robar una gran cantidad de datos requería un acceso físico a un entorno controlado y la capacidad para robar o copiar una cantidad considerable de documentos, hoy en día ese mismo ataque puede realizarse mediante un sencillo *pendrive* que albergue en su interior gigas y gigas de información sensible. Mucho más sencillo para el atacante –y por tanto más probable– y, desde luego, con un impacto mayor para la Organización.
3. Así, parece claro que en la actualidad, la información es un activo más de cualquier Organización y, en muchos casos, debe considerarse el más valioso de ésta (por detrás, claro está, de las personas). Si a eso se añade la imparable marcha hacia la conectividad permanente gracias a la disponibilidad cada día más generalizada de las nuevas tecnologías, parece evidente que hay que preocuparse por la seguridad de la información. Conforme aumenta la interconexión lo hacen también los riesgos para la información, hasta el punto que en ocasiones la responsabilidad de la protección pasa a recaer en el propio usuario de los datos.
4. No obstante, a pesar de la importancia demostrada de la seguridad, en contra de lo que pudiera pensarse, las pérdidas asociadas a fallos de seguridad continúan creciendo y las causas en un alto porcentaje de los casos están vinculadas a problemas internos de la Organización, en especial al uso que las personas hacen de los datos. Por tanto, el objetivo de la seguridad de la información será proteger adecuadamente la información de una Organización y los sistemas que la tratan, garantizando en la medida de lo posible tres características básicas que se describirán más adelante en esta misma guía: confidencialidad, integridad y disponibilidad.

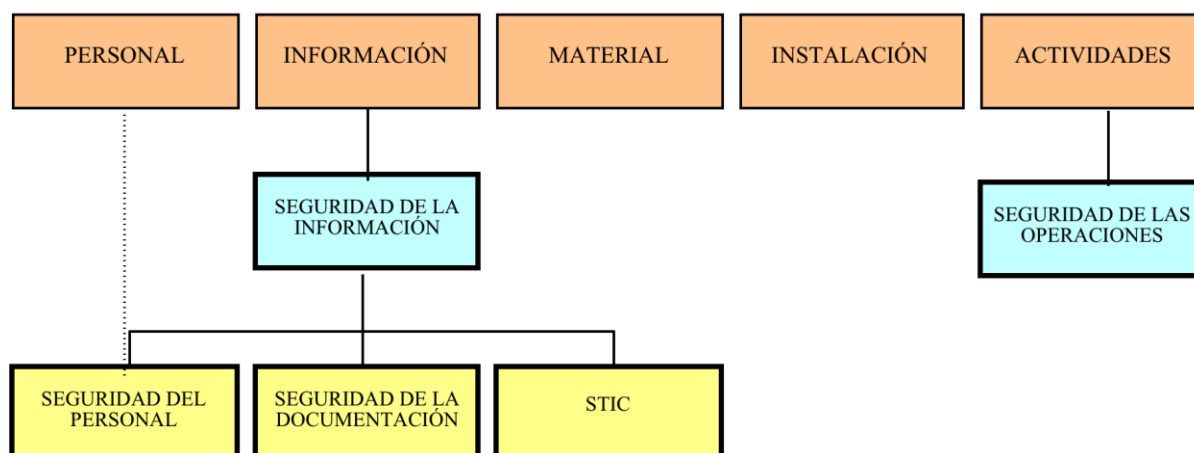
### 1.2. MODELO CONCEPTUAL DE LA SEGURIDAD

5. Al hablar de “seguridad” se aceptan, de forma genérica, tres grandes significados del término:

- a. Seguridad como **condición** alcanzada por un activo (Organización, sistema, persona...) cuando es protegido de forma adecuada.
- b. Seguridad como conjunto de **medidas** de protección.
- c. Seguridad como **organización** responsable de proporcionar esta condición.

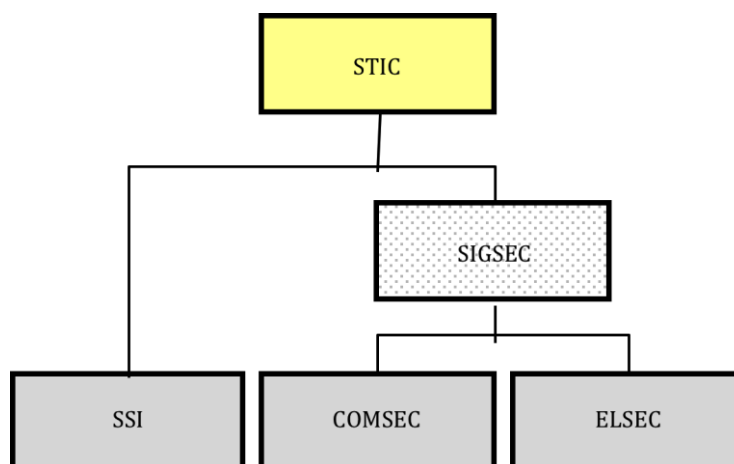


6. También es generalmente aceptado que el objetivo de la seguridad es proteger los activos (personal, información, material, instalaciones) y las actividades. Por tanto, según el tipo de activo a proteger, se utilizan los términos de seguridad del personal, seguridad de la información, seguridad del material, seguridad de las instalaciones o seguridad de las operaciones. En concreto, cuando se trata de proteger la información, ésta puede existir en las personas, físicamente en un documento o en forma electromagnética en un sistema y, por lo tanto, se utilizan los términos de seguridad del personal, seguridad de la documentación o, para el soporte electromagnético y tratamiento automatizado, Seguridad de las Tecnologías de la Información y Comunicaciones (STIC).



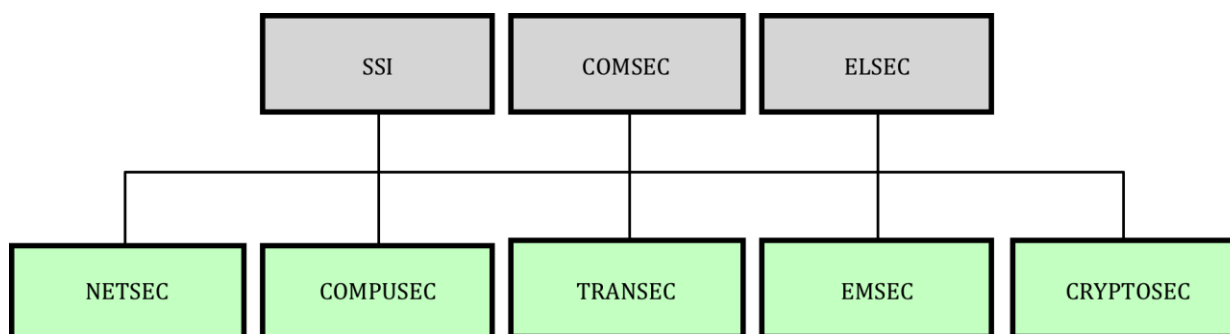
7. Como se ve en el gráfico anterior, el término relativo a seguridad del personal tiene dos acepciones:
  - a. Protección de las personas (su integridad, en especial la física).
  - b. Protección de la información que conocen las personas mediante medidas de seguridad aplicadas sobre ellas (habilitaciones, necesidad de conocer, concienciación, etc.).
8. De esta forma, el término STIC hace referencia a la protección de la información en los sistemas de información, en los sistemas de comunicaciones y en los sistemas electrónicos (como por ejemplo sensores, equipos de medida, etc.) de

manera que se asegure o garantice su confidencialidad, integridad y disponibilidad. Dependiendo del sistema donde se encuentre la información también se utilizan los términos de Seguridad de los Sistemas de Información (SSI), Seguridad de los Sistemas de Comunicaciones (COMSEC) y Seguridad Electrónica (ELSEC). Este último término se aplica a todos aquellos Sistemas que no son de comunicaciones tales como sensores, sistemas de identificación, sistemas de navegación, etc. Debido a la similitud existente con la terminología de inteligencia que agrupa en el término Inteligencia de Señales (SIGINT), a los términos de Inteligencia de Comunicaciones (COMINT) e Inteligencia Electrónica (ELINT), también en STIC algunos autores agrupan los términos COMSEC y ELSEC en otro denominado SIGSEC (Seguridad de las Señales):



9. Según la definición del término STIC, la seguridad de la información y de los sistemas que la tratan puede conseguirse protegiendo cada uno de los recursos que componen la configuración de dichos sistemas. De este modo, las medidas de seguridad, en función del objeto de protección en cada caso, pueden clasificarse en:
  - a. TRANSEC. Medidas que aseguran los canales de transmisión (Seguridad de las Transmisiones).
  - b. COMPUSEC. Medidas que protegen el proceso automático de datos (Seguridad de los Ordenadores).
  - c. EMSEC. Medidas que protegen a los equipos frente a la emisión de radiaciones no deseadas (Seguridad de las Emisiones).
  - d. NETSEC. Medidas que protegen los elementos de red (Seguridad de las Redes).
  - e. CRYPTOSEC. Medidas que aseguran que la información está protegida mediante procedimientos criptográficos adecuados (Seguridad Criptológica).
10. Conviene señalar que el término NETSEC está relacionado con la protección de las redes contra la modificación, destrucción o revelación de la información mientras circula por ellas, diferenciándose así del término TRANSEC, vinculado

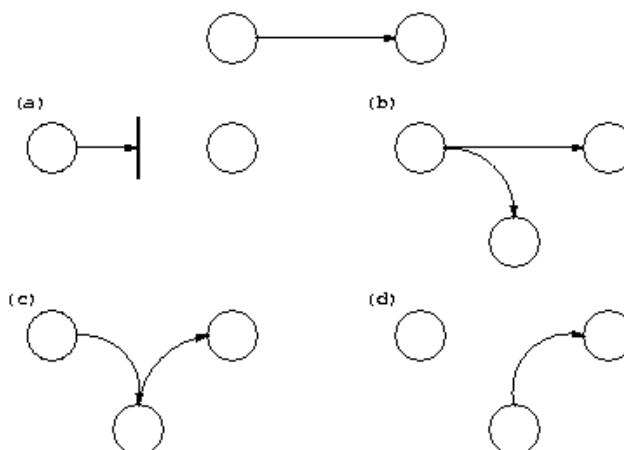
este último con la prevención contra la obtención de información por medio de la interceptación, radiolocalización y análisis de las señales electromagnéticas.



### 1.2.1. SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (STIC)

11. El concepto de seguridad de las TIC es mucho más amplio que la simple protección de los datos desde un punto de vista lógico, interviniendo factores tecnológicos pero también aspectos como la protección física, las salvaguardas organizativas o el cumplimiento normativo y teniendo en cuenta múltiples condicionantes, tanto internos como externos a una Organización. Así, la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) hace referencia al conjunto de medidas de seguridad para proteger la información almacenada, procesada o transmitida por sistemas de información y telecomunicaciones, de manera que se preserve la **confidencialidad**, **integridad** y **disponibilidad** de la información y la integridad y la disponibilidad de los elementos que la tratan.
12. Por tanto, los objetivos de la STIC se concretan en el mantenimiento de las características enumeradas previamente:
  - a. Confidencialidad: la información ha de ser accedida únicamente por actores autorizados y éstos no van a convertirla en disponibles para otros actores.
  - b. Integridad: la información sólo puede ser modificada por actores autorizados y de una manera controlada. La integridad garantiza la exactitud de la información contra la alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
  - c. Disponibilidad: la información tiene que permanecer accesibles para los actores autorizados cuándo y cómo éstos requieran.
13. En base a lo anterior, la taxonomía más básica de amenazas que afectan a estas características es la siguiente:
  - a. Interrupción (disponibilidad): Amenazas que motivan la pérdida, inutilización o no disponibilidad de la información.
  - b. Interceptación (confidencialidad): Amenazas que motivan el acceso de un actor no autorizado a la información.

- c. Modificación (integridad): Amenazas que motivan la alteración no autorizada de la información; un caso especial es la destrucción, entendida como modificación que inutiliza la información.
  - d. Fabricación: Amenazas que tratan de generar información similar de forma que sea difícil distinguir entre la versión original y la fabricada.
14. Gráficamente se pueden ver estas amenazas en la siguiente figura, en la que se representa el flujo original de información entre actores (emisor-receptor) y las amenazas de interrupción (a), interceptación (b), modificación (c) y fabricación (d).



15. La protección de la información es un reto cada vez más complejo debido entre otros factores a la conectividad permanente a redes públicas, como Internet, que quedan fuera del control de la Organización, a la movilidad requerida por el personal de la Organización o al riesgo de que un tercero realice ataques remotos contra los datos. La seguridad absoluta, con una probabilidad del 100 %, no existe, siendo imposible de alcanzar debido al obligatorio compromiso entre el nivel de seguridad, los recursos disponibles y la funcionalidad deseada. La seguridad es proporcional al coste de las medidas de protección y, por tanto, se opone a los sistemas abiertos, sin ningún tipo de protección, que pretenden facilitar el acceso a cualquier usuario.
16. En definitiva, la implementación de seguridad es un problema de ingeniería, un compromiso entre costes, funcionalidad y protección. Para implementar seguridad en una Organización de forma adecuada se deben planificar y tener en cuenta los aspectos siguientes:
- a. Análisis de Riesgos: estudio de los riesgos existentes y valoración de las consecuencias de los mismos sobre los activos de información.
  - b. Gestión de Riesgos: valoración de los diferentes controles (elementos que reducen el riesgo) y decisión sobre los más adecuados en cada caso. Esto permite determinar el riesgo residual.
  - c. Política de Seguridad: adaptación de la operativa habitual de la Organización a las medidas de seguridad requeridas.
  - d. Mantenimiento: control continuo de la eficiencia de las medidas de seguridad desplegadas y adecuación de las mismas a nuevos escenarios de riesgo.

- e. Planes de Contingencia: determinación de las medidas a adoptar ante un incidente de seguridad.

### 1.2.2. AMENAZAS Y VULNERABILIDADES DE LOS SISTEMAS

17. El desarrollo que en la sociedad han alcanzado las tecnologías de la información y comunicaciones durante los últimos años ha sido espectacular. Tal y como se ha indicado, estas tecnologías aportan múltiples beneficios (racionalización de costes, aparición de nuevos servicios y mejora de los existentes, apoyo a la toma de decisiones, etc.), pero a medida que se ha ido alcanzando un mayor grado de utilización de la tecnologías, también ha ido creciendo el grado de dependencia con respecto a las mismas. El uso de estos entornos implica nuevos riesgos, que hay que valorar y gestionar convenientemente y cuya importancia depende de las vulnerabilidades y amenazas a las que se deba hacer frente.
18. En términos generales, se puede definir una **amenaza** como la ocurrencia de uno o más acontecimientos de los que se deriva una situación en la que la información puede sufrir una degradación de su seguridad en cualquiera de sus dimensiones: confidencialidad (acceso, difusión, observación, copiado, robo...), integridad (modificar, sustituir, reordenar, distorsionar...) o disponibilidad (destruir, dañar, contaminar, dejar fuera de servicio...). Las amenazas van desde desastres naturales, tales como inundaciones, accidentes o incendios, hasta abusos deliberados como fraudes, robos o virus, con un origen tanto interno como externo a la Organización.
19. Junto a la definición de amenaza es necesario especificar que una **vulnerabilidad** es una debilidad en la seguridad de un entorno que puede llegar a permitir o facilitar la actuación de una amenaza; las vulnerabilidades pueden ser de naturaleza técnica, procedimental u operacional. Habitualmente, en el ámbito TIC, la vulnerabilidad suele ir asociada a un defecto en el *software* o en la configuración del mismo que puede permitir que se materialice una amenaza.

### 1.2.3. EL FACTOR HUMANO

20. Las personas constituyen el elemento más vulnerable en el marco de la seguridad de las tecnologías de la información y comunicaciones. Voluntaria o involuntariamente, el punto más débil de la seguridad de la información lo constituyen las personas que la tratan: errores, desconocimiento, ataques intencionados... Por este motivo, son las personas un objetivo prioritario en cualquier atacante que quiera acceder de forma no autorizada a la información corporativa.
21. Uno de los ataques más habituales contra la seguridad de la información a través de las personas es sin duda la ingeniería social, consistente en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. Aunque la manipulación en algunos casos no es excesivamente perjudicial, si las intenciones de quien la pone en práctica no son buenas se convierte quizás el método de ataque más sencillo, menos peligroso para el atacante y por desgracia en uno de los más efectivos: raras veces hay que recurrir a un ataque técnico, ya que como se suele decir es más fácil convencer al administrador de la red de que requerimos un acceso a la misma que pasar



días o semanas probando la robustez de esta red, buscando debilidades con la posibilidad de ser detectado por el equipo de seguridad. Un atacante *amateur* se decantaría por atacar directamente al entorno tecnológico, pero un atacante profesional aprovecharía las vulnerabilidades que presentan las personas.

22. No todos los ataques con éxito basados en ingeniería social son debidos a la ingenuidad de los empleados; la mayoría de los casos se debe a la ignorancia de buenas prácticas de seguridad y a la falta de concienciación por parte de los usuarios de la Organización. Hay que considerar que cuanto más sofisticadas sean las tecnologías empleadas para proteger la información, más se van a centrar los ataques en explotar las debilidades de las personas debido a la complejidad de la vía técnica. El usuario de las tecnologías puede constituir un buen aliado para la seguridad, pero para ello necesita ser formado y concienciado. De lo contrario, ese mismo usuario se erigirá como el peor enemigo de la seguridad, debido al desconocimiento de las buenas prácticas habituales.
23. No hay que olvidar que los usuarios son la principal razón para que un sistema de información sea operativo, pero se debe considerar que, como se ha expresado anteriormente, constituyen una amenaza significativa para la seguridad de la Organización. El personal interno es el responsable de buena parte de los problemas de seguridad de la información, tanto que este tipo de atacantes hasta ha recibido un nombre propio: el *insider*.

### 1.3. MEDIDAS DE PROTECCIÓN

24. El hecho de que gran parte de las actividades y servicios sea cada vez más dependientes de las tecnologías de la información y las comunicaciones hace que la seguridad juegue un papel decisivo en cualquier Organización. Por este motivo se debe proteger convenientemente la información y los sistemas que la tratan desde múltiples puntos de vista (técnico, tanto lógico como físico, organizativo y normativo) y en diferentes ámbitos (prevención, detección y respuesta). Se denomina **control** o **salvaguarda** a cualquier medida que reduzca el riesgo de seguridad en la Organización.
25. Los controles técnicos pretenden proteger desde un punto de vista operativo, tanto física como lógicamente, a la información y a los sistemas que la procesan frente a amenazas de cualquier tipo. Las medidas de carácter organizativo se ocupan de dictar controles de índole administrativa y organizativa (asignación de responsabilidades, establecimiento de política de seguridad, política de personal, análisis de riesgos y planes de contingencia) para instrumentar, reforzar o complementar las restantes medidas. Finalmente, las medidas de protección normativa comprenden los aspectos de cumplimiento obligatorio de aplicación en cada caso, en especial desde el punto de vista legal (conjunto de disposiciones legales adoptadas por los poderes legislativo o ejecutivo para proteger, vía sanciones penales o administrativas, la información y los sistemas que la soportan).
26. Aparte de la división anterior, a partir del punto de vista particular de la seguridad en el que un control actúa, los controles se dividen también en tres grandes grupos: de prevención, de detección y de respuesta, en función de en qué punto aportan seguridad de forma principal (muchos controles pueden estar

en varias de estas familias). Los mecanismos de **prevención** son aquellos que aumentan la seguridad de un sistema de información durante el funcionamiento normal de éste, previniendo la ocurrencia de violaciones a la seguridad e incluyendo los correspondientes a **disuasión**. Por mecanismos de **detección** se conoce a aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación y finalmente, los mecanismos de **respuesta** son aquellos que se aplican cuando se ha detectado una violación de la seguridad.

#### 1.4. LA ESTRATEGIA DE SEGURIDAD

27. El diseñar una estrategia de seguridad depende en general de la actividad que se desarrolle en cada Organización; sin embargo, se pueden considerar los siguientes pasos comunes en cualquier caso:
  - a. Crear una política de seguridad.
  - b. Realizar un análisis de riesgos.
  - c. Aplicar las salvaguardas correspondientes.
  - d. Concienciar a los usuarios
28. La **política de seguridad** establece el estado en que se encuentra la información dentro de la Organización y debe contener un objetivo general; adicionalmente debe destacar la importancia de las tecnologías de la información para la Organización, el período de validez de la política, los recursos con que se cuenta y los objetivos específicos a cubrir.
29. Con el **análisis de riesgos** se pretende identificar los problemas a los cuales está expuesta la información a partir de los activos de la Organización, las amenazas que existen sobre los mismos, las probabilidades de que éstas se materialicen y el impacto asociado a la materialización. Es necesario revisar y actualizar periódicamente este análisis de riesgos tomando como base de partida el último realizado y las salvaguardas implementadas hasta la fecha.
30. Una vez que se establece la política de seguridad, determinando el riesgo residual (el existente tras la aplicación de controles) que se está dispuesto a aceptar, se deben establecer las **salvaguardas** que den cumplimiento a la misma y mitiguen los riesgos analizados. La gestión de riesgos utiliza los resultados del análisis de riesgos para seleccionar e implantar los controles adecuados para mitigar los riesgos identificados. Se puede dividir estos controles, tal y como se ha indicado previamente, en:
  - a. Medidas preventivas (su objetivo es reducir el riesgo):
  - b. Protección Física: guardias, control de acceso, protección hardware, etc.
  - c. Medidas Técnicas: cortafuegos, detectores de intrusos, criptografía, etc.
  - d. Medidas Procedimentales: cursos de mentalización, actualización de conocimientos, normas de acceso a la información, etc.
  - e. Medidas de detección (su objetivo es identificar el riesgo):
  - f. Protección Física: sistemas de vigilancia, sensores de movimiento, etc.
  - g. Medidas Técnicas: control de acceso lógico, sesión de autenticación, etc.

- h. Medidas Procedimentales: monitorización de auditoría, etc.
  - i. Medidas de respuesta (su objetivo es impedir o reducir el impacto sobre los activos):
  - j. Protección Física: respaldo de fuente de alimentación (SAI), etc.
  - k. Medidas Técnicas: programa antivirus, auditorías, respaldo de seguridad, etc.
  - l. Medidas Procedimentales: planes de contingencia, etc.
31. Tal y como se ha indicado, el mayor problema de seguridad para la información suelen ser las personas. Por este motivo, la **formación y concienciación del personal** es uno de los objetivos fundamentales que se deben perseguir con la implementación de un programa de concienciación en seguridad. Los diferentes usuarios de la Organización deben asumir su responsabilidad en la protección de la confidencialidad, integridad y disponibilidad de los activos (información) de la Organización y comprender que esto no es sólo competencia de los especialistas en seguridad. La seguridad debe considerarse como parte de la operativa estándar, no como algo añadido al trabajo habitual, siendo fundamental la incorporación de la seguridad a la actividad laboral.
32. Un programa de concienciación debe perseguir dejar claro no sólo cómo proteger los activos de la Organización sino también por qué es importante su protección y cómo los usuarios se convierten en la primera barrera de seguridad para ellos. La implementación del programa ayuda a minimizar los costes ocasionados por los incidentes de seguridad dado que actúa directamente sobre uno de los eslabones más débiles en la cadena de seguridad, los usuarios.

## II. CIFRADO DE DATOS

## 2. INTRODUCCIÓN A LA CRIPTOLOGÍA

### 2.1. INTRODUCCIÓN

33. La criptología (del griego *krypto* y *logos*, estudio de lo oculto, lo escondido) es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones (en el ámbito tecnológico, ese canal suele ser una red de computadoras). Esta ciencia está dividida en dos grandes ramas:
- a. La **criptografía**, ocupada del cifrado de mensajes y del diseño de criptosistemas. Se entiende por cifra, genéricamente, la transformación de una información hasta hacerla ininteligible, según un procedimiento y una clave determinados que pretende que sólo quien conozca dichos procedimientos y clave pueda acceder a la información original.
  - b. El **criptoanálisis**, que trata de descifrar los mensajes en clave, rompiendo así el criptosistema; consiste por tanto en los pasos y operaciones orientadas a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado y/o la clave. Se puede considerar como la rama ofensiva de la criptología, siendo la cifra la parte defensiva de la misma.
34. La criptografía es una de las ciencias consideradas como más antiguas, ya que sus orígenes se remontan al nacimiento de la civilización. Su uso original era el proteger la confidencialidad de informaciones militares y políticas, pero en la actualidad es una ciencia interesante no sólo en esos círculos cerrados, sino para cualquiera que esté interesado en la confidencialidad de unos determinados datos. Aunque el objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente la privacidad o confidencialidad de los datos, sino que se busca además garantizar la autenticidad de los mismos (el emisor del mensaje es quien dice ser, y no otro), su integridad (el mensaje que lee el receptor es el mismo que le fue enviado) y su no repudio (el emisor no puede negar el haber enviado el mensaje). Por tanto, mediante técnicas criptográficas se podrá:
- a. Garantizar la **confidencialidad de la información** que ha sido transformada mediante la aplicación de alguna de las técnicas criptográficas. Este es el primero de los problemas que pretende solucionar la criptografía y, sin duda, el que motivó el nacimiento de la misma. En definitiva, con la aplicación de transformaciones criptográficas se pretende que la información sólo sea recibida por destinatarios autorizados para ello.
  - b. Garantizar la **autenticidad de origen** de un documento, es decir, garantizar que el documento o comunicación provienen de la persona o entidad de quien dice provenir. En los documentos en formato papel, esto se consigue mediante la firma física del emisor de dicho documento, en los documentos digitales esto se lleva a cabo, análogamente, mediante el empleo de la firma digital.
  - c. Garantizar la **autenticidad del contenido** o integridad del documento, es decir, que dicho documento no ha sido modificado por ningún agente

externo a la comunicación. Dada la facilidad de insertar código en un documento digital sin dejar rastro, se hace necesario utilizar procedimientos criptográficos, principalmente con las denominadas funciones hash, que garanticen la integridad.

- d. Evitar el **repudio interesado** de los mensajes por parte de los comunicantes. El problema surge ante la posibilidad de que el emisor o receptor de un determinado mensaje intente negar si ello le conviene, la emisión o recepción del mismo.
- e. Verificar la **identidad de los comunicantes**. El problema es una extensión de la autenticidad a los dos corresponsales que van a establecer una comunicación. En resumen se trata de asegurar que emisor y receptor son quien dicen ser, previo al intercambio de cualquier documento, bien en un sólo sentido o en ambos.

## 2.2. SEGURIDAD CRIPTOGRÁFICA

- 35. En primer lugar, es preciso indicar en este punto que la seguridad absoluta no existe. La criptografía es únicamente capaz de poner barreras más o menos complicadas de franquear para poder garantizar la comunicación con un cierto nivel de confianza. Partiendo de esta premisa, se van a considerar dos campos diferenciados al hablar de la seguridad ofrecida por la criptografía:
  - a. Seguridad de los algoritmos.
  - b. Seguridad de los protocolos.
- 36. La seguridad de los algoritmos se considera comprometida cuando ha sido posible obtener las claves secretas del sistema mientras que la seguridad de los protocolos se considera vulnerada cuando ha sido posible recuperar la información contenida en una comunicación cifrada sin necesidad de recuperar las claves secretas de cifrado. Se pueden distinguir los siguientes niveles de seguridad:
  - a. Seguridad **incondicional** es la ofrecida por los métodos de cifrado para los que se puede demostrar, desde el punto de vista de la Teoría de la Información (Shannon), que no existe la posibilidad de predecir la clave secreta de cifrado conocido el o los textos cifrados. Es decir, el conocimiento del cifrado no aporta ninguna información adicional o residual que permita obtener las claves de cifrado o el texto original que fue cifrado. Los cifrados que satisfacen esta condición se denominan cifrados perfectos.
  - b. Seguridad **computacional** es la ofrecida por aquellos métodos de cifrado tales que no existe capacidad de cálculo suficiente en el universo para obtener su clave secreta asociada. La seguridad computacional está definida de acuerdo con la teoría de la complejidad, los conocimientos matemáticos y las prestaciones de los ordenadores actuales. RSA es un ejemplo de algoritmo de cifrado cuya seguridad se demuestra computacionalmente.
  - c. Seguridad **probable** es la relacionada con aquellos métodos de cifrado que, aún sin estar basados en principios matemáticos de seguridad

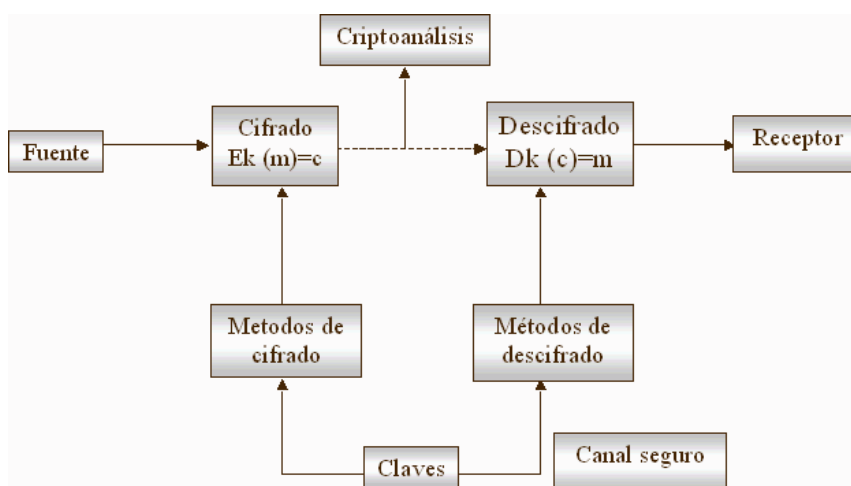
demostrable, no han podido ser violados pese a los esfuerzos para conseguirlo. DES es uno de los algoritmos que se incluyen en este apartado como ejemplo.

- d. Seguridad **condicional** es la ofrecida por los métodos de cifrado diseñados con fines específicos, donde la dificultad para el quebrantamiento de la seguridad es siempre superior a la supuesta capacidad de análisis del potencial agresor.

## 2.3. DEFINICIÓN DE CRIPTOSISTEMA

37. En la transformación de un mensaje inteligible en un mensaje cifrado intervienen diversos componentes, disponiéndose de un criptosistema cuando estos componentes interactúan de forma adecuada. En general, al menos, un criptosistema se define como una cuaterna de elementos  $\{A, K, E, D\}$ :

- a. Un conjunto finito llamado **alfabeto**,  $A$ , a partir del cual, y utilizando ciertas normas sintácticas y semánticas, será posible emitir un mensaje en claro (*plain text*) u obtener el texto en claro correspondiente a un mensaje cifrado (*cipher text*); frecuentemente, este alfabeto es el conjunto de los enteros módulo  $q$ ,  $Z_q$ , para un  $q$  dado. Se puede dividir el alfabeto  $A$  en dos espacios diferentes: el espacio de mensajes,  $M$ , formado por los textos en claro que se pueden formar con el alfabeto, y el espacio de cifrados,  $C$ , formado por todos los posibles criptogramas que el cifrador es capaz de producir
- b. Otro conjunto finito denominado **espacio de claves**,  $K$ , formado por todas las posibles claves, tanto de cifrado como de descifrado, del criptosistema.
- c. Una familia de aplicaciones del alfabeto en sí mismo,  $E: A \rightarrow A$ , llamadas **transformaciones de cifrado**. El proceso de cifrado se suele representar como  $E(k, a) = c$ , donde  $k \in K$ ,  $a \in A$  y  $c \in A$ .
- d. Otra familia de aplicaciones del alfabeto en sí mismo,  $D: A \rightarrow A$ , llamadas **transformaciones de descifrado**. Análogamente al proceso de cifrado, el de descifrado se representa como  $D(k', c) = m$ , donde  $k' \in K$ ,  $c \in A$  y  $m \in A$ .



38. El emisor emite un texto en claro, que es tratado por un cifrador con la ayuda de una cierta clave,  $k$ , creando un texto cifrado (criptograma). Este criptograma llega al descifrador a través de un canal de comunicaciones (como se ha dicho antes, este canal será habitualmente algún tipo de red), y este convierte el criptograma de nuevo en texto claro, apoyándose ahora en otra clave (esta clave puede o no ser la misma que la utilizada para cifrar). Este texto claro ha de coincidir con el emitido inicialmente para que se cumplan los principios básicos de la criptografía moderna: en este hecho radica toda la importancia de los criptosistemas, ya que la condición necesaria y suficiente para que exista un criptosistema es que para una clave dada  $k$ , la transformación  $D_k$  sea la inversa de  $E_k$ ; es decir:

a.  $D_k(E_k(m)) = m, m \in M$

39. Aunque habitualmente se cumple que para una clave  $k$ , la transformación  $E_k$  también es la inversa de la transformación  $D_k$  esta condición no es necesaria, y en el caso de darse no es suficiente para que exista un criptosistema.
40. Es obvio, a la vista de lo expuesto anteriormente, que el elemento más importante de todo el criptosistema es el cifrador, que ha de utilizar el algoritmo de cifrado para convertir el texto claro en un criptograma. Usualmente, para hacer esto, el cifrador depende de un parámetro exterior, llamado **clave de cifrado** (o de descifrado, si se trata del descifrador) que es aplicado a una función matemática irreversible (al menos, computacionalmente): no es posible invertir la función a no ser que se disponga de la clave de descifrado. De esta forma, cualquier conocedor de la clave (y, por supuesto, de la función), será capaz de descifrar el criptograma, y nadie que no conozca dicha clave puede ser capaz de descifrarlo, aún en el caso de que se conozca la función utilizada.
41. Para finalizar este punto, es necesario indicar que si se atiende a una definición más amplia de un criptosistema, en la que se incluya la generación y distribución de claves como algo inseparable del criptosistema, se puede considerar que los generadores aleatorios y los generadores de números primos son necesarios en cualquier criptosistema. Los primeros para la generación de vectores iniciales, claves de mensaje e incluso las propias claves del sistema y los segundos para la generación de las parejas de claves (pública y privada) utilizadas en los criptosistemas asimétricos.

### 2.3.1. PRINCIPIOS DE LOS CRIPTOSISTEMAS DE CLAVE SECRETA

42. Se denomina **criptosistema de clave secreta** (de clave privada, de clave única o simétrico) a aquel criptosistema en el que la clave de cifrado,  $K$ , puede ser calculada a partir de la de descifrado,  $K'$ , y viceversa. En la mayoría de estos sistemas, ambas claves coinciden, y por supuesto han de mantenerse como un secreto entre emisor y receptor: si un atacante descubre la clave utilizada en la comunicación, ha roto el criptosistema.
43. El secreto se garantiza ya que se utiliza la clave de forma secreta tanto para cifrar como para descifrar la información. La autenticidad se logra al permanecer secreta la clave, sólo el emisor legítimo puede producir un cierto mensaje



cifrado que puede a su vez ser descifrado por el receptor haciendo uso de la clave compartida por ambos.

44. Hasta la década de los setenta, la invulnerabilidad de todos los sistemas dependía del mantenimiento en secreto de la clave de cifrado. Este hecho presentaba una gran desventaja: había que enviar, aparte del criptograma, la clave de cifrado del emisor al receptor, para que éste fuera capaz de descifrar el mensaje; por tanto, se incurría en los mismos peligros al enviar la clave, por un sistema que había de ser supuestamente seguro, que al enviar el texto plano. Adicionalmente, desde el punto de vista del intercambio de información el hecho de que exista al menos una clave de cifrado y descifrado entre cada dos usuarios de un sistema haría inviable la existencia de criptosistemas simétricos en las grandes redes de computadores de hoy en día: para un sistema de computación con  $N$  usuarios, se precisarían  $N \cdot (N-1)/2$  claves diferentes, lo cual es obviamente imposible en grandes sistemas. Por este motivo, la cifra de clave secreta se utiliza actualmente y de forma principal para cifrar datos en sistemas de almacenamiento, permitiendo recuperarlos mediante el conocimiento de la contraseña de cifrado.

### 2.3.2. PRINCIPIOS DE LOS CRIPTOSISTEMAS DE CLAVE PÚBLICA

45. En 1976, Whitfield Diffie y Martin Hellman, de la Universidad de Stanford, demostraron la posibilidad de construir criptosistemas que no precisaran de la transferencia de una clave secreta, dando así lugar a lo que se denomina criptografía de clave pública.
46. Los criptosistemas de clave pública se caracterizan por utilizar **dos claves** para cada participante. Una sirve en general para la operación de cifrado y es pública mientras que la otra clave, la de descifrado, es secreta y única para poder recuperar la información cifrada. Ambas claves no son independientes, pero del conocimiento de la pública no es posible deducir la privada sin ningún otro dato (cabe recordar que en los sistemas de clave privada sucedía lo contrario). Se tiene pues un par clave pública-clave privada. La existencia de ambas claves diferentes, para cifrar o descifrar, hace que también se conozca a estos criptosistemas como **asimétricos**.
47. La función que utiliza la **operación** de cifrado es una **función unidireccional con trampa** que permite realizar el descifrado fácilmente por el poseedor de la clave secreta (trampa) y representa un problema de un orden de complejidad computacional elevado si no se posee.
48. Los criptosistemas de clave pública tienen la ventaja sobre los de clave secreta o convencionales, en que estos últimos tienen que intercambiar previamente las claves de sesión manejando un número elevado de las mismas equivalente a " $n(n-1)/2$ " (siendo  $n$  el número de usuarios). En los criptosistemas de clave secreta el número de claves es equivalente a " $2n$ " estableciéndose al dar de alta a los usuarios en el sistema (una única vez).
49. Cada usuario **A** tiene un par de claves, una **E<sub>AB</sub>** pública para el cifrado y otra **D<sub>AV</sub>** secreta para el descifrado. De tal forma, que con **D<sub>AV</sub>** se descifra lo que se ha cifrado con la clave pública de cifrado **E<sub>AB</sub>** correspondiente:

- a.  $M = D_{AV} (E_{AB} (M))$

50. y además, se verifica que:
- $M = E_{AB}(D_{AV}(M))$
51. lo que significa que cualquier usuario puede cifrar un mensaje con su clave privada de descifrado y recuperarlo otro usuario con la clave pública  $E_{AB}$  del primero. Esta facultad permite la implantación de la firma electrónica, permitiéndose el uso de  $E_{AB}$  y  $D_{AV}$  en cualquier orden pero obligando a que los espacios de mensajes y cifrados sean el mismo. La firma electrónica o digital es la propiedad exclusiva de un individuo o proceso que se utiliza para la firma de información o mensajes, de tal forma que la información que se añade al mensaje garantiza la autenticidad del remitente, al igual que lo consigue la firma manuscrita.

## 2.4. TEORÍA DE NÚMEROS

52. La base de la criptografía es puramente matemática y está estrechamente relacionada con otras ciencias como la estadística, la teoría de la complejidad o la teoría de números. En este punto se van a presentar unas bases matemáticas elementales para poder comprender diferentes aspectos de la criptografía.

### 2.4.1. NÚMEROS PRIMOS

53. Se denomina **número primo** a cualquier entero mayor que 1 divisible únicamente por él mismo y por la unidad: estos son sus únicos factores. Ejemplos de números primos son 2, 3 o 5, aunque en criptografía (sobre todo en la de clave pública) es únicamente útil la utilización de números primos extremadamente grandes, de 512 bits o incluso más, como  $2^{756839}-1$ . El conjunto de números primos es obviamente infinito.
54. Se dice que dos números  $a$  y  $b$  son **relativamente primos** si no comparten entre sí más factores que la unidad; un número primo es relativamente primo al resto de números, excepto a sus múltiplos. Otra forma de decir que dos números son relativamente primos es que su máximo común divisor sea la unidad ( $\text{mcd}(a,b)=1$ ), definiendo el máximo común divisor de dos números como el número más grande que divide a ambos. Una forma habitual de calcular el máximo común divisor de dos números es mediante el algoritmo de Euclides.

### 2.4.2. ARITMÉTICA MODULAR

55. Definimos la relación de **congruencia** módulo  $p$ , denotada por  $a \equiv b \pmod{p}$ , si se cumple que  $a=b+k \cdot p$ , para un entero dado  $p$  (dicho de otra forma, si  $a-b$  es múltiplo de  $p$ ). En esta relación,  $b$  se denomina **residuo** de  $a \pmod{p}$ , y se dice que  $a$  es **congruente** con  $b \pmod{p}$ . Al conjunto de enteros de 0 a  $p-1$  se le denomina conjunto completo de residuos módulo  $p$ : esto significa que para cada entero  $a$ , su residuo módulo  $p$  es un número entero entre 0 y  $p-1$ . La operación  $a \pmod{p}$  se denomina **reducción modular**, y denota el residuo de  $a$ , de forma que este residuo es un entero entre 0 y  $p-1$ ; por ejemplo,  $100=34 \pmod{11}$ , ya que  $100=34+11 \cdot 6$ . Como la aritmética entera, la modular cumple las propiedades conmutativa, asociativa y distributiva.

56. En criptografía es habitual el uso de la aritmética modular debido a que el cálculo de logaritmos discretos y raíces cuadradas mod  $p$  pueden ser problemas computacionalmente costosos; además, la aritmética modular utiliza cálculos que se realizan cómodamente en ordenadores, ya que restringe tanto el rango de valores intermedios calculados como el resultado final: no es necesario que utilizar grandes números (y por tanto, grandes reservas de memoria) para almacenar resultados, ya que su tamaño siempre estará limitado.
57. Cuando el número  $p$  al que se ha hecho referencia es primo forma lo que se denomina un Campo de Galois módulo  $p$ , denotado  $GF(p)$ , en el que se cumplen las leyes habituales de la aritmética entera, y que es enormemente utilizado en protocolos criptográficos, como se verá a continuación.

### 2.4.3. EXPONENCIACIÓN Y LOGARITMO DISCRETO

58. Muchos sistemas criptográficos utilizan operaciones de potenciación (exponenciación) en Campos de Galois: elevar una base  $a$  a una potencia  $e$  módulo  $p$ :
  - a.  $b = a^e \text{ mod } p$  (1)
59. Esta potenciación no es más que una serie de multiplicaciones y divisiones, que computacionalmente tienen un coste lineal con  $p$  ( $O(p)$ ). Existen aceleraciones al algoritmo directo (multiplicar  $e-1$  veces la base por sí misma y luego efectuar una reducción modular de un número grande), como la realización de multiplicaciones y reducciones modulares más pequeñas. Por ejemplo, si se quiere calcular  $a^8 \text{ mod } p$ , es posible efectuar la operación directa
  - a.  $(a \times a \times a \times a \times a \times a \times a \times a) \text{ mod } p$
60. que evidentemente tiene un elevado coste, o realizar un cálculo equivalente y computacionalmente más barato:
  - a.  $((a^2 \text{ mod } p)^2 \text{ mod } p)^2 \text{ mod } p$
61. El problema inverso a la exponenciación es el cálculo del **logaritmo discreto** de un número módulo  $p$ : encontrar  $x$  tal que  $a \cdot x = b \text{ mod } p$ . Mientras que el problema de la exponenciación es relativamente sencillo, el cálculo del logaritmo discreto es generalmente un problema intratable, y de ahí su interés criptográfico.

## 2.5. TEORÍA DEL SECRETO PERFECTO

62. En un criptosistema siempre se deberán tener en cuenta los objetivos de confidencialidad y autenticidad definidos por Shannon:
  - a. **Confidencialidad:** considerada como la incapacidad, para un criptoanalista, de determinar el texto original a partir del texto cifrado que se haya podido interceptar.
  - b. **Autenticidad:** considerada como la incapacidad, para un criptoanalista, de improvisar o sustituir un texto cifrado falso  $c'$  en lugar del texto cifrado real  $c$  sin que el receptor lo detecte. El concepto de autenticidad va asociado al concepto de “integridad” de la información, si bien puede darse la circunstancia de que un mensaje sea auténtico y sin embargo no

sea íntegro (mensajes distorsionados a causa del ruido del canal empleado).

63. La definición de autenticidad introducida por Shannon ha derivado hoy en día en dos conceptos diferentes: por un lado la autenticidad del origen de la transmisión y por otro la autenticidad del contenido de la transmisión, también denominada habitualmente integridad. Dado que en la actualidad se almacena gran cantidad de información digitalmente se hace necesario, una vez que se ha garantizado la autenticidad del origen, poder garantizar en todo momento la autenticidad del contenido, de forma que cualquier manipulación de la información pueda ser detectada.

#### 2.5.1. TEORÍA DE LA CONFIDENCIALIDAD PERFECTA

64. Las propiedades de los sistemas criptográficos fueron estudiadas por Shannon desde el punto de vista de la **Teoría de la Información**:
  - a. Mensajes originales **M**, con probabilidades **p(m)**, tales que  $\sum_m p(m) = 1$ .
  - b. Mensajes cifrados **C**, con probabilidades **p(c)**, tales que  $\sum_c p(c) = 1$ .
  - c. Claves **K**, escogidas con probabilidades **p(k)**, tales que  $\sum_k p(k) = 1$ .
65. Sea **p(m<sub>i</sub> | c<sub>j</sub>)** la probabilidad de que el mensaje **m<sub>i</sub>** haya sido enviado, supuesto que **c<sub>j</sub>** ha sido recibido (**c<sub>j</sub>** es el criptograma asociado al mensaje original **m<sub>j</sub>**), se da el *secreto perfecto* si y sólo si **p(m | c) = p(m)**, es decir sólo si la interceptación del texto cifrado no da ninguna información al criptoanalista.

#### 2.5.2. AUTENTICIDAD PERFECTA EN UN CRIPTOSISTEMA

66. Treinta y cinco años después de que Shannon desarrollara su teoría de la seguridad perfecta, Simmons publicó una formalización de la teoría de la autenticidad perfecta. En este estudio se supone que el criptoanalista tiene más libertad y que puede generar criptogramas fraudulentos y, tal como ya hizo Shannon, Simmons supone que la clave tan sólo puede ser usada una vez para formar el criptograma auténtico.
67. Con estas suposiciones, el criptoanalista puede llevar a cabo dos tipos de ataque:
  - a. Ataque de Personalización: consiste en formar un criptograma fraudulento **c'** sin esperar a ver el criptograma auténtico **c**. Se considera que este ataque tiene éxito si el receptor legal acepta **c'** como auténtico.
  - b. Ataque de Sustitución: consiste en formar un criptograma fraudulento **c'** una vez visto el criptograma auténtico **c**. Se considera que este ataque tiene éxito si el receptor legal acepta **c'** como auténtico y  $D_k(c') = m' \neq m$ , siendo **m** ∈ **M** el mensaje original.
68. Según lo anterior, si definimos la probabilidad de éxito del ataque de personalización como **P<sub>p</sub>** y definimos la probabilidad de éxito del ataque de sustitución como **P<sub>s</sub>**, la probabilidad de engaño **P<sub>e</sub>** será el máximo entre la probabilidad de personalización y la probabilidad de sustitución.
  - a.  $P_e = \max(P_p, P_s)$

69. De esta manera un criptosistema tiene la propiedad de autenticidad perfecta si se verifica que la probabilidad de engaño es cero ( $P_e = 0$ ).

### 2.5.3. ATAQUE DE SUSTITUCIÓN EN UN SISTEMA DE CLAVE PÚBLICA

70. Un ataque típico de sustitución denominado *man-in-the-middle* (hombre en el medio) permite obtener los textos claros transmitidos entre **A** y **B** modificándolos, borrándolos o incluso generando uno totalmente distinto (en este caso se trataría de un ataque de personalización). La forma de realizarlo es como sigue:
- Si un atacante **C** tiene acceso al directorio de claves públicas donde se encuentran depositadas las claves públicas de **A** y **B**, puede proceder a sustituirlas por dos claves públicas generadas por él mismo y de las que tiene las correspondientes claves privadas, almacenando las verdaderas claves de **A** y **B**.
  - Una vez que las claves han sido sustituidas, cuando **A** manda un mensaje a **B** lo cifra con una clave pública que en realidad pertenece al atacante. En estas condiciones **C** intercepta el mensaje de **A** y lo puede descifrar puesto que tiene la clave privada correspondiente.
  - Una vez que **C** tiene el texto descifrado puede optar por mantenerlo como está, modificarlo o incluso hacer uno nuevo, el cual es cifrado con la verdadera clave pública de **B** y remitido a su destino.
  - El receptor **B** recibe el mensaje, lo descifra correctamente y piensa que efectivamente es de **A** y que solo él ha tenido acceso al mismo.
  - El ataque funciona igual en sentido inverso.
71. Como conclusión del ataque descrito se puede decir que las claves públicas únicamente deben estar accesibles dentro del grupo de usuarios que intercambian información; en cualquier otro caso, se necesita una Autoridad de Certificación (CA) que actúe de intermediario a la hora de entregar las claves públicas de los usuarios. La autoridad de certificación debe garantizar que las claves públicas que suministra son de los destinatarios a los que se quiere enviar la información.

### 2.5.4. IMPLEMENTACIÓN PRÁCTICA DEL SECRETO PERFECTO

72. En 1916, G. S. Vernam, ingeniero de AT&T, publicó un método de cifrado para usar con el código de Baudot. El cifrado de Vernam es parecido al de César, sólo que ahora **M**, **C** y **K** toman valores en el alfabeto binario  $\{0,1\}$  y la adición es módulo 2. La idea introducida por Vernam fue usar **la clave sólo una vez (OTK)**, es decir, cifrar cada nuevo bit de texto original con un nuevo bit de clave escogido aleatoriamente. Desde el punto de vista de la Teoría de la Información se demuestra que el cifrado de Vernam es el único incondicionalmente seguro, al cumplir las condiciones del secreto perfecto definidas por Shannon. Para poder llevar a cabo este proceso, hace falta transmitir de manera segura tanta longitud de clave como longitud del mensaje original se quiera cifrar, pero tiene como ventaja que se obtiene realmente un cifrado irrompible.

73. El cifrado de Vernam y su implementación práctica en el conocido sistema de “Cinta Aleatoria” consistente en disponer de cintas de cifrado y descifrado idénticas que se distribuyen en los distintos centros, siendo su longitud superior a cualquier mensaje a transmitir. El proceso de cifrado y descifrado se realiza mediante la operación XOR entre el mensaje y la clave. Una vez utilizada la cinta, ésta debe destruirse.
74. Este sistema, que aún hoy día se sigue utilizando, presenta dos inconvenientes importantes que condicionan su campo de aplicación:
  - a. Necesidad de un canal de distribución de claves seguro, que si se dispone de éste, también se podría utilizar para remitir la información al ser del mismo tamaño.
  - b. Cuando el número de mensajes a transmitir es muy elevado, la distribución de claves puede llegar a ser inviable por dificultades económicas, de espacio, de tiempo, de almacenamiento, etc...

## 2.6. FUNCIONES RESUMEN

75. Matemáticamente se definen las funciones resumen (*hash functions*) como proyecciones de un conjunto, generalmente con un número elevado de elementos (incluso infinitos), sobre un conjunto de tamaño fijo y mucho más pequeño que el anterior. Por ejemplo, se podría definir la siguiente función resumen, que va de un conjunto con un número infinito de elementos a otro con únicamente 10:
  - a.  $H(x) = x \bmod 10, x \in \mathcal{R}, H(x) \in [0,9]$
76. Sin embargo, aunque la anterior sea una función resumen en sentido estricto, no es especialmente interesante en aplicaciones criptográficas; para serlo, habría de cumplir los siguientes requisitos:
  - a. La entrada puede ser de un tamaño indeterminado.
  - b. La salida es de un tamaño fijo, varios órdenes de magnitud más pequeño que el anterior.
  - c. Para un cierto  $x$ , calcular  $H(x)$  es computacionalmente barato.
  - d.  $H(x)$  es de un solo sentido.
  - e.  $H(x)$  no presenta colisiones.
77. El que una función *hash* sea de un **solo sentido** (lo que se denomina *One-Way hash function*) no implica más que a partir del valor de  $H(x)$  no puedo obtener el de  $x$ : no existe, o su cálculo es computacionalmente difícil. Las colisiones en una función resumen se producen cuando para dos entradas diferentes  $x$  e  $y$ ,  $H(x)=H(y)$ , y se habla de funciones *hash* **débilmente libres de colisiones** (*weakly collision free*) cuando es computacionalmente imposible encontrar dos elementos  $x$  e  $y$  tales que cumplan  $H(x)=H(y)$ ; si aparte de computacionalmente imposible también lo es matemáticamente, se habla de funciones resumen **fuertemente libres de colisiones** (*strongly collision free*).
78. Una de las aplicaciones criptográficas más importante de las funciones resumen es sin duda la verificación de integridad de archivos. La idea es sencilla: en un



sistema del que se tenga constancia que está limpio (esto es, que no ha sido troyanizado o modificado de cualquier forma por un atacante) es posible generar resúmenes de todos los ficheros considerados clave para el correcto funcionamiento de la máquina y guardar dichos resúmenes - como ya indica su nombre, mucho más cortos que los archivos originales - en un dispositivo de sólo lectura. Periódicamente se vuelven a generar los resúmenes y comparar su resultado con el almacenado previamente: si no coinciden, se puede estar seguro (o casi seguro) de que el fichero ha sido modificado. Para este tipo de aplicaciones se suelen utilizar funciones resumen como MD5 o SHA.

79. Otra aplicación importante de las funciones resumen es la firma digital de mensajes - documentos - y su marca de tiempo (*timestamping*); en el primer caso, como los algoritmos de firma digital suelen ser lentos, o al menos más lentos que las funciones *hash*, es habitual calcular la firma digital de un resumen del fichero original, en lugar de hacer el cálculo sobre el propio fichero (evidentemente, de tamaño mayor que su resumen). Con respecto al *timestamping*, las funciones *hash* son útiles porque permiten publicar un resumen de un documento sin publicar su contenido, lo cual permite a una parte obtener un *timestamp* de un documento sin que la autoridad de *timestamp* conozca el contenido del mismo, pero asegurándose la validez del procedimiento en caso de repudio; en ambos casos, tanto en la firma digital como en el *timestamping*, trabajar con el resumen es completamente equivalente a trabajar con el archivo original.

## 2.7. CRITERIOS DE DISEÑO DE UN CRIPTOSISTEMA

80. Shannon indicó algunas técnicas útiles a la hora de diseñar un algoritmo o procedimiento de cifrado. De ellas las más importantes son la realización de operaciones para ocasionar difusión y confusión en el proceso de cifrado de la información.
  - a. **Difusión:** consiste en expandir la influencia de cada símbolo del texto original sobre tantos símbolos del texto cifrado como sean necesarios para evitar un ataque sobre la clave basado en un fraccionamiento del texto cifrado (sustituciones).
  - b. **Confusión:** consiste en el uso de transformaciones de cifrado que compliquen la realización de correlaciones estadísticas entre el texto original y el texto cifrado (transposiciones).
81. Un ejemplo de algoritmos de cifrado, que se ajustan a los principios de difusión y confusión, son los cifrados concatenados, basados en transposiciones (permutación de los símbolos del texto original) y sustituciones (reemplazamiento de cada símbolo del texto original por otro símbolo del mismo alfabeto) que se van encadenando hasta dar el texto cifrado la robustez suficiente.

### 2.7.1. ATAQUES A UN CRIPTOSISTEMA

82. El criptoanálisis es la ciencia opuesta a la criptografía (quizás no es muy afortunado hablar de ciencias opuestas, sino más bien de ciencias complementarias), ya que si ésta trata principalmente de crear y analizar

- criptosistemas seguros, la primera intenta romper esos sistemas, demostrando su vulnerabilidad: dicho de otra forma, trata de descifrar los criptogramas.
83. En el análisis para establecer las posibles debilidades de un sistema de cifrado, se han de asumir las denominadas **condiciones del peor caso**:
- a. El criptoanalista tiene acceso completo al algoritmo de cifrado.
  - b. El criptoanalista tiene una cantidad considerable de texto cifrado.
  - c. El criptoanalista conoce el texto en claro de parte de ese texto cifrado.
84. También se asume generalmente el **Principio de Kerckhoffs**, que establece que la seguridad del cifrado ha de residir exclusivamente en el secreto de la clave, y no en el mecanismo de cifrado:
85. “Si la fortaleza de tu criptosistema descansa en el hecho de que el criptoanalista no conoce los algoritmos empleados, estás perdido. Si crees que guardando en secreto tus algoritmos mejoras la seguridad de tu criptosistema, en vez de permitir que la comunidad académica lo analice para determinar su fortaleza, estás equivocado. Y si tú piensas que nadie desensamblará tu código o realizará ingeniería inversa de tu criptosistema, eres un ingenuo. Los mejores algoritmos son aquellos que se han hecho públicos, que han sido atacados por los mejores criptoanalistas del mundo y todavía son irrompibles”.
86. Aunque para validar la robustez de un criptosistema normalmente se suponen todas las condiciones del peor caso, existen ataques más específicos, en los que no se cumplen todas estas condiciones. Cuando el método de ataque consiste simplemente en probar todas y cada una de las posibles claves del espacio de claves hasta encontrar la correcta, se trata de un ataque de fuerza bruta o **ataque exhaustivo**. Si el atacante conoce el algoritmo de cifrado y sólo tiene acceso al criptograma, se plantea un ataque **sólo al criptograma**; un caso más favorable para el criptoanalista se produce cuando el ataque cumple todas las condiciones del peor caso; en este caso, el criptoanálisis se denomina de **texto en claro conocido**. Si además el atacante puede cifrar una cantidad indeterminada de texto en claro al ataque se le denomina de **texto en claro escogido** (a este ataque también se le llama **de diccionario**, debido a que el atacante suele utilizar un fichero diccionario con los textos en claro que va a utilizar). El caso más favorable para un analista se produce cuando puede obtener el texto en claro correspondiente a criptogramas de su elección; en este caso el ataque se denomina de **texto cifrado escogido**.
87. Cualquier algoritmo de cifrado, para ser considerado seguro, ha de soportar todos estos ataques y otros no citados. Sin embargo, en la criptografía, como en cualquier aspecto de la seguridad, informática o no, no se debe olvidar un factor muy importante: las personas. El sistema más robusto caerá fácilmente si se tortura al emisor o al receptor hasta que desvelen el contenido del mensaje, o si se le ofrece a uno de ellos una gran cantidad de dinero; este tipo de ataques (sobornos, amenazas, extorsión, tortura...) se consideran siempre los más efectivos.
88. A la hora de medir la complejidad de un determinado ataque, se suele hacer mediante la expresión de los recursos computacionales que va a necesitar el mismo. En general, suele expresarse de una de las siguientes formas:



- a. Ocupación en memoria: cantidad de espacio necesario para poder disponer en memoria principal de los datos de entrada al ataque.
- b. Complejidad de proceso: tiempo necesario para procesar un ataque determinado. Como los ordenadores evolucionan constantemente, a veces se expresa en el número de operaciones necesarias para completar un ataque; en función del número de operaciones necesarias y del ordenador disponible se puede calcular el tiempo real del ataque.
- c. Almacenamiento necesario: cantidad de memoria no volátil de almacenamiento necesaria para guardar los datos de entrada al ataque.

## 2.8. ESTEGANOGRAFÍA

89. La esteganografía (también llamada cifra encubierta) es la ciencia que estudia los procedimientos encaminados a ocultar la existencia de un mensaje en lugar de ocultar su contenido; mientras que la criptografía pretende que un atacante que consigue un mensaje no sea capaz de averiguar su contenido, el objetivo de la esteganografía es ocultar ese mensaje dentro de otro sin información importante, de forma que el atacante ni siquiera se entere de la existencia de dicha información oculta. No se trata de sustituir al cifrado convencional sino de complementarlo: ocultar un mensaje reduce las posibilidades de que sea descubierto. No obstante, si lo es, el que ese mensaje haya sido cifrado introduce un nivel adicional de seguridad.
90. A lo largo de la historia han existido multitud de métodos para ocultar información. Quizás los más conocidos hayan sido la tinta invisible, muy utilizada durante la Segunda Guerra Mundial, o las marcas de cualquier tipo sobre ciertos caracteres (desde pequeños pinchazos de alfiler hasta trazos a lápiz que marcan un mensaje oculto en un texto), pero otros mecanismos más extravagantes también han sido utilizados: por ejemplo, afeitar la cabeza de un mensajero y tatuar en el cuero cabelludo el mensaje, dejando después que el crecimiento del pelo lo oculte.
91. Con el auge de la informática, el mecanismo esteganográfico más extendido está basado en diferentes formatos digitales (audio, video, imagen...) y su excelente capacidad para ocultar información. En los últimos tiempos el interés por los mecanismos de ocultación de información en formatos de audio (principalmente MP3) y video ha ido en aumento. Y no es de extrañar: a nadie se le escapa que con la cantidad de mecanismos de intercambio de archivos existentes en la actualidad y que son usados por millones de usuarios para intercambiar ficheros a través de la red, el volumen de información que puede viajar camuflada en los mismos es impresionante. Por este motivo, actualmente la esteganografía es un área de especial interés debido al peligro que entraña el intercambio de información discreto, rápido y efectivo que puede establecerse entre miembros de redes o grupos malintencionados desde cualquier punto del planeta con un simple equipo conectado a Internet.

### 3. CRIPTOSISTEMAS Y MODO DE EMPLEO DE LA CIFRA

#### 3.1. CLASIFICACIÓN DE LOS CRIPTOSISTEMAS

##### 3.1.1. INTRODUCCIÓN

92. Los sistemas de cifrado se pueden clasificar de dos formas diferentes: según el tipo de algoritmo de cifrado empleado y según el modo en que el algoritmo produce el criptograma. En el primero de los casos, según el tipo de algoritmo empleado, los criptosistemas se pueden clasificar en tres grandes grupos:
- a. **Simétricos.** Utilizan una sola clave tanto para cifrar como para descifrar.
  - b. **Asimétricos.** Utilizan un par de claves, una pública para cifrar y una privada para descifrar.
  - c. **Híbridos.** Utilizan una combinación de los anteriores.
93. Dependiendo del modo utilizado por el algoritmo para generar el texto cifrado o criptograma, se pueden dividir en dos grupos:
- a. **Cifrado en bloque.** El sistema de cifrado va operando con bloques de bits de una longitud determinada, por ejemplo 64 bits.
  - b. **Cifrado en serie o de flujo.** El sistema sólo puede cifrar un bit de texto claro al mismo tiempo y por tanto la cifra se realiza bit a bit, esto es, desplazando previamente el conjunto de bits existente en el estado anterior, en número suficiente, para albergar a los nuevos.

##### 3.1.2. CIFRADO SIMÉTRICO

94. En los sistemas de cifrado simétricos la clave de cifrado y descifrado es la misma o bien fácilmente deducible una a partir de la otra. Partiendo de la base que el método de cifrado utilizado se conoce, es imprescindible proteger las claves de cifrado para alcanzar, al mismo tiempo, la confidencialidad y la autenticidad.
95. Estos sistemas de cifrado de una sola clave proporcionan una excelente vía para cifrar la información. Cada usuario **A** tiene sus transformaciones privadas **E<sub>A</sub>** y **D<sub>A</sub>** para cifrar y descifrar el contenido de sus datos. De esta forma, si los demás usuarios no tienen acceso a **E<sub>A</sub>** y **D<sub>A</sub>**, la autenticidad y la confidencialidad están aseguradas.
96. Un típico canal de información es aquel donde emisor y receptor comparten una clave secreta para su comunicación. Si ambas partes son mutuamente confiables, pueden asegurar tanto la confidencialidad como la autenticidad de la comunicación.

##### 3.1.3. CIFRADO ASIMÉTRICO

97. Tal y como se ha indicado en esta misma guía, en 1976 W. Diffie y M. E. Hellman formularon una serie de requisitos que caracterizan a todo sistema de cifrado asimétrico, dando así origen a la criptografía de clave pública. La nueva idea permitía que sistemas prácticamente seguros, para privacidad y

- autenticación de datos, puedan ser implantados sin la necesidad de una transferencia secreta de claves de cifrado.
98. El concepto fundamental de un sistema asimétrico se caracteriza porque las claves vienen dadas en pares (pública/privada) y soportadas en el concepto de funciones unidireccionales con trampa. Cada uno de estos pares de claves cumple con las siguientes propiedades:
    - a. Cualquier información cifrada con una de las claves puede ser descifrada únicamente por la otra clave.
    - b. Dada una clave, la pública, es computacionalmente imposible descubrir la otra, la privada.
  99. Esta distinción entre las claves, una para cifrar y otra para descifrar, hace posible que los usuarios de un sistema de comunicación divulguen sus claves públicas en un "directorio de claves" a semejanza de un listín telefónico.
  100. Un usuario de la red puede mandar un mensaje privado a otro usuario simplemente cifrando dicho mensaje con la clave pública del usuario receptor. Sólo ese usuario, que posee la correspondiente clave privada asociada, puede descifrarlo y recuperar el mensaje original. Incluso quien cifra el mensaje es incapaz de recuperar el texto original del cifrado.
  101. Un usuario puede certificar (firmar o autenticar) un mensaje cifrando dicho mensaje con su propia clave privada. Cualquiera con acceso al directorio de claves públicas puede verificar que el mensaje fue cifrado con la clave asociada a la privada.
  102. En un sistema de comunicación típico con " $n$ " usuarios se requieren " $n(n-1)/2$ " claves diferentes para establecer comunicaciones seguras de cada usuario con el resto, utilizando para ello un sistema de cifrado simétrico. En el mismo sistema de " $n$ " usuarios, usando métodos de cifrado con clave pública se requerirán sólo " $2n$ " claves, de las cuales " $n$ " serán públicas y almacenadas en un directorio de claves públicas del sistema y " $n$ " serán privadas, una para cada uno de los usuarios.
  103. En un criptosistema asimétrico, cada usuario  $U$  dispone de una transformación de cifrado  $E_U$ , registrada en un fichero público y de una transformación de descifrado  $D_U$ , que solo él conoce. Mientras  $D_U$  está descrita en términos de una clave privada, la transformación  $E_U$  lo está mediante un algoritmo o función que no permita, a pesar de su conocimiento y desde un punto de vista computacional, la revelación de  $D_U$ .
  104. En este tipo de criptosistemas la confidencialidad está asegurada, pero la autenticidad no queda protegida ya que todos los usuarios pueden conocer  $E_B$  e intentar transmitir cualquier mensaje haciéndolo pasar por un mensaje legal. En general, para poder conseguir confidencialidad y autenticidad simultáneamente se necesita construir un protocolo más complejo, en el que como paso previo se debe calcular un identificador del mensaje a transmitir mediante una función hash. El identificador será cifrado con la clave privada del emisor y el mensaje con la clave pública del destinatario.

#### 3.1.4. CIFRADO EN BLOQUE

105. El cifrado en bloque trabaja con grupos de bits de una determinada longitud fija, denominados bloques, de manera que cada bloque se cifra con la clave de forma independiente. La fortaleza de este tipo de algoritmos reside en la función de cifrado aplicada, normalmente extraordinariamente compleja y en la que se aplican los principios de confusión y difusión.
106. El funcionamiento básico para cifrar es el siguiente: siendo  $\mathbf{M}$  el texto claro y  $\mathbf{E}_k$  la transformación de cifrado, se divide  $\mathbf{M}$  en sucesivos bloques  $\mathbf{m}_1, \mathbf{m}_2, \mathbf{m}_3, \dots$  y se cifra cada bloque con  $\mathbf{E}_k$ .
- a.  $E_k(\mathbf{M}) = E_k(m_1) E_k(m_2) \dots$
107. Cada bloque es tratado por separado, de la misma manera que el anterior, con lo que cada bloque del mensaje es cifrado utilizándose únicamente a él mismo y la clave de cifrado. El cifrado en bloque puede ser utilizado de tres formas distintas: cifrado en bloque puro, cifrado en bloques encadenados y cifrado en bloques realimentados, cada una de las cuales tiene diversos modos de implementación.

### 3.1.5. CIFRADO EN SERIE

108. En un sistema de cifrado en serie, el mensaje  $\mathbf{M}$  es considerado como una sucesión de caracteres o bits  $\mathbf{m}_1, \mathbf{m}_2, \dots, \mathbf{m}_n$ . De esta forma, cada elemento  $\mathbf{m}_i$  se cifra con un elemento  $\mathbf{k}_i$  que procede de una secuencia  $\mathbf{K} = (\mathbf{k}_i)_{i=1..n}$  denominada serie cifrante.

a.  $E_K(\mathbf{M}) = E_{k_1}(m_1)E_{k_2}(m_2) \dots$

### 3.1.6. SISTEMAS HÍBRIDOS

109. En las implementaciones reales, los algoritmos de clave pública no son empleados para cifrar grandes volúmenes de datos, utilizándose únicamente para cifrar las claves de sesión o los identificadores de los mensajes. Esto es debido a dos razones fundamentales:
- a. Los algoritmos de clave pública son bastante **lentos**: los algoritmos simétricos, en el peor de los casos, son del orden de mil veces más rápidos que los algoritmos asimétricos. Es cierto que los ordenadores cada vez son más potentes pero no es menos cierto que cada vez el volumen de datos a ser cifrado también crece, como mínimo, en la misma proporción que la velocidad de proceso de los ordenadores.
- b. Los criptosistemas de clave pública son **vulnerables a un ataque por texto claro escogido**. Este ataque se basa en el hecho de que si el número de posibles claros a cifrar es limitado, entonces cifrando todos ellos con la correspondiente clave pública se puede determinar cuál es el claro que fue cifrado, aunque no sea posible determinar cuál es la correspondiente clave de descifrado (por ejemplo, en una transacción bancaria donde figura únicamente una cantidad de dinero inferior a quinientos millones).
110. De esta forma, no se debe considerar en ningún caso que la criptografía de clave pública es un sustituto de la criptografía de clave secreta, sino más bien un complemento de ésta a la hora de poder implementar criptosistemas más

versátiles. Así, los criptosistemas híbridos disponen de un algoritmo de cada clase (simétrico y asimétrico), empleándose el algoritmo de clave pública para cifrar la clave de sesión que se utiliza para el cifrado de los datos mediante cifra simétrica. El esquema de funcionamiento es el siguiente:

- a. El usuario **A** que pretende mandar un mensaje cifrado al usuario **B** genera aleatoriamente una clave de sesión.
  - b. Con la clave seleccionada como clave de sesión, **A** cifra el mensaje empleando para ello el algoritmo de clave secreta.
  - c. El usuario **A** cifra la clave de sesión utilizada con la clave pública del destinatario **B** y añade esta información al final del mensaje cifrado, remitiendo toda esta información al destinatario.
  - d. El destinatario **B** recibe la comunicación y, de la misma, extrae la parte correspondiente al cifrado de la clave de sesión. Con su clave privada es capaz de descifrar la clave de sesión y, por lo tanto, disponer de ella.
  - e. Una vez que **B** tiene la clave de sesión, descifra el mensaje utilizando para ello el algoritmo de clave secreta.
111. En los sistemas híbridos el algoritmo de clave secreta se emplea para el cifrado del mensaje y el algoritmo de clave pública para disponer de un canal seguro por donde transmitir la clave empleada en el cifrado del mensaje.

### 3.1.7. COMPONENTES DE UN CRIPTOSISTEMA MODERNO

112. Los criptosistemas modernos, pensados para operar con un gran número de corresponsales y en los que se trata de poder ofrecer todos los servicios criptográficos (confidencialidad, autenticidad, integridad...) disponen básicamente de cinco componentes:
- a. Un algoritmo de clave secreta.
  - b. Un algoritmo de clave pública.
  - c. Un algoritmo hash.
  - d. Un generador aleatorio.
  - e. Un generador de números primos.

## 3.2. MODOS DE EMPLEO DE LA CIFRA

### 3.2.1. CIFRADO LOCAL DE LA INFORMACIÓN

113. En la actualidad el empleo de equipos informáticos, tanto fijos como móviles, con gran capacidad para procesar y almacenar datos está generalizado en cualquier Organización. Las precauciones de seguridad y restricción en los accesos a la información que se aplican en los entornos servidor son, en ocasiones, mucho más débiles –o inexistentes- en los entornos de usuario (equipo sobremesa, portátil, móvil, *tablet*...), mientras que por otro lado son estos equipos los que muchas veces manejan información crítica para la Organización. Se hace necesario, por lo tanto, mejorar la protección de la información gestionada en los entornos de usuario, prestando especial atención

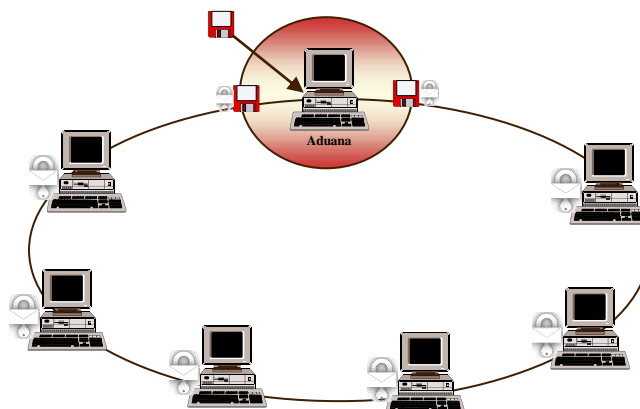
al peligro que supone la facilidad existente para introducir y extraer información de los mismos.

114. Adicionalmente, en una Organización, en contra de lo que mayoritariamente se tiende a pensar, el usuario no debe considerarse el propietario ni de los equipos ni de la información con la que trabaja, haciéndose necesario arbitrar una serie de medidas que permitan la protección de éstos (equipos-información) frente a posibles acciones (accidentales y/o intencionadas) del usuario, limitando la capacidad de acción del mismo dentro de unos márgenes previamente establecidos.
115. De todo lo anterior, se desprende la necesidad de introducir elementos que permitan controlar la utilización que los usuarios hacen de los recursos puestos a su disposición, en especial en lo respectivo a la confidencialidad y protección de la información corporativa, proporcionando así, tanto al usuario como a la Organización en su conjunto, un entorno de trabajo seguro y fiable. Además, para garantizar la máxima funcionalidad y seguridad, las medidas de protección a desplegar deben ser lo más transparentes posible al usuario, de manera que éste no vea entorpecido su trabajo habitual.
116. Una de las medidas básicas de protección a desplegar en los entornos de usuario de una Organización es el cifrado local de toda la información contenida en los soportes de almacenamiento del ordenador y particularmente el cifrado de los dispositivos extraíbles; dicho cifrado (y por supuesto el descifrado) debe producirse de forma que para el usuario sea lo más transparente posible. El cifrado en línea de los soportes de almacenamiento de información no solo soluciona el problema de las fugas indiscriminadas de información en dichos soportes sino que además permite controlar la entrada de información en el ordenador en soportes de almacenamiento, pudiendo así fiscalizar la entrada de software malicioso en el ordenador (virus, caballos de Troya...).

### 3.2.2. CIRCUITO CERRADO DE INFORMACIÓN

117. Se define circuito de información como un conjunto de elementos (dispositivos o equipos informáticos y medios de transmisión) que permiten el intercambio de información entre ellos. Igualmente, se define circuito cerrado de información (CCI) como aquel circuito de información en el que se aplican mecanismos mediante el empleo de técnicas criptográficas para impedir o limitar el intercambio de información con elementos ajenos al mismo.
118. La implantación de un CCI se consigue cifrando los dispositivos de almacenamiento de información de todos los equipos que forman parte del mismo; una vez realizado esto, los equipos quedan totalmente aislados del exterior con lo que no se puede extraer ni incorporar información a los equipos del circuito constituido. Como es lógico, no hay ninguna Organización que pueda permanecer aislada, por lo tanto el CCI crea una serie de “puestos aduana” para relacionarse con el exterior, que serán los encargados de introducir o extraer la información. Estos puestos aduana son los únicos que manejan información abierta en el momento de incorporarla o extraerla del CCI, actuando de pasarela.





**Figura 1.-** Puesto aduana en un Circuito Cerrado de Información

119. En los circuitos cerrados de información resulta complejo el efectuar un cambio de claves, puesto que en este caso es necesario reconvertir todos los soportes de almacenamiento de información, tarea que en algunos casos puede resultar muy compleja. De todas formas, todos aquellos soportes que no sean extraíbles y, por lo tanto, susceptibles de ser utilizados en más de un ordenador, pueden ser cifrados con claves diferentes (cifrado local) y únicamente los soportes removibles necesitan cifrarse con claves conocidas por aquellos componentes del CCI que van a necesitar procesar dichos soportes.
120. Mediante la definición de diferentes claves de cifrado de los soportes extraíbles se puede crear una topología determinada, en general, con la creación de subcircuitos cerrados de información que se ajusten a la estructura de una determinada Organización, permitiendo el intercambio de información entre aquellos subcircuitos que tengan una clave común.
121. En general, el cambio de claves de los dispositivos se contempla únicamente cuando hay indicios racionales de que la seguridad puede estar amenazada o ya ha sido vulnerada; dado que las claves de los soportes no extraíbles de cada equipo tendrán claves diferentes de unos equipos a otros, el compromiso de uno de ellos no afecta a los demás miembros del CCI, por lo que los compromisos de seguridad se pueden tratar de forma independiente.

### 3.2.3. CIFRADO DE COMUNICACIONES

122. Este tipo de cifrado es el utilizado habitualmente, principalmente por la vulnerabilidad que supone el envío de la información desde el emisor hasta el receptor; en función del medio de comunicación empleado la vulnerabilidad es diferente (no es lo mismo utilizar una radio en HF que un cable de fibra óptica) pero en cualquiera de los casos la vulnerabilidad existe y, por lo tanto, se asume que el atacante potencial tiene acceso a las comunicaciones.
123. Se pueden considerar dos formas diferentes de materializar el cifrado de las comunicaciones: cifrado en línea y cifrado fuera de línea. En el primero de los casos, el proceso de cifrado se realiza simultáneamente al proceso de envío de la información (en realidad la información es cifrada inmediatamente antes de ser enviada, pero a una velocidad tal, que es transparente al usuario); en el segundo de los casos, el cifrado de la información se realiza de forma local y, una vez que se dispone de la información cifrada, ésta es enviada al destinatario que igualmente una vez recibida puede almacenarla o descifrarla de forma local.

### 3.2.3.1. COMUNICACIÓN PUNTO A PUNTO

124. El caso más elemental está constituido por un enlace con dos corresponsales involucrados; en el cifrado simétrico se requiere una sola clave, si la misma es utilizada tanto para cifrar en un sentido como en el otro o dos claves, si es distinta la clave según el sentido de la transmisión. Para el caso de un sistema asimétrico, se requieren dos parejas de claves, una para cada corresponsal.



Figura 2.- Comunicación punto a punto entre dos corresponsales

### 3.2.3.2. RED EN ESTRELLA CENTRALIZADO

125. En este esquema uno de los corresponsales actúa como centro de enlace con todos los demás; es la configuración más habitual de cualquier red de comunicaciones cifrada asociada a una Organización.

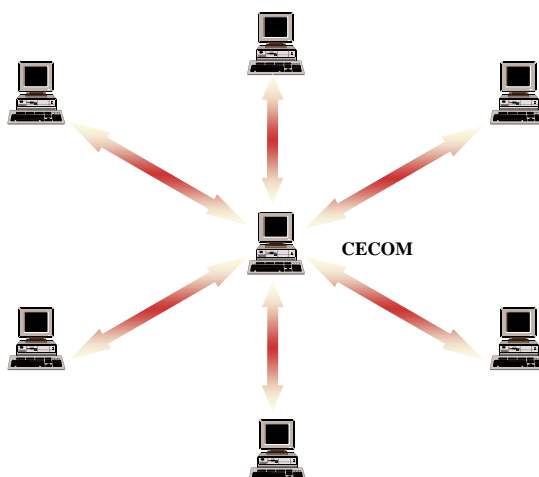


Figura 3.- Esquema de red en estrella centralizado

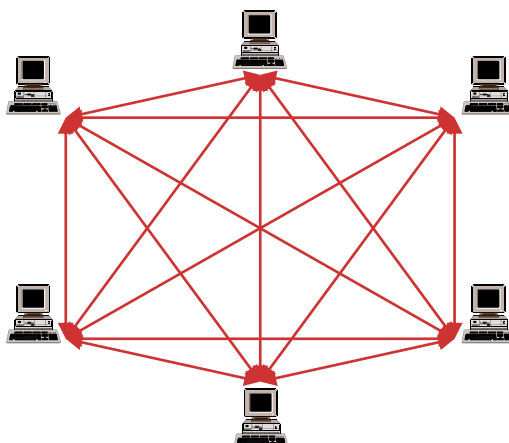
126. En el caso de cifrado simétrico se pueden distinguir los siguientes casos en cuanto al número de claves a emplear en este tipo de red:
- Una sola clave de cifrado para todos los corresponsales, válida para cifrar en cualquiera de los dos sentidos. Esta configuración permite que se puedan producir enlaces no deseados entre los corresponsales al estar todos los equipos con la misma clave: es decir, no garantiza que la configuración de la red sea la que se ha diseñado.
  - Dos claves de cifrado, una para cifrar en un sentido de la comunicación (entrante al centro de comunicaciones) y otra clave para cifrar el sentido opuesto (saliente del centro de comunicaciones). Al igual que en el caso anterior, se pueden producir enlaces no deseados entre los corresponsales.
  - Tantas claves como corresponsales haya en la red que se utilizan para cifrar en ambos sentidos de la comunicación. Es decir se necesitan " $n$ "



- claves, si " $n$ " es el número de corresponsales. En este caso, cada corresponsal únicamente conoce o tiene implementada en su máquina su clave de cifrado y, por lo tanto, no se pueden producir enlaces no deseados entre los corresponsales.
- d. Dos claves de cifrado por corresponsal, una para el cifrado en un sentido de la comunicación y otra para el cifrado en el sentido contrario. Es decir, " $2n$ " claves para una red de " $n$ " corresponsales. Al igual que en el caso anterior, cada corresponsal sólo conoce o tiene implementadas en su máquina sus claves de cifrado y, por lo tanto, no se pueden producir enlaces no deseados.
127. En el caso de implementar un sistema de cifrado basado en clave pública o asimétrico, el número de claves sigue siendo una pareja de claves por corresponsal. En este caso, el centro de comunicaciones debe ser considerado un corresponsal más y, por lo tanto, el número de claves necesario es  $2(n+1)$ . Los enlaces no deseados se producirían a no ser que las claves públicas pasaran a ser secretas, es decir, que no todos los corresponsales tuvieran el listado completo de las claves públicas de los usuarios de la red de comunicaciones.

### 3.2.3.3. RED COMPLETA DE ENLACE

128. En esta configuración todos los enlaces están permitidos, por tanto, no se puede hablar de la existencia de un centro de comunicaciones sino sólo de corresponsales. Para clave secreta se podría utilizar:
- Una sola clave para todos los corresponsales.
  - " $n(n-1)/2$ " claves, si cada enlace tiene su propia clave.
  - " $n(n-1)$ " claves, si cada enlace tiene dos claves, una para cada sentido.



**Figura 4.-** Configuración de red completa de enlace

129. Para el caso de emplear clave pública, se necesitaría una pareja de claves (pública/privada) para cada corresponsal, es decir " $2n$ " claves.

### 3.2.4. GESTIÓN DE CLAVES

130. La gestión de claves de un sistema de cifra es habitualmente la parte más compleja del mismo: diseñar algoritmos criptográficos seguros es difícil, pero guardar en secreto las claves del sistema puede serlo mucho más.
131. Los criptoanalistas atacan los sistemas de cifra a través de una gestión de claves débil, entendiendo por gestión de claves el proceso que incluye generación, transporte, almacenamiento, uso y destrucción de las claves. Hay que tener en cuenta, como en otros ámbitos de la seguridad, que la fortaleza real de un sistema de cifra será la fortaleza del componente más débil del mismo.

#### 3.2.4.1. GENERACIÓN DE CLAVES

132. La seguridad de un criptosistema reside en el secreto de las claves; si se está utilizando un sistema criptográficamente débil para generar las claves, el sistema en su conjunto es débil. Será más sencillo tratar de atacar mediante un criptoanálisis adecuado el proceso de recuperación de las claves, para posteriormente recuperar el contenido de los cifrados (sería un ataque al protocolo de generación de claves).
133. En general, el principal problema en la generación de claves es que se restrinja el espacio posible de claves a valores inferiores a los que proporciona la fortaleza del algoritmo. Por ejemplo, el algoritmo DES utiliza una clave de 56 bits y, por tanto, su fortaleza es de  $2^{56}$ . Sin embargo, hay programas que solo permiten introducir claves de cifrado a través del teclado de un ordenador, obligando a que el octavo bit de cada carácter sea siempre 0 y reduciendo, de esta manera, el espacio “real” de claves posibles. Adicionalmente, otros programas convierten las letras minúsculas a mayúsculas, lo cual vuelve a reducir el espacio de claves y, finalmente desprecia el bit menos significativo de cada byte, resultando que la fortaleza máxima que se puede obtener es de  $2^{40}$ . Esto es una generación de claves que restringe el espacio de las mismas.
134. Otro problema importante a la hora de generar claves es utilizar palabras reales de un idioma: este tipo de claves son vulnerables a un “ataque por diccionario”, el cual consiste en probar todas las palabras de un diccionario como clave de un sistema para verificar si alguna descifra. Existen variantes del ataque por diccionario en el que se combinan las palabras del diccionario entre sí o con un número limitado de caracteres no alfabéticos, de forma que se mejora la probabilidad de encontrar la clave empleada.

#### 3.2.4.2. CLAVES ALEATORIAS

135. Las claves en un criptosistema de clave secreta deben haber sido generadas aleatoriamente, de forma que si, por ejemplo, una clave tiene longitud 128 bits, todas las  $2^{128}$  claves sean igualmente posibles. En resumen, se debe emplear un generador de ruido aleatorio o un generador pseudoaleatorio criptográficamente seguro. Un sistema de generación de claves “pobre” puede dar al traste con la seguridad del mejor criptosistema.
136. La generación de las claves de un criptosistema de clave pública es algo más complejo que lo expresado en el párrafo anterior. En general, las claves de este tipo de criptosistemas deben cumplir ciertas propiedades matemáticas para considerarlas “claves seguras” (ser un número primo, un resto cuadrático...).

### 3.2.4.3. DISTRIBUCIÓN DE CLAVES

137. Para el proceso de distribución de claves se debe disponer de un canal seguro, ya que de otra forma no habrá garantía de que las claves utilizadas no hayan sido comprometidas. Tradicionalmente, este canal se ha habilitado mediante el envío de las claves en valija conducida, que si bien puede considerarse como seguro, es un procedimiento extremadamente caro. Como problema añadido, se ha demostrado necesario proteger las claves que se transportan en valija, en previsión de robos o pérdida de las mismas.
138. Para solucionar el problema de coste que tiene la distribución de claves en valija conducida, actualmente se tiende a emplear otro procedimiento denominado OTAR (*On The Air Rekeying*) que exige disponer de una clave específica para realizar este cometido que se denomina clave de cifrado de claves.
139. Hay que considerar el problema que puede representar la distribución de claves en una red con un gran número de corresponsales en la que se emplea un algoritmo de clave secreta y se pretende que cada enlace de la red se haga con claves diferentes. Para solucionar este problema, la tendencia actual es utilizar criptosistemas híbridos en los que se utiliza una clave de sesión que se envía cifrada con un algoritmo asimétrico, mientras que los datos se cifran con el algoritmo simétrico (cifrados con la clave de sesión).
140. En los criptosistemas híbridos no existen claves acordadas previamente sino un procedimiento para enviar la clave a emplear (clave de sesión) en el momento de enviar o recibir un cifrado.
141. Finalmente, la tendencia actual es a disponer de un mecanismo de almacenamiento, transporte y actualización de claves que impida que el usuario de los medios de cifra conozca las claves que van a ser empleadas. Esta tendencia pretende evitar la posible fuga de claves a través de ataques a los usuarios, como la ingeniería social.

### 3.2.4.4. ALMACENAMIENTO Y DESTRUCCIÓN DE CLAVES

142. Las claves de un criptosistema se deben almacenar de forma segura.; tradicionalmente, esto se ha conseguido depositándolas en una caja fuerte o un espacio equivalente. Hoy en día, es habitual que estas claves se encuentren depositadas, únicamente, en el interior de los equipos en un tipo de memoria especial que impide su extracción fraudulenta. En ocasiones, las claves están cifradas en el interior de estas memorias y, habitualmente, se dispone de algún mecanismo de borrado de emergencia en caso de apertura del equipo.
143. Las claves, una vez que han perdido vigencia, deben ser destruidas por algún procedimiento seguro que garantice la imposibilidad de reproducirlas u obtenerlas después de su destrucción.

### 3.2.4.5. TIPOS DE CLAVES

144. A continuación, se van a reseñar los tipos de clave más frecuentemente utilizadas en los equipos de cifrado:
  - a. **Clave Estructural.** Clave común a todos los equipos de una red de cifra, de carácter semipermanente. Se implementa en software o hardware no

pudiendo, normalmente, ser cambiada por el usuario. A veces, son utilizadas por los propios fabricantes para garantizar que equipos suministrados a diferentes clientes sean incompatibles, caso en el que las claves son permanentes. En otros casos, se utiliza para aislar subredes de cifra dentro de una red mayor que las engloba, permitiendo que el resto de las claves sean iguales, lo cual facilita la gestión de las claves. Este tipo de clave está sufriendo la transformación a dos claves distintas, una la “clave de familia” que sería responsabilidad del fabricante y que casi se puede considerar como parte del algoritmo de cifrado y otra, la propia clave estructural, que sería responsabilidad del usuario.

- b. **Clave Maestra.** Clave de menor jerarquía que la clave estructural pero de máxima jerarquía dentro de las que puede cambiar el usuario. A veces sólo se utiliza para cifrar las claves primarias y secundarias, no utilizándose para el cifrado de mensajes. Normalmente se almacena en un módulo de seguridad del equipo de cifra.
- c. **Claves Primaria y Secundaria.** También llamadas “clave básica” y “clave auxiliar”, son dos de las claves que siempre intervienen en el proceso de cifrado y descifrado de los mensajes. Estas claves o bien son almacenadas cifradas con la clave maestra, o bien se almacenan en un módulo de seguridad de la máquina.
- d. **Clave para Generación de Claves.** Esta clave no siempre existe y su utilización es para generar las claves de mensaje y vectores de inicialización. Cuando el proceso de generación de los anteriores reside en el reloj o similar, este tipo de clave no existe.
- e. **Clave de Mensaje.** Clave generada aleatoriamente o pseudoaleatoriamente que se manda al principio de la transmisión de un cifrado. Su misión es mezclarse con las claves primaria y secundaria para garantizar que no existen dos mensajes cifrados exactamente en las mismas condiciones.
- f. **Vector de Inicialización.** Enviado también al principio de la transmisión, su misión es determinar el punto de la serie cifrante en que empieza el cifrado de los datos.
- g. **Clave de Sesión.** Se denomina así a la clave primaria o secundaria que ha sido generada aleatoriamente antes de proceder al cifrado del mensaje. Se acuerda mediante un procedimiento seguro entre los corresponsales o se envía cifrada al receptor del mensaje para que pueda descifrarlo correctamente.
- h. **Clave Pública.** Clave que se da a conocer a todos los corresponsales de una red que está empleando un sistema de cifrado basado en un algoritmo de cifrado asimétrico.
- i. **Clave Privada.** Clave que cada usuario debe mantener secreta en una red que emplea un sistema de cifrado basado en un algoritmo de cifrado asimétrico.

#### 3.2.4.6. PERÍODO DE VIGENCIA DE LAS CLAVES

145. Dado que los sistemas de cifrado no son de seguridad absoluta y que una clave queda de alguna forma expuesta cada vez que se usa, resultando más comprometida con su reutilización, es conveniente renovar las claves con cierta frecuencia.
146. Aunque no se puede dar un tiempo de vigencia que sea válido para todos los sistemas de cifrado, sí se puede decir que lo ideal es que cada clave de cifrado primaria o secundaria sea utilizada una sola vez. Por lo tanto, la vigencia de un conjunto de claves será aquel período de tiempo en el que se hayan utilizado todas las claves disponibles.

#### **3.2.4.7. OTRAS CONSIDERACIONES FINALES**

147. Es recomendable utilizar claves distintas para cometidos distintos: autenticación, transmisión, almacenamiento, distribución, etc. De la misma manera, es necesario dotar de claves diferentes a grupos o usuarios diferentes que no están autorizados a comunicarse entre sí.
148. Por último, es necesario anular inmediatamente las claves de cifrado de los usuarios que han perdido los privilegios y que ya no tienen que tener acceso a la red de comunicaciones ni a los mensajes que en ella se procesan; de la misma forma, es necesario anular las claves en caso de compromiso de las mismas.

## 4. INTRODUCCIÓN A LA CRIPTOFONÍA

### 4.1. GENERALIDADES

149. El habla es una de las habilidades fundamentales que posee el ser humano sin la cual no podría entenderse fácilmente con otros congéneres, jugando ésta un papel muy importante en la transmisión del conocimiento y en el propio desarrollo del ser humano. En la sociedad actual la comunicación de voz realizada a distancia mediante un determinado sistema de transmisión tiene una importancia capital, debida fundamentalmente a la imperiosa necesidad que tiene el ser humano de utilizar el habla para comunicarse.
150. Por la propia evolución de la tecnología, muchos de los distintos sistemas para transmisión de la voz son relativamente fáciles de interceptar. Como se puede observar en la siguiente tabla, los distintos sistemas de transmisión de voz presentan una elevada vulnerabilidad, que se pone de manifiesto en la estimación del riesgo al que está sometida la información.

SISTEMA TRANSMISIÓN VOZ	RIESGO SEGURIDAD
Telefonía Celular Analógica	Alto
Telefonía Celular Digital	Medio
Telefonía fija	Alto
Buzones de voz	Medio
Radiotelefonía analógica	Alto
Radiotelefonía digital	Medio
Radiotelefonía digital (DES)	Bajo
Internet	Alto

151. Por lo tanto, parece claro que es necesario proteger las comunicaciones de voz a través de los distintos sistemas o medios de transmisión. En determinadas aplicaciones, mantener la confidencialidad de la información puede ser de vital importancia, dada la trascendencia que tiene la información que se envía por los distintos medios de transmisión y el daño que podría causar su conocimiento por parte de determinadas personas u Organizaciones. La necesidad de proteger la información, de forma que únicamente las personas autorizadas tengan acceso a ella, viene impuesta fundamentalmente por la vulnerabilidad de estos canales de transmisión.
152. La seguridad de las comunicaciones de voz se puede tratar de garantizar mediante diferentes procedimientos que son complementarios. Entre estos procedimientos se pueden destacar como más eficaces los que se basan en la aplicación de la criptología a la señal de voz que se va a transmitir.
153. La criptofonía es la rama de la criptología que estudia la forma de hacer ininteligibles las señales de voz que se transmiten a través de los diferentes medios de comunicación. Conviene no olvidar que existen otras medidas que pueden resultar muy útiles para proteger las comunicaciones que complementan e incrementan la seguridad que proporciona el cifrado de las señales de voz.
154. Al equipo de cifra utilizado para el cifrado de la voz se le conoce como criptófono o secráfono, diferenciando ambos términos en el sentido de que el primero se suele utilizar cuando su salida es una señal de voz cifrada digital y el segundo cuando se trata de una señal de voz cifrada analógica. El término

secráfono se ha empleado en determinados ambientes en el mismo sentido que el término inglés *scrambler*, aunque actualmente parece en desuso. En este apartado se utilizará la nomenclatura de criptófono en general, puntualizando si se trata de un criptófono analógico o digital.

## 4.2. CRIPTÓFONOS ANALÓGICOS Y DIGITALES

### 4.2.1. CONSIDERACIONES GENERALES

155. Los criptófonos empleados para proteger las comunicaciones de voz se pueden clasificar de forma general en criptófonos analógicos y digitales, en función de la forma en que realizan la transmisión de la señal de voz cifrada.
156. En el caso de los criptófonos **analógicos**, la señal de voz cifrada se transmite de forma analógica, es decir, la señal transmitida es continua en el tiempo y mantiene el ancho de banda de la señal original. En estos equipos, el proceso de cifrado de la señal de voz en claro se puede realizar de forma analógica o digital. Estos últimos deben convertir, en primer lugar, la señal en claro a formato digital y posteriormente la señal cifrada a formato analógico antes de su transmisión. La señal de voz cifrada que transmite un criptófono digital se encuentra en formato digital, es decir, está formada por una secuencia binaria modulada convenientemente en función del canal de transmisión que se vaya a emplear. En este caso, el ancho de banda de la señal cifrada suele ser mayor y, básicamente, depende del régimen binario de transmisión.
157. Los criptófonos analógicos actuales realizan el cifrado de la voz mediante procesado digital de la señal, aunque los principios de tratamiento de la voz son similares a las de los antiguos secráfonos. Este tipo de cifrador proporciona una calidad de la señal de voz reconstruida similar a la de la voz en claro y, además, el ancho de banda de la señal cifrada es similar al de la voz en claro, por lo que se puede utilizar en canales con ancho de banda limitado.
158. Los criptófonos **digitales** cifran la señal digital de voz de forma similar a como se cifran los datos, de manera que la señal de voz cifrada se asemeja a una transmisión de datos. La principal desventaja de este tipo de criptófonos es la limitación en la posible utilización en un canal de comunicación dado, ya que la señal cifrada tiene un ancho de banda superior al de la señal de voz original. Por otra parte, la calidad de la señal de audio depende de la frecuencia de digitalización: cuanto mayor sea ésta, mayor es la calidad en la señal de voz aunque el ancho de banda también será mayor. La ventaja más importante de este tipo de criptófonos es el elevado nivel de seguridad que proporcionan, que permite su empleo para proteger información del máximo nivel de clasificación.
159. A continuación se resumen las características más importantes de cada uno de los tipos de criptófonos:
  - a. **Criptófonos analógicos.** La señal de voz se transforma en otra señal analógica no inteligible, mediante un procedimiento cuyos parámetros vienen gobernados por un algoritmo de cifrado. La inteligibilidad residual puede variar entre el 3% y el 80%, por lo que el nivel de seguridad es muy variable. Se reconoce la existencia de una señal de voz



en el canal de transmisión e incluso algunas de sus características, hecho que podría facilitar el ataque a este tipo de equipos.

- b. **Criptófonos digitales.** La señal de voz se transforma en una secuencia binaria y se cifra mediante una serie cifrante generada por el algoritmo de cifrado. No se puede reconocer la señal de voz en el canal de transmisión ya que sólo se escucha un ruido similar a una transmisión de datos. Normalmente proporcionan un elevado nivel de seguridad y la calidad de la señal reconstruida depende de la velocidad de transmisión. Las características del canal de transmisión pueden limitar la utilización de este tipo de criptófono en determinadas aplicaciones.

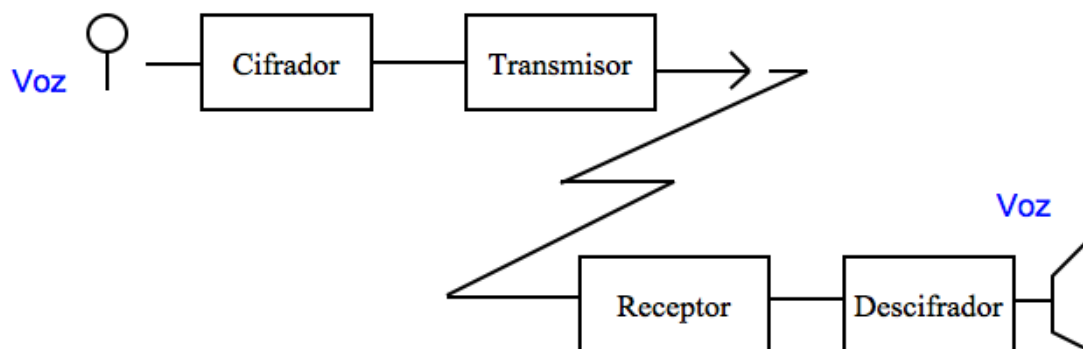
#### 4.2.2. TIPOS DE CRIPTÓFONOS SEGÚN CANAL DE TRANSMISIÓN

- 160. **Líneas telefónicas.** Normalmente se pueden utilizar tanto criptófonos analógicos como digitales; en teoría los criptófonos digitales tienen un mayor nivel de seguridad y, por lo tanto, pueden emplearse para proteger información clasificada con el máximo nivel. Excepto cuando el coste es un factor primordial o en el caso de líneas analógicas de muy mala calidad, lo normal es emplear un criptófono digital, sólo en determinados casos con información de bajo nivel de clasificación o en conversaciones que sólo precisan mantener cierta privacidad puede considerarse razonable el uso de un criptófono analógico.
- 161. **Canal telefónico móvil.** Una posible forma de cifrar las comunicaciones entre terminales móviles es la utilización de un módulo cripto que cifre la voz digital y que transmita esta señal digital utilizando el modo de transmisión de datos del estándar GSM.
- 162. **Canal radio.** El cifrado de las señales de voz transmitidas en este tipo de canales depende de la banda empleada. Normalmente en la banda de HF se emplean sistemas para cifrado de voz analógicos o digitales a baja velocidad (2400 b/s), ya que este tipo de canal no suele permitir el empleo de velocidades de transmisión elevadas. En VHF y UHF se podrían emplear sistemas para cifrado de voz digitales, aunque en este caso pueden presentarse problemas de pérdidas de sincronismo.
- 163. **Enlace multicanal de alta velocidad.** Este tipo de enlaces permite la transmisión de gran cantidad de información, tanto de datos como de voz digital, entre los extremos del enlace. En este caso se suelen emplear cifradores de grupo que realizan el cifrado de todo el enlace (*bulk encryption*).

#### 4.2.3. DIAGRAMA DE BLOQUES DE CIFRADORES ANALÓGICOS Y DIGITALES

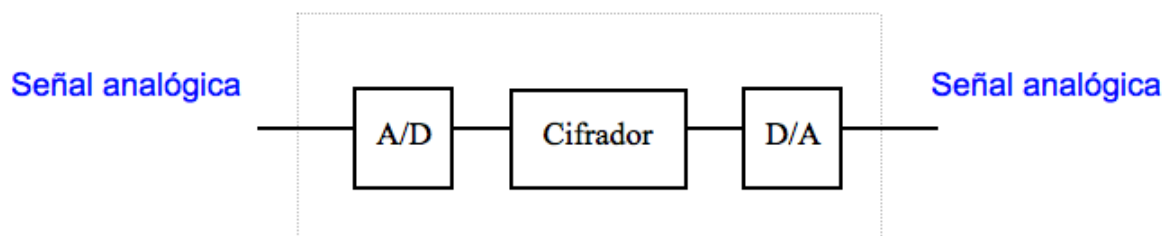
- 164. A continuación se pueden ver los diagramas de bloques simplificados de los sistemas criptofónicos analógicos y digitales, que como puede apreciarse son bastante parecidos: en ambos casos, existe un cifrador que realiza una determinada transformación sobre la señal de voz en claro y un transmisor/receptor que permite la comunicación entre los corresponsales. La diferencia fundamental estriba en la existencia, en los sistemas criptofónicos digitales, de un convertidor A/D (analógico/digital) en los extremos del sistema, además de que las transformaciones que se realizan sobre la señal de voz en claro en ambos tipos de sistemas siguen principios diferentes.

165. Básicamente, el cifrador analógico transforma la señal de voz en claro en otra señal analógica, que posteriormente es transmitida por el transmisor de uno de los correspondientes; en el otro extremo, el equipo del otro correspondiente realiza el procedimiento inverso, obteniendo la señal de voz analógica en claro. En este tipo de sistema criptofónico, la señal de voz, tanto en claro como cifrada, son analógicas aunque el tratamiento de la voz podría realizarse en el cifrador de forma analógica o digital. Actualmente, es más normal que el tratamiento se realice de forma digital.



**Figura 5.-** Diagrama de bloques de un sistema criptofónico analógico

166. En el caso de un sistema criptofónico digital, como se puede ver en la siguiente figura, la señal de voz está en formato binario, excepto a la entrada y salida en donde se encuentra en formato analógico.



**Figura 6.-** Diagrama de bloques de un criptófono analógico con tratamiento digital

167. En este tipo de sistema, la señal en claro se digitaliza mediante un convertidor analógico/digital, se cifra mediante la correspondiente serie cifrante y posteriormente se transmite al extremo receptor. En este extremo, el sistema descifra la señal digital que ha recibido y reconstruye a formato analógico la señal en claro mediante el correspondiente convertidor digital/analógico.

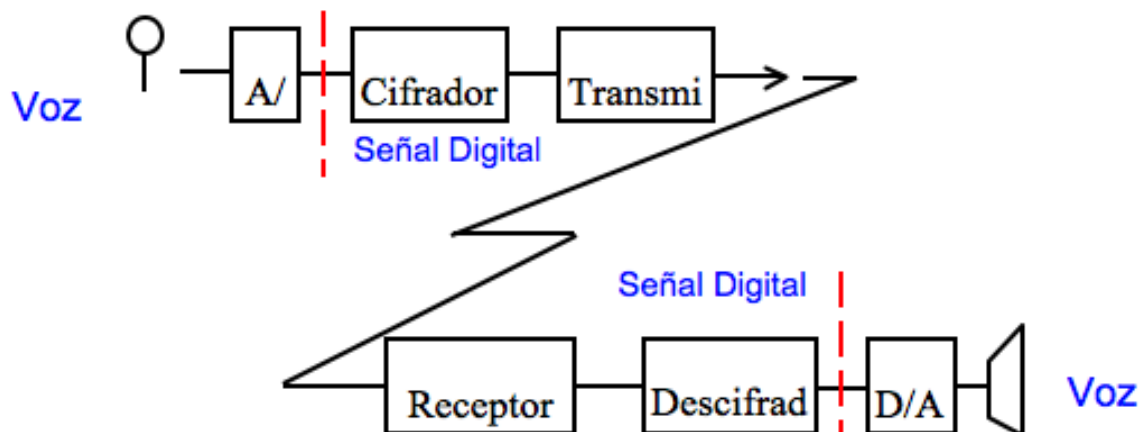
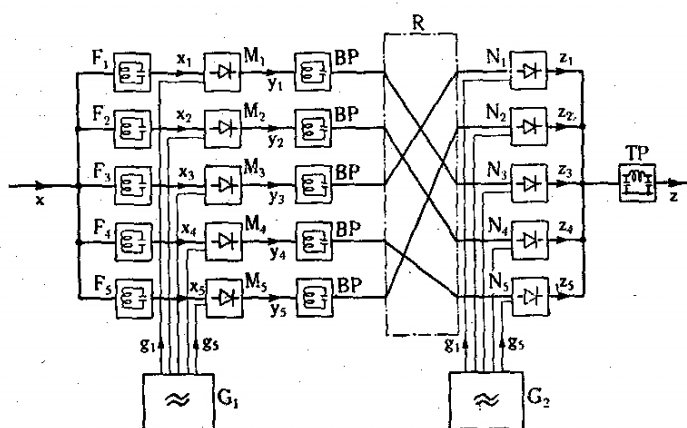


Figura 7.- Diagrama de bloques de un sistema criptofónico digital

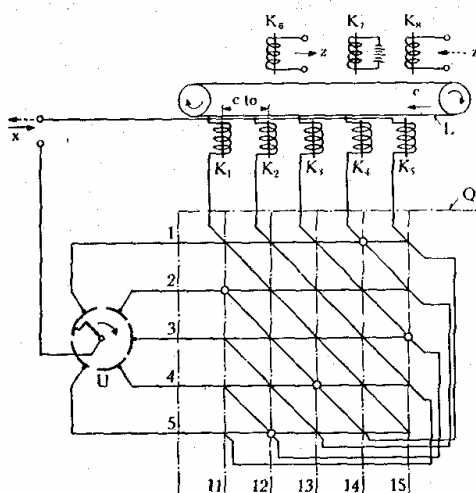
168. Ambos tipos de sistemas necesitan para su correcto funcionamiento emplear las mismas claves y la misma serie cifrante. La selección de la clave se puede hacer de forma manual o automática, transparente al usuario. Para lograr que las series cifrantes coincidan, los criptófonos deben emplear un procedimiento que determine un origen común de tiempos. A este procedimiento se le denomina sincronización y se consigue mediante unas señales conocidas como sincronismos que normalmente preceden a la transmisión cifrada.

#### 4.3. BREVE RESEÑA HISTÓRICA DE LA CRIPTOFONÍA

169. La preocupación por proteger las comunicaciones de voz surgió casi al mismo tiempo que la invención del teléfono: cinco años después de la invención de aquél, concretamente en diciembre de 1881, James Harris Rogers describió un procedimiento para tratar de garantizar la seguridad de la información transmitida por teléfono. Este procedimiento consistía en enviar la señal de voz por diferentes circuitos de forma alternativa. Aunque no se trataba de un método relacionado estrictamente con la criptofonía, este hecho puede considerarse como un antecedente lejano de dicha disciplina o, hablando más estrictamente, de los métodos que tratan de garantizar la seguridad de la transmisión.
170. El desarrollo de la criptofonía tuvo lugar fundamentalmente durante los años veinte y treinta del siglo XX y es consecuencia en gran medida del progreso que experimentan la telefonía y las radiocomunicaciones. Durante esos años se establecen las bases teóricas y se desarrollan distintos tipos de criptófonos. Asimismo se desarrollan diversas herramientas de análisis espectral de aplicación al criptoanálisis.
171. A finales de los años veinte, la compañía norteamericana AT&T introduce los primeros criptófonos analógicos en sus líneas telefónicas y en el enlace radio entre América y Europa. Estos primeros criptófonos son simples inversores de frecuencia, pero posteriormente aparecen equipos con un nivel de seguridad relativamente mayor: concretamente, en el año 1937 se instala por primera vez un criptófono, denominado A3, que realiza una permutación de sub-bandas en el dominio de la frecuencia, desarrollado por los Laboratorios Bell Telephone de AT&T.



**Figura 8.-** Diagrama de bloques de cifrador analógico en el dominio de la frecuencia



**Figura 9.-** Diagrama de bloques de cifrador analógico en el dominio temporal

172. Puede afirmarse que la II Guerra Mundial marca un importante hito en el desarrollo de la criptofonía, tanto desde un punto de vista ofensivo como defensivo. Desde el punto de vista ofensivo, cabe destacar los esfuerzos criptoanalíticos realizados por Alemania y los Estados Unidos. Ambos países se dieron cuenta de la importancia de la inteligencia de comunicaciones y de la necesidad de dedicar recursos a obtener información en claro. Existen bastantes ejemplos de interceptaciones de mensajes, incluida alguna conversación telefónica entre Churchill y Roosevelt, lo que demuestra el nivel adquirido en el criptoanálisis de voz en dicha época. A principios del año 1944, el A3 fue sustituido por un criptófono más seguro que operaba en el dominio temporal y de la frecuencia.
173. La II Guerra Mundial marca también el comienzo de la criptofonía digital. Concretamente, el 15 de julio de 1943 se produce la primera transmisión de voz digital cifrada a través de línea telefónica entre Washington y Londres. El sistema, denominado SIGSALY, estuvo operativo hasta el año 1946, empleándose en más de 3.000 ocasiones.



**Figura 10.-** Fotografía instalación sistema SIGSALY

174. Como se ha mencionado anteriormente, la criptofonía analógica fue empleada para proteger las comunicaciones de voz desde casi el comienzo de la telefonía y las radiocomunicaciones. Sin embargo, la seguridad de estos equipos era limitada debido a los procedimientos empleados que venían impuestos por la tecnología existente. La evolución de la tecnología, especialmente en el campo del tratamiento digital de señal y de la electrónica digital favoreció el desarrollo de criptófonos analógicos más seguros en la década de los años 70 del siglo XX. Este tipo de equipos permitió que existieran criptófonos adecuados para proteger la seguridad de la información efectivamente en diversos medios de transmisión.
175. La criptofonía digital comienza su andadura en los años sesenta, con la puesta en servicio del criptófono HY-2, equipo que presentaba el problema de generar voz sintética no natural. El primer criptófono digital con cierta calidad en la voz reconstruida (voz natural) aparece en los Estados Unidos en el año 1975 (STU-I). Posteriormente, en el año 1983 se pone en servicio el STU-II y el STU-III a finales de los años 80, que incluye diversos tipos de equipos interoperables para distintos sistemas de transmisión. También es interesante mencionar la entrada en servicio en los Estados Unidos, a mediados de los 80, del sistema digital ANDVT (*Advanced Narrowband Digital Voice Terminal*) con módulo cripto KYV-5 que permitía transmitir voz digital y datos cifrados en banda estrecha en radiofrecuencia y vía satélite.
176. Igualmente, desde los años 80 existen diferentes criptófonos digitales desarrollados por diversos fabricantes europeos, en primer lugar para red telefónica básica y en los últimos tiempos para telefonía digital fija (RDSI) y móvil (GSM). Actualmente, conviven ambos tipos de criptófonos, aunque los nuevos desarrollos suelen ser de tipo digital. Se puede afirmar que los criptófonos analógicos siguen teniendo su campo de aplicación, aunque la seguridad que ofrecen los criptófonos digitales es muy superior.

## III. POLÍTICA Y ORGANIZACIÓN

## 5. POLÍTICA DE SEGURIDAD

### 5.1. POLÍTICAS DE SEGURIDAD

177. El término **política de seguridad** hace referencia al conjunto de requisitos definidos por los responsables directos o indirectos de un entorno, que indica en términos generales qué está y qué no está permitido en la Organización. Así, constituye una declaración de intenciones de alto nivel que identifica responsabilidades y establece los objetivos para una protección apropiada y consistente de todos los activos de la Organización. La implementación de la política busca reducir el riesgo corporativo en su conjunto y, en el caso de los activos de información, reducir la probabilidad de que accidental o intencionadamente se divulgue, modifique, destruya o haga mal uso de los datos.
178. La política de seguridad debe describir QUÉ se intenta proteger y POR QUÉ se debe hacer, sin entrar a detalles acerca del CÓMO, que corresponden a un plan de implementación o a refinamientos de la política: al tratar la política de términos generales, tal y como se ha indicado, aplicables a situaciones o recursos muy diversos, suele ser necesario refinar los requisitos de la política para convertirlos en indicaciones precisas de qué es lo permitido y lo denegado en cierto ámbito de la Organización, lo que en ocasiones se denomina política de aplicación específica. Adicionalmente, una vez establecida la política se debe planificar su revisión periódica en la Organización, ya que las necesidades y requisitos cambiarán con el tiempo y las normas establecidas pueden volverse demasiado estrictas o, por el contrario, demasiado relajadas.
179. Uno de los objetivos principales a la hora de establecer una política de seguridad es reducir los riesgos todo lo posible, implementando adecuadamente las diferentes medidas de seguridad que implantan los especificados en la política de alto nivel. El incremento exponencial del uso de las nuevas tecnologías en las Organizaciones, y la cada vez mayor dependencia de los sistemas de información, hacen aumentar la importancia de la disponibilidad de dichos sistemas de información, y de la integridad y confidencialidad de los datos que éstos gestionan. Si bien este incremento aporta innumerables beneficios, también introduce riesgos considerables que es necesario tratar correctamente en la Organización.
180. Aunque la tecnología evoluciona de forma vertiginosa y a pesar de lo cambiante del entorno, los requisitos de seguridad que una política debe contemplar no han cambiado:
- Disponibilidad.** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
  - Utilidad.** Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
  - Integridad.** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
  - Autenticidad.** El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.



- e. **Confidencialidad.** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- f. **Posesión.** Los propietarios de un sistema han de ser capaces de controlarlo en todo momento. Perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

#### 5.1.1. POLÍTICA GENERAL O CORPORATIVA

- 181. Toda Organización debe definir un marco general de políticas de seguridad para administrar los riesgos asociados al procesamiento de información y por medio del cual se orientarán todas las acciones a seguir por parte de todos sus integrantes.
- 182. La información puede existir en muchas formas (impresa, escrita en papel, almacenada electrónicamente, transmitida usando medios electrónicos, videos, conversaciones, etc.) pero con independencia de la forma que la información tome, ésta siempre debe ser protegida adecuadamente.
- 183. La seguridad de la información debe orientarse a la preservación de la confidencialidad, integridad y disponibilidad. La administración de la seguridad de la información requiere, como mínimo, participación de todo el personal de la Organización.

#### 5.1.2. POLÍTICAS SOBRE ASPECTOS DE SEGURIDAD

- 184. Se constituyen en un documento que cubre todas las decisiones administrativas, intenciones, definiciones y reglas relacionadas con la seguridad de la información en un momento determinado. Estas políticas determinan el nivel mínimo aceptable de seguridad y establecen los criterios de medición de resultados.
- 185. Con todo ello se consigue un marco de trabajo de manera formal, y ayuda a su vez a proveer el fundamento para las diferentes guías, estándares y procedimientos de seguridad de la información que deben ser tenidos en cuenta.

#### 5.1.3. POLÍTICAS ESPECÍFICAS

- 186. Las políticas específicas son documentos que describen la implantación funcional de la política de seguridad de la información en un área o categoría de tecnología específica. Es una guía que traduce los objetivos estratégicos de la política de seguridad de la información a un tipo específico de tecnología o proceso de soporte.

### 5.2. SEGURIDAD DE LOS SISTEMAS

- 187. La política de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) como conjunto de normas, planes, procedimientos y productos no se ocupa directamente de la protección de la información sino de que existan las condiciones de seguridad suficientes en los sistemas y tecnologías que manejan ésta. La política STIC está orientada a proporcionar los conocimientos, productos y procedimientos de garantía, relacionados con las

Tecnologías de la Información y Comunicaciones a los responsables de la protección de la información.

188. Lógicamente, el grado con el que se apliquen las medidas de seguridad proporcionará diferentes niveles de protección que serán directamente proporcionales a los recursos a emplear. En general, se considera que la seguridad está aplicada siempre en función de la importancia de la disponibilidad, integridad y confidencialidad de la información o la disponibilidad e integridad de los propios sistemas.
189. Todos los sistemas que manejen información clasificada deberán disponer de un conjunto equilibrado de servicios de seguridad que permitan alcanzar los objetivos de seguridad requeridos y protejan los sistemas de forma adecuada. Estos servicios de seguridad permitirán, cuando sea apropiado, lo siguiente:
  - a. Identificar y autenticar al personal con acceso autorizado.
  - b. Controlar los accesos a la información en función de la necesidad de conocer.
  - c. Verificar la integridad y el origen de la información y de los elementos del sistema.
  - d. Mantener la integridad de la información y de los elementos del sistema.
  - e. Garantizar y verificar el funcionamiento de los mecanismos de seguridad del sistema.
  - f. Registrar y auditar la actividad de los usuarios del Sistema.
  - g. Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información o a la integridad y disponibilidad del sistema que la soporta.

### 5.3. MODOS SEGUROS DE OPERACIÓN

190. Los sistemas que manejen información clasificada deben funcionar de acuerdo a unos determinados modos seguros de operación:
  - a. **Modo dedicado:** es aquel en el que todo el personal con acceso al sistema está autorizado para acceder al nivel más alto de clasificación de la información manejada por el mismo y además posee la misma necesidad de conocer. Con estas premisas, la separación de los datos no es un requisito del sistema.
  - b. **Modo unificado a nivel superior:** es aquel en el que todo el personal con acceso al sistema está autorizado para acceder al nivel más alto de clasificación de la información manejada por el mismo, pero no tienen la misma necesidad de conocer; dicha necesidad de conocer se establece mediante procesos informales o de forma individual. El sistema realiza de manera fiable la separación de los datos y dispone de control de acceso selectivo a la información conforme a la diferente necesidad de conocer.
  - c. **Modo compartimentado:** es aquel en el que todo el personal con acceso al sistema está autorizado para acceder a nivel más alto de clasificación

de la información manejada por el sistema pero no todos los individuos con acceso al sistema tienen una autorización formal para acceder a toda la información manejada por el sistema; esta autorización formal implica una gestión centralizada y formalizada para el control de accesos, a diferencia de los criterios individuales de concesión.

- d. **Modo multinivel:** es aquel en el que un sistema maneja información con diferentes grados de clasificación. Permite el acceso selectivo y simultáneo al personal autorizado con diferentes grados de clasificación de la información y distinta necesidad de conocer. El sistema realiza de manera fiable la completa separación de los datos y el control de acceso selectivo.
191. Los controles físicos, de personal y de procedimientos deben cumplir los requisitos impuestos para el mayor grado de clasificación de la información almacenada, con independencia del modo seguro de operación.

#### 5.4. LA PROBLEMÁTICA DE SEGURIDAD

192. Con frecuencia se suele decir que la seguridad de una Organización se basa en tres grandes pilares: personas, procesos y tecnología. En cada uno de ellos se encuentran habitualmente problemas genéricos que son compartidos por diferentes organizaciones o administraciones y cuya identificación particular constituye el hito inicial para la planificación de la seguridad, tal y como se verá en el punto siguiente.
193. Desde el punto de vista de los **procesos** existen problemas estructurales de base en muchas organizaciones. Es especialmente habitual la inexistencia de estructuras diseñadas desde el punto de vista de la seguridad, lo que ya de entrada motiva que no estén formalmente definidas ni las funciones ni las responsabilidades relativas a la seguridad. A su vez esta situación implica que nadie asuma como responsabilidad el mitigar los riesgos de la Organización a partir de un análisis correcto (esto podría incluso verse como una dificultad para el proceso de negocio o de servicio por parte de quien lo proponga), por lo que las salvaguardas aplicadas suelen ser iniciativas aisladas en la Organización, promovidas por un departamento concreto (informática, seguridad...) y sin la coherencia necesaria para considerarlas alineadas con las necesidades y los riesgos corporativos. Incluso, en determinadas ocasiones, dichas salvaguardas son puramente reactivas, resultado de riesgos muy altos –o ya materializados en el pasado- que dificultan enormemente el servicio y se mitigan por la propia supervivencia de la Organización.
194. Al hablar de la problemática asociada a las **personas**, que como se suele decir son el eslabón más débil en la cadena de la seguridad, se aprecia en primera instancia una falta de concienciación en la protección de la información corporativa, motivada quizás por el desconocimiento de los riesgos a los que dicha información está expuesta. Esta falta de concienciación motiva de nuevo que la seguridad no esté contemplada en la estructura corporativa y potencia la reactividad: se toman medidas –se aplican salvaguardas- cuando un impacto significativo se materializa en la organización.

195. Finalmente, desde el punto de vista de la **tecnología**, en ocasiones se considera a las herramientas de seguridad como una panacea capaz de mitigar cualquiera de los riesgos corporativos. Dichas herramientas deben ser consideradas un simple soporte que implementa la Organización y la gestión de la seguridad definida por las personas. Además de que no se puede confiar la seguridad en exclusiva a determinadas herramientas TI, éstas no cubren todas las necesidades corporativas en la materia, llegando en ocasiones a generar una falsa sensación de seguridad que puede ser incluso peor que la inexistencia de controles tecnológicos.

## 5.5. PLANIFICACIÓN DE LA SEGURIDAD

196. Una vez identificados los problemas hay que saber cómo abordar la seguridad en la Organización. El plan de seguridad debe ser un proyecto que desarrolle los objetivos de seguridad de la Organización a largo plazo, siguiendo un ciclo de vida completo desde la definición hasta la implementación y revisión.
197. La política de seguridad debe definir QUÉ se quiere hacer en materia de seguridad en la Organización, para a partir de ésta decidir mediante un adecuado plan de implementación CÓMO se alcanzarán en la práctica los objetivos fijados. La política de seguridad englobará pues los objetivos, conductas, normas y métodos de actuación además de la distribución de responsabilidades, ejerciendo como documento de requisitos para la implementación de los mecanismos de seguridad.
198. La política debe contemplar al menos la definición de funciones de seguridad, la realización de un análisis de riesgos, la definición de normativa y procedimientos, la definición de planes de contingencia y la definición del plan de auditoría. A partir de la política de seguridad se podrá definir el plan de implementación, en el que se contemplará el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.
199. Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad:
- a. La política debe ser aprobada por la autoridad competente, de tal manera, que se asegure su cumplimiento y la asignación de recursos, realizando revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno.
  - b. La política de seguridad y el plan de implementación están íntimamente relacionados:
  - c. La política de seguridad define el plan de implementación, ya que su ejecución debe ser un fiel reflejo de los procedimientos y normas establecidos en la política.
  - d. El plan de seguridad debe ser revisado para adaptarse a las nuevas necesidades del entorno, los servicios que vayan apareciendo y a las aportaciones que usuarios, administradores, etc. vayan proponiendo en función de su experiencia. Los plazos de revisión deben estar fijados y permitir además revisiones extraordinarias en función de determinados eventos (por ejemplo, incidentes).

- e. El plan de implementación debe ser verificado para tener la certeza de su adecuación a las normas.
- f. El plan de implementación debe realimentar a la política de seguridad. La experiencia, los problemas de implantación, las limitaciones y los avances tecnológicos, etc. permitirán que la política pueda adecuarse a la realidad, evitando la inoperancia por ser demasiado utópica y la mejorarán cuando el progreso lo permita.

#### 5.5.1. SERVICIOS DE SEGURIDAD

200. Para proteger la información se utilizan los servicios de seguridad, que constituyen el resultado de aplicar uno o varios mecanismos de seguridad ofreciendo garantías de confianza.
- a. **Autenticación**: permiten al receptor de un mensaje estar seguro de la identidad del emisor y que la comunicación es auténtica. Asegura que el usuario y la información transmitida son auténticos.
  - b. **Control de Accesos**: protege los recursos del Sistema contra su utilización no autorizada. Los servicios de control de acceso están íntimamente ligados a los de autenticación.
  - c. **Confidencialidad**: evita el acceso no autorizado a la información, protegiéndola de revelaciones deliberadas o accidentales no permitidas.
  - d. **Integridad**: protege los datos de alteraciones no autorizadas, detectando cualquier modificación, inserción, eliminación o retransmisión. Comprueba que la información no ha sido modificada sin autorización.
  - e. **No Repudio**: previenen que la entidad emisora y receptora nieguen haber enviado o recibido un mensaje. Cuando se recibe un mensaje no sólo es necesario poder identificar de forma unívoca al remitente sino que éste asuma todas las responsabilidades derivadas de la información que haya podido enviar. En este sentido, es fundamental impedir el repudio, es decir, la negativa por parte de una entidad de haber participado en una comunicación o parte de ella.

Ataques Servicios			
	Disponibilidad	Confidencialidad	Integridad
<b>Autenticación</b>		X	X
<b>Control accesos</b>		X	X
<b>Confidencialidad</b>		X	
<b>Integridad</b>			X
<b>No repudio</b>	X		

#### 5.5.2. MECANISMOS DE IMPLEMENTACIÓN

201. Los mecanismos de seguridad constituyen técnicas o funcionalidades de detección y prevención de amenazas. Por el ámbito de su aplicación se pueden dividir en dos grandes grupos: los mecanismos específicos y los generales. Los mecanismos **específicos** se aplican a un determinado nivel de la capa OSI

(físico, enlace, red, transporte, sesión, presentación y aplicación) del sistema para implementar un servicio; son los siguientes:

- a. Cifrado: se transforman los datos para que sólo sean inteligibles a los usuarios autorizados (criptosistemas simétricos o asimétricos).
- b. Firma digital: a la información se le añaden unos identificadores que sólo pueden ser generados por un usuario concreto, además no permiten la modificación de la información por otros usuarios (funciones hash).
- c. Intercambio de autenticación: corrobora que la identidad de una entidad (origen/destino) es la deseada.
- d. Control de accesos: permite que sólo aquellos usuarios autorizados accedan a los correspondientes recursos. Los usuarios deben estar previamente autenticados.
- e. Integridad de datos: garantiza que los datos no puedan ser modificados durante su transmisión por la red. Añade identificadores a la información que permiten detectar si ésta ha sido modificada.
- f. Tráfico de relleno: se inyecta tráfico sin información en las redes para confundir a los posibles observadores de la red.
- g. Control de encaminamiento: transmisión de información por ciertas rutas o caminos en función del nivel de seguridad requerido. Se utilizan sistemas de encaminamiento para proteger la información.
- h. Notariado: una tercera persona física o jurídica confirma la procedencia e integridad de los datos. Se recogen determinadas propiedades de los datos transmitidos para que las posea una tercera parte.

Servicios Mecanismos	Autenticación	Control de Accesos	Confidencialidad	Integridad	No repudio
Cifrado	X		X	X	
Firma Digital	X			X	X
Integridad				X	X
Control Accesos		X			
Tráfico Relleno			X		
Encaminamiento			X		
Notariado					X

202. La mayoría de estos mecanismos utilizan la criptología para su implementación (cifrado, firma digital, control de accesos e integridad).
203. El segundo tipo de mecanismos de seguridad son los **generales**, aquellos que se aplican al sistema para cumplir la política general:
  - a. Funcionalidad de confianza: el sistema de seguridad está libre de ataques.
  - b. Etiquetas: clasifica la información por niveles de seguridad (SECRETO, RESERVADO, CONFIDENCIAL, etc...).
  - c. Auditorías: almacena las acciones realizadas sobre el Sistema.

- d. Detección de eventos: detecta acciones peligrosas dentro del Sistema.
- e. Recuperación ante desastres: políticas para recuperar la información después de un incidente (copias de respaldo, etc...).
- f. Políticas de personal: formación/concienciación y normativas relativas a las actuaciones del personal.

## 5.6. DESARROLLO NORMATIVO

204. La política de seguridad como declaración de intenciones de alto nivel deberá tener un desarrollo normativo basado en Procedimientos, Normas, Instrucciones Técnicas y Guías:
- a. Los **Procedimientos STIC** establecerán el marco común de actuación en los procesos de valoración y acreditación de las TIC y cualquier otro campo que se considere.
  - b. Las **Instrucciones Técnicas STIC** atenderán a un objetivo de seguridad específico. Son de obligado cumplimiento en su ámbito de actuación y establecerán los requisitos de seguridad generales a implementar en un sistema. Son responsabilidad de la Autoridad emisora y serán vinculantes dentro del ámbito que compete a cada Autoridad.
  - c. Las **Normas STIC** son reglas generales que se deben seguir o a las que se deben de ajustar las conductas, tareas o actividades de las personas y Organizaciones en relación con la protección de la información cuando es manejada por un sistema. Estas normas establecerán las directrices para la redacción de la documentación de seguridad, la realización de análisis de riesgos, la ejecución de inspecciones STIC o cualquier otra que se considere oportuna. Son responsabilidad de la Autoridad emisora y serán vinculantes dentro del ámbito que compete a cada Autoridad.
  - d. Las **Guías STIC** son recomendaciones o informaciones relativas a temas concretos de seguridad de los sistemas. Estas guías establecerán las configuraciones mínimas de seguridad de los diferentes elementos de un Sistema, recomendaciones de uso u otro tipo de recomendaciones.



## 6. ORGANIZACIÓN Y GESTIÓN DE SEGURIDAD

### 6.1. INTRODUCCIÓN

205. El mantenimiento y gestión de la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones van íntimamente ligados al establecimiento de una **Organización de Seguridad**, mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los Sistemas y la implantación de una estructura que las soporte.
206. Es responsabilidad de cada organismo establecer su propia Organización de Seguridad acorde con sus necesidades y limitaciones. La Autoridad responsable de la acreditación del Sistema determina la aprobación de cualquier estructura de seguridad que sustenta al Sistema y que permite el cumplimiento de los requisitos de seguridad necesarios para manejar la información que soporta.

### 6.2. ORGANIZACIÓN DE SEGURIDAD

207. La Organización de la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) está constituida por las Autoridades responsables del establecimiento y aplicación de los procedimientos y normas STIC en el Sistema.
208. Dentro de cada Organización STIC se establecen dos tipos fundamentales de estructuras:
- a. Estructura de Seguridad de las TIC de la Organización: responsable de establecer y aprobar los requisitos de seguridad para el Sistema además de verificar y supervisar la correcta implementación y mantenimiento de los mismos.
  - b. Estructura TIC del Sistema: responsable de la implementación y mantenimiento de los requisitos de seguridad aprobados para el Sistema por la Alta Dirección.

### 6.3. ESTRUCTURA TIC DEL SISTEMA

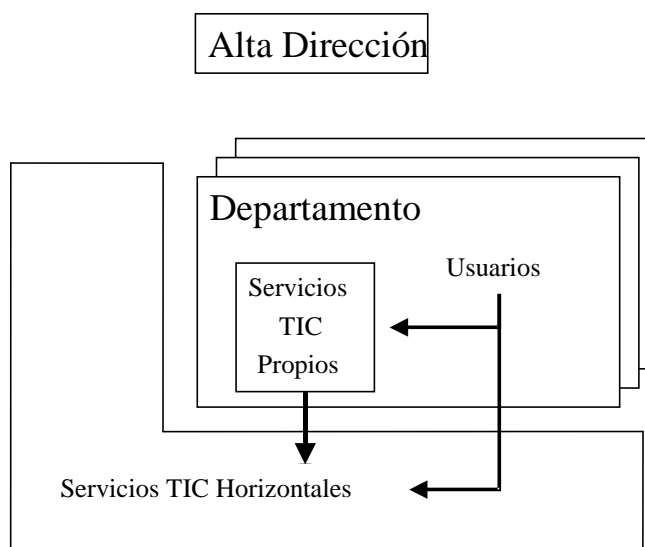
209. Las Organizaciones, públicas o privadas, suelen diferenciar entre una Alta Dirección y una serie de Unidades Operativas, Áreas o Departamentos<sup>1</sup>; cada uno de estos departamentos tiene un responsable que informa a la Alta Dirección, y pueden disponer de recursos TIC propios, para sus usuarios, o limitarse a utilizar los servicios TIC horizontales. Generalmente las áreas con requisitos técnicos muy concretos (por ejemplo, Departamentos de Seguridad o Departamentos de Producción) utilizarán recursos propios y horizontales, mientras que las áreas con unos requisitos generalistas utilizarán en exclusiva los servicios horizontales (Administración, Atención al cliente...).

---

<sup>1</sup> En el ámbito privado es frecuente hablar de “Áreas de Negocio”, mientras en la administración pública se suelen denominar “Servicios”. La terminología es mucho más variada en la práctica.

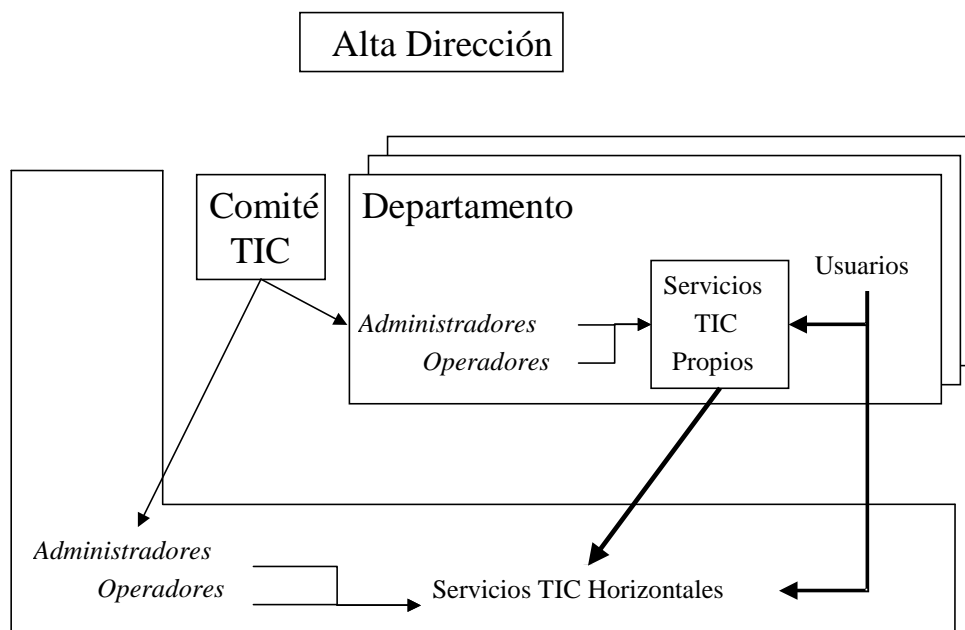
210. En teoría, los servicios TIC pueden organizarse según un simple esquema donde:

- a. Los responsables de los Departamentos imponen las necesidades de la Organización.
- b. Los responsables de los Sistemas TIC proporcionan soluciones eficaces y eficientes a las necesidades planteadas.



#### 6.3.1. COMITÉ TIC

211. En la práctica es muy conveniente coordinar las actividades TIC por medio de un Comité específico en el que se coordinan adquisiciones y desarrollos, decidiendo inversiones y controlando el gasto, así como servicios para evitar disfunciones y maximizar el uso y la eficiencia de los mismos; este Comité no es técnico, pero recaba del personal técnico de los Departamentos la información pertinente para tomar decisiones.



212. El Comité TIC delega en una red de administradores y operadores TIC las tareas decididas:

- a. Los administradores se encargan de la instalación y configuración de aplicaciones, equipos y comunicaciones
- b. Los operadores se encargan de la operación continua de los servicios TIC.

### 6.3.2. ADMINISTRADORES STIC

213. Los administradores STIC son los responsables de la implantación, configuración y mantenimiento de los servicios de seguridad relacionados con las TIC; pueden ser las mismas personas que cumplen el papel de administradores del sistema (opción preferible siempre que sea posible) o tratarse de personas diferentes.

214. Existirán administradores STIC de servicios horizontales, pudiendo aparecer administradores STIC asignados a áreas que disponen de un Responsable STIC Delegado. Entre sus funciones destacan:

- a. Ejecutar los procedimientos que les competan en cuanto a actividad rutinaria.
- b. Ejecutar los procedimientos que les sean asignados en la resolución de incidentes recibidos de los operadores y usuarios.

215. Los administradores deben informar de cualquier inseguridad o debilidad, real o supuesta, que perciban durante la realización de sus tareas. Se informará al Responsable de Seguridad inmediato superior.

### 6.3.3. OPERADORES

216. Son los responsables de la operación diaria de los servicios de seguridad relacionados con las TIC; existirán operadores de servicios horizontales, pudiendo aparecer operadores asignados a áreas que disponen de un Responsable STIC Delegado.
217. Los operadores reciben instrucciones e informan a su Responsable de Seguridad inmediato superior. Sus funciones son las siguientes:
  - a. Ejecutar los procedimientos que les competan en cuanto a actividad rutinaria.
  - b. Recibir en primera instancia las incidencias que se produzcan, notificadas por usuarios.
  - c. Resolver las incidencias que por procedimiento les competan y elevar al Administrador STIC correspondiente las que les excedan, siempre ajustándose a procedimiento. Las incidencias para las que no exista procedimiento de reacción se trasladarán al Responsable de Seguridad inmediato superior para su tratamiento.
218. Los operadores deben reportar cualquier inseguridad o debilidad, real o supuesta, que perciban durante la realización de sus tareas. Se informará al Responsable de Seguridad inmediato superior.

#### 6.3.4. USUARIOS

219. Los usuarios se relacionan con los servicios TIC para cumplir sus obligaciones laborales. En cada Sistema, además tendrán cabida las siguientes figuras:
  - a. **Administrador del Sistema:** tiene por misión realizar las tareas de administración del Sistema. Son los responsables de la implantación, configuración y mantenimiento de los servicios TIC y ejecutarán los procedimientos que les competan en cuanto a actividad rutinaria.
  - b. **Administrador de Red:** encargado de las tareas de administración de red, siendo responsable de aspectos de seguridad, como enrutamiento y filtrado, relativos a la infraestructura de red (enrutadores/switches, dispositivos de protección de perímetro, redes privadas virtuales, detección de intrusos, dispositivos trampa, etc.).
  - c. **Usuarios del Sistema:** constituyen el personal autorizado para acceder al Sistema utilizando las posibilidades que les ofrece el mismo.
220. Los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del Sistema; por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio Sistema. Para mitigar este riesgo, los usuarios deben estar debidamente informados de sus obligaciones y responsabilidades, así como haber sido instruidos para la labor que desempeñan.
221. Los usuarios del Sistema son responsables entre otras cosas de:
  - a. Conocer los procedimientos que les competen,.
  - b. Asegurarse de que están preparados adecuadamente para llevar a cabo operaciones en el Sistema, en particular las correspondientes a la gestión

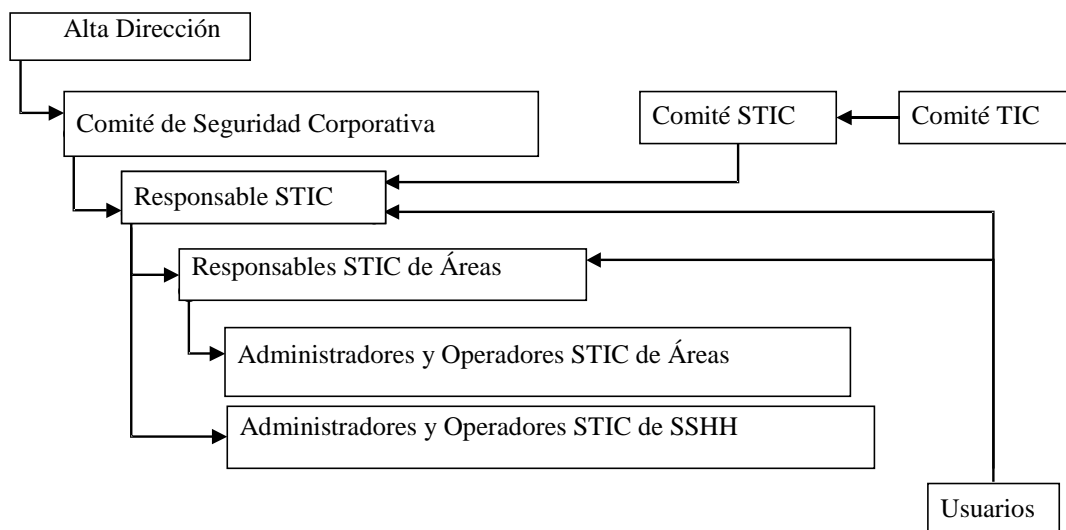
de mecanismos de identificación y al procedimiento de gestión de incidentes.

- c. Informar de cualquier incidente de seguridad o acontecimiento inusual que sea observado durante la operación de su Sistema.

#### 6.4. ESTRUCTURA STIC DE LA ORGANIZACIÓN

- 222. La seguridad necesita estar coordinada tanto o más que los servicios TIC, tanto para racionalizar el gasto y la inversión como para evitar disfunciones que introduzcan debilidades de seguridad, al ofrecer el Sistema puntos débiles donde pudieran ocurrir accidentes o se pudieran perpetrar ataques.
- 223. La Seguridad de las TIC (STIC) debe estar coordinada en un Comité STIC y debe existir un responsable STIC. Este **Comité STIC** no es un comité técnico, pero recabará regularmente del personal técnico, propio o externo, la información pertinente para tomar decisiones. El Comité STIC debe estar perfectamente coordinado con el Comité TIC, siendo lo idóneo que la representación formal de los Departamentos en dichos comités sea la misma persona, sin perjuicio de que la representación real se delegue en especialistas diferentes, que informen a un único representante por Departamento.
- 224. El **Responsable STIC** es el Secretario del Comité STIC y como tal:
  - a. Convoca las reuniones del Comité STIC.
  - b. Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
  - c. Es responsable de la ejecución directa o delegada de las decisiones del Comité.
- 225. Los responsables STIC pueden contar con responsables delegados o intermedios centrados en un Departamento, un aspecto tecnológico o un proyecto concreto, apareciendo:
  - a. Responsables STIC departamentales.
  - b. Responsables de la seguridad de determinadas aplicaciones informáticas (bases de datos, sistemas operativos, etc.).
  - c. Responsables de la seguridad de determinado equipamiento (equipos móviles o sedes remotas).
  - d. Responsables de la seguridad de las redes de comunicaciones.
  - e. Responsables de seguridad de un proyecto de adquisición o desarrollo que termina con el proyecto y que luego pasa a los responsables de explotación.
  - f. Responsables de seguridad en las relaciones con otras Organizaciones.
- 226. En teoría los diferentes roles STIC se limitan a una jerarquía simple: el Comité STIC da instrucciones al Responsable STIC, que a su vez se encarga de supervisar que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la

Organización. No obstante, en la práctica la situación es menos simple y existe también un flujo inverso en el que administradores, operadores y usuarios transmiten incidencias, debilidades (reales o supuestas) e informes de explotación para que se tomen las medidas preventivas o correctivas que el Comité STIC o el Responsable STIC por delegación, consideren oportunas. Adicionalmente, el Comité STIC también escuchará las inquietudes de la Alta Dirección y del Comité TIC e informará a todos ellos del estado de seguridad de las TIC.



227. En grandes Organizaciones aparecerá una nueva figura entre la Alta Dirección y el Comité TIC: se trata del Comité de Seguridad Corporativa con su propio Secretario, el Responsable de Seguridad Corporativa. El Responsable STIC queda como miembro del Comité de Seguridad Corporativa junto con otros responsables de otras áreas, tales como:
- Responsables de la seguridad de instalaciones y áreas (seguridad física).
  - Responsables de la seguridad de la información.
  - Responsables de seguridad industrial.
  - Responsables de seguridad operacional.
228. En este tipo de organizaciones es muy importante la figura del Responsable de Seguridad Corporativa (con el cargo que corresponda en cada caso), un punto único de responsabilidad en todo lo que respecta a la seguridad de la Organización desde el punto de vista de protección operativa del negocio o servicio, siguiendo las tendencias actuales que hablan de **convergencia de la seguridad**. La convergencia proporciona a las organizaciones unos beneficios claros en materia de seguridad, como son la visión holística del riesgo, la reducción de costes o la existencia de un punto único de referencia en la materia. Viene catalizada por diferentes factores, entre los que es necesario destacar la convergencia o la existencia de amenazas comunes en todos los frentes. Por contra, a la hora de converger se presentan barreras que en muchos casos son difíciles de superar, siendo la mayor de todas ellas la diferencia cultural que existe entre las “seguridades” particulares en cada caso.

#### 6.4.1. ALTA DIRECCIÓN

229. La Alta Dirección es responsable de que la Organización alcance sus objetivos a corto, medio y largo plazo. Debe respaldar explícita y notoriamente las actividades STIC en la Organización y expresa sus inquietudes al Comité de Seguridad Corporativa a través del Responsable de Seguridad Corporativa. Entre sus funciones destacan las siguientes:

- a. Aprueba la Política de Seguridad de la Organización.
- b. Aprueba presupuestos presentados por el Comité de Seguridad Corporativa cuando sobrepasen una cantidad determinada.

#### 6.4.2. COMITÉ DE SEGURIDAD CORPORATIVA

230. Este comité centraliza, con el Director de Seguridad Corporativa al frente, toda la gestión de la seguridad de la Organización en sus diferentes ámbitos con objeto de proteger el servicio de forma correcta, completa y eficiente. Sus funciones serán las siguientes:

- a. Coordina todas las funciones de seguridad de la Organización.
- b. Vela por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- c. Vela por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- d. Es responsable de la elaboración de la Política de Seguridad Corporativa, que será aprobada por la Alta Dirección.
- e. Aprueba las políticas de seguridad de las diferentes áreas, que serán presentadas por los correspondientes responsables de seguridad.
- f. Coordina y aprueba las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad. Los presupuestos elevados serán transmitidos a la Alta Dirección para su aprobación. Los responsables de seguridad se encargarán de llevar a cabo un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- g. Escucha las inquietudes de la Alta Dirección y las transmite a los Responsables de Seguridad pertinentes. De estos últimos recaba respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.
- h. Recaba de los Responsables de Seguridad informes regulares del estado de seguridad de la Organización y de los posibles incidentes; estos informes se consolidan y resumen para la Alta Dirección.
- i. Coordina y da respuesta a las inquietudes transmitidas a través de los Responsables de Seguridad.
- j. Debe definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.



#### 6.4.3. RESPONSABLE DE SEGURIDAD CORPORATIVA

231. La figura del Responsable de Seguridad Corporativa es el máximo exponente de la seguridad en la Organización. Debe ser un perfil capaz de gestionar el riesgo corporativo desde un punto de vista global, convirtiéndose en la referencia corporativa en materias de seguridad y en el punto de contacto único de la Organización en este ámbito. Entre sus responsabilidades están las siguientes:
- a. Es el responsable último de la seguridad de la Organización.
  - b. Es responsable, junto con los diferentes Responsables de Seguridad, de estar al tanto de cambios normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la Organización, debiendo informarse de las consecuencias para las actividades de la Organización, alertando al Comité de Seguridad Corporativo y proponiendo las medidas oportunas de adecuación al nuevo marco.
  - c. Actúa como Secretario del Comité de Seguridad Corporativa.
  - d. Convoca al Comité de Seguridad Corporativa, recopilando la información pertinente.
  - e. Escucha las inquietudes de la Alta Dirección y de los responsables de seguridad y las incorpora al orden del día para su discusión en las reuniones del Comité de Seguridad Corporativa.
  - f. Es el responsable de la toma de decisiones día a día entre las reuniones del Comité de Seguridad Corporativa. Estas decisiones serán respuesta a propuestas de los responsables de seguridad, velando por la unidad de acción y la coordinación de actuaciones, en general y en especial en caso de incidencias que tengan repercusión fuera de la Organización y en caso de desastres.
  - g. En caso de desastre se incorporará al Comité de Crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad de la Organización.

#### 6.4.4. COMITÉ STIC

232. Este Comité es el órgano director de la seguridad de las TIC en la Organización, manteniendo a través del responsable STIC una relación directa con el Comité de Seguridad Corporativa para aportar a éste todo lo relacionado con la seguridad TIC que pueda ser significativo para la protección de la Organización en su conjunto. Entre sus responsabilidades destacan:
233. Es responsable de la redacción de la Política de Seguridad de las TIC, que será presentada al Comité de Seguridad Corporativa para su aprobación.
- a. Coordinación de todas las actividades relacionadas con la seguridad de las TIC.
  - b. Creación y aprobación de las normas que enmarcan el uso de los servicios TIC.
  - c. Aprobación de los procedimientos de actuación en lo relativo al uso de los servicios TIC.

- d. Aprobación los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.
234. El Comité STIC se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse mediante grupos de trabajo especializados internos, externos o mixtos, consultoría externa o asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias, por poner sólo unos ejemplos.

#### 6.4.5. RESPONSABLE STIC

235. El Responsable STIC es el máximo exponente de la seguridad TIC en la Organización actuando como Secretario del Comité STIC, representando este ámbito en el Comité de Seguridad Corporativa y reportando directamente al Responsable de Seguridad Corporativa. Entre las funciones del Responsable STIC están las siguientes:
- a. Actúa como Secretario del Comité STIC, trasladando al Comité de Seguridad Corporativa las decisiones adoptadas por el Comité STIC.
  - b. Es informado de los cambios significativos en la tecnología o el entorno en el que vive la Organización, analizando las consecuencias para las actividades STIC, alertando al Comité de STIC en caso de considerarse oportuno y proponiendo las medidas oportunas de adecuación al nuevo marco.
  - c. Es responsable de la redacción de los procedimientos de actuación en lo relativo al uso de los servicios TIC desde el punto de vista de la seguridad (la redacción de los procedimientos puede delegarse en los Responsables STIC de Áreas); estos procedimientos se presentarán al Comité STIC para su aprobación.
  - d. Es responsable de la correcta ejecución de las instrucciones emanadas del Comité STIC, ejecución que materializará transmitiendo instrucciones a los administradores y operadores STIC, directamente o a través de los Responsables STIC de Áreas.
  - e. Es responsable de la presentación regular de informes sobre el estado de seguridad de los servicios TIC. Estos informes se presentarán al Comité STIC, elaborando adicionalmente un informe ejecutivo para ser presentado al Comité de Seguridad Corporativa.
  - f. Es responsable de la preparación de informes en caso de incidentes excepcionalmente graves y en caso de desastres. Se presentará un informe detallado al Comité STIC y un informe ejecutivo al Comité de Seguridad Corporativa.
  - g. Es responsable de la elaboración de un Análisis de Riesgos de los sistemas de las TIC, análisis que será presentado al Comité STIC para su aprobación. Este análisis deberá actualizarse regularmente (cada 6 meses) y se presentará al Comité de Seguridad Corporativa para ser incluido en el Análisis de Riesgos Corporativo, coordinado por el Responsable de Seguridad Corporativa.

- h. Es responsable de que se ejecuten regularmente verificaciones de seguridad según un plan predeterminado y aprobado por el Comité STIC. Los resultados de estas inspecciones se presentarán al Comité STIC para su conocimiento y aprobación y un resumen ejecutivo será presentado al Comité de Seguridad Corporativa; si como resultado de la inspección aparecen incumplimientos, el Responsable STIC propondrá medidas correctoras que presentará al Comité STIC para su aprobación, responsabilizándose de que sean llevadas a cabo.
- i. Es responsable de la elaboración y seguimiento del Plan de Seguridad, en el que intervendrán los Responsables STIC de Áreas. Este plan será presentado al Comité STIC para su aprobación y al Comité de Seguridad Corporativo para su conocimiento y aprobación.
- j. Elabora para su aprobación por el Comité STIC los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de las TIC.
- k. Es responsable de la identificación de tareas de administración y operación que garanticen la satisfacción de los criterios y requisitos de segregación de tareas impuestos por el Comité de Seguridad Corporativa.
- l. Es el interlocutor oficial en comunicaciones con otras Organizaciones en el ámbito de la Seguridad TIC, tarea que puede asumir personalmente o delegar según las circunstancias, pero nunca debe haber más de un interlocutor.
- m. Es el responsable de coordinar la respuesta ante incidentes que desborden los casos previstos y procedimentados. Es el responsable de coordinar la investigación forense relacionada con incidentes que se consideren relevantes.

#### 6.4.6. RESPONSABLES STIC DELEGADOS

236. En aquellos casos en que existan varios Sistemas que por su complejidad, diversidad, distribución, etc. requieran de una mayor dedicación, se podrán nombrar Responsables STIC Delegados cuyo ámbito de responsabilidad se limitará al área TIC para el que son designados. Estos responsables dependen funcionalmente del Responsable STIC que será, en última instancia, responsable de su adecuado desempeño. Entre las funciones de los Responsables STIC Delegados están las siguientes:
- a. Elaborar procedimientos de actuación en el área que les compete, siguiendo las instrucciones recibidas del Responsable STIC.
  - b. Elaborar informes regulares para el Responsable STIC sobre el estado de seguridad del área que les compete.
  - c. Elaborar informes detallados para el Responsable STIC de incidencias no rutinarias en el área que les compete.
  - d. Coordinar la adecuada competencia y formación continua de los administradores y operadores asignados a su área de competencia.

## 6.5. ANÁLISIS DE RIESGOS

237. En un entorno informático existen una serie de recursos (humanos, técnicos, de infraestructura...) que están expuestos a diferentes tipos de riesgos: los normales, aquellos comunes a cualquier entorno, y los excepcionales, originados por situaciones concretas que afectan o pueden afectar a parte de una Organización o a toda la misma, como la inestabilidad política en un país o una región sensible a terremotos. Para tratar de minimizar los efectos de un problema de seguridad se realiza un **análisis de riesgos**, término que hace referencia al proceso necesario para responder a tres cuestiones básicas sobre la seguridad:
- ¿Qué se quiere proteger?
  - ¿Contra quién o qué se quiere proteger?
  - ¿Cómo se puede proteger?
238. De esta forma, el análisis de riesgos es la herramienta a través de la cual se puede obtener una visión clara y priorizada de los riesgos a los que se enfrenta una Organización: tiene como propósito identificar los principales riesgos a los que una entidad está expuesta, ya sean desastres naturales, fallos en infraestructura o riesgos introducidos por el propio personal. En este sentido pretende identificar los riesgos más significativos que pueden afectar a la operativa de la Organización y priorizar medidas a implantar para minimizar la probabilidad de materialización de dichos riesgos o el impacto en caso de materializarse.
239. En la práctica existen dos aproximaciones para responder a estas cuestiones, una **cuantitativa** y otra cualitativa. La primera de ellas es con diferencia la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se basa en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del coste o las pérdidas en caso de que así sea; el producto de ambos términos es lo que se denomina coste anual estimado (EAC, *Estimated Annual Cost*), y aunque teóricamente es posible conocer el riesgo de cualquier evento (el EAC) y tomar decisiones en función de estos datos, en la práctica la inexactitud en la estimación o en el cálculo de parámetros hace difícil y poco realista esta aproximación.
240. El segundo método de análisis de riesgos es el **cualitativo**, de uso muy difundido en la actualidad. Es mucho más sencillo e intuitivo que el anterior, ya que ahora no entran en juego probabilidades exactas sino simplemente una estimación de pérdidas potenciales. Para ello se interrelacionan cuatro elementos principales: las amenazas, por definición siempre presentes en cualquier sistema, las vulnerabilidades, que potencian el efecto de las amenazas, el impacto asociado a una amenaza, que indica los daños sobre un activo por la materialización de dicha amenaza, y los controles o salvaguardas, contramedidas para minimizar las vulnerabilidades (controles preventivos) o el impacto (controles curativos). Por ejemplo, una amenaza sería un pirata que va a tratar de modificar la página web principal de la Organización. El impacto sería una medida del daño que causaría si lo lograra, una vulnerabilidad sería una configuración incorrecta del servidor que ofrece las páginas, y un control la reconfiguración de dicho servidor o el incremento de su nivel de parcheado. Con

estos cuatro elementos se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la Organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

241. En el ámbito de las Administraciones Públicas, a las que va destinada la presente guía CCN-STIC, es necesario referenciar la metodología de análisis de riesgos desarrollada desde el Consejo Superior de Informática (Ministerio de Administraciones Públicas) y denominada **MAGERIT** (Metodología de Análisis y GEstión de Riesgos de los sistemas de Información de las adminisTraciones públicas). Se trata de un método formal para realizar un análisis de riesgos y recomendar los controles necesarios para su minimización. MAGERIT se basa en una aproximación cualitativa que intenta cubrir un amplio espectro de usuarios genéricos gracias a un enfoque orientado a la adaptación del mecanismo dentro de diferentes entornos, generalmente con necesidades de seguridad y nivel de sensibilidad también diferentes.
242. Se han realizado dos versiones de MAGERIT. La primera de ellas data de 1997 y la versión vigente data de 2005. La versión 2 de la metodología está compuesta de tres libros:
  - a. El primero se denomina **Método** y describe las tareas a realizar para acometer proyectos de análisis y gestión de riesgos, aportando una guía para el desarrollo de análisis de riesgos, aspectos prácticos y consejos para facilitar la tarea.
  - b. El segundo libro, **Catálogo de elementos**, recoge el catálogo de elementos implicados en el análisis de riesgos tales como: una categorización de activos, las dimensiones aplicables (DICAT), criterios para valoración de activos como procesos de negocio o datos, catálogo de amenazas y un catálogo de medidas a implantar para mitigar los riesgos a los que están expuestos los sistemas de información. Por último indica cómo desarrollar un informe.
  - c. El tercer libro, **Guía de Técnicas**, proporciona técnicas para el análisis de riesgos tales como: algoritmos de análisis, árboles ataque, análisis coste-beneficio, diagramas de flujo, tablas de procesos o técnicas de trabajo.
243. En la página web del Consejo Superior de Informática se puede encontrar información más detallada acerca de esta metodología, así como algunos ejemplos de ejecución de la misma. Adicionalmente, de forma complementaria a MAGERIT, es obligatorio referenciar la herramienta **PILAR** (Procedimiento Informático Lógico de Análisis de Riesgos), una aplicación desarrollada en Java que implementa la segunda versión de la metodología MAGERIT y de amplia utilización en la Administración Pública española.
244. La herramienta permite la realización de análisis de riesgos bajo un enfoque tanto cualitativo como cuantitativo (empleando valores simbólicos o económicos respectivamente) y la realización de análisis de impacto en el ámbito de la continuidad de negocio. Se complementa con **PILAR Basic**, enfocada a su uso en PYMEs, que simplifica parcialmente la herramienta y rebaja el coste de

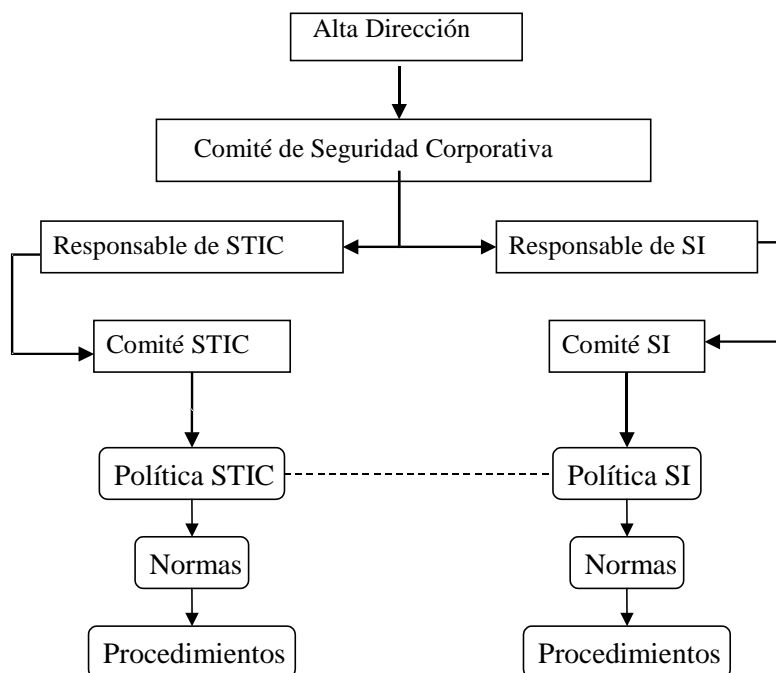
licencia y **MicroPILAR**, enfocado a facilitar y a automatizar el proceso de análisis de riesgos.

245. En cualquier caso, e independientemente de metodologías y herramientas, tras obtener mediante cualquier mecanismo los indicadores de riesgo en la Organización llega la hora de evaluarlos para tomar decisiones organizativas acerca de la gestión de la seguridad y sus prioridades. Por una parte está el riesgo calculado, resultante del análisis, y este riesgo calculado se ha de comparar con un cierto umbral (**umbral de riesgo**) determinado por la política de seguridad de la Organización. El umbral de riesgo puede ser o bien un número o bien una etiqueta de riesgo y cualquier riesgo calculado superior al umbral ha de implicar una decisión de reducción de riesgo. Si por el contrario el calculado es menor que el umbral, se habla de **riesgo residual**, y el mismo se considera asumible (no hay porqué tomar medidas para reducirlo). El concepto de asumible es diferente al de riesgo asumido, que denota aquellos riesgos calculados superiores al umbral pero sobre los que por cualquier razón (política, económica...) se decide no tomar medidas de reducción. Evidentemente, siempre se ha de evitar esta situación.
246. Una vez conocidos y evaluados de cualquier forma los riesgos a los que se enfrenta la Organización, se podrán definir las políticas e implementar las soluciones prácticas para minimizar sus efectos.

## 6.6. SEGURIDAD DE LA INFORMACIÓN

247. La seguridad de la información no es equivalente a la seguridad de las TIC, pero la relación correcta entre ambas es crítica debido a que buena parte de la información corporativa es gestionada (almacenada, transmitida, procesada...) por elementos tecnológicos de la Organización.
248. La clasificación de la información (como SECRETO, RESERVADO, CONFIDENCIAL o de DIFUSIÓN LIMITADA), la clasificación de la información de carácter personal (nivel alto, medio o bajo según la LOPD) u otros tipos de clasificaciones propios de la Organización y derivados de la política propia o de obligaciones regulatorias o sectoriales no se deciden por criterios TIC o STIC, pero una vez determinadas estas clasificaciones van a implicar una serie de requisitos sobre su manipulación mediante servicios TIC.
249. La Política de Seguridad Corporativa recogerá los tipos de clasificación de la información que se maneja, desarrollándose de forma coordinada en las Políticas de Seguridad de las TIC. Esta coordinación se garantiza en el Comité de Seguridad Corporativa y los Responsables STIC y SI son responsables de su traslado a los correspondientes Comités STIC y SI.





250. El Responsable STIC es responsable del desarrollo de normas y procedimientos que permitan satisfacer los requisitos de los diferentes tipos de información, así como de vigilar su cumplimiento.
251. El Comité STIC se responsabilizará de que la normativa y procedimientos STIC estén alineados con las necesidades establecidas en la política para los diferentes tipos de información. En particular, el Comité STIC aprobará el Documento de Seguridad relativo a información de carácter personal.

## 6.7. DOCUMENTACIÓN DE SEGURIDAD

252. La **Política de Seguridad Corporativa** será elaborada por el Responsable de Seguridad Corporativa y aprobada por el Comité de Seguridad Corporativa y por la Alta Dirección.
253. La **Política de Seguridad de las TIC** será elaborada por el Responsable STIC y aprobada por el Comité STIC y el Comité de Seguridad Corporativa; debe estar alineada en todo momento con la Política de Seguridad Corporativa.
254. Las **normas STIC** y los **procedimientos STIC** serán elaborados por el Responsable STIC y aprobados por el Comité STIC; la elaboración podrá delegarse en los Responsables STIC de Áreas, en particular cuando estos documentos no sean de carácter general.
255. El **Documento de Seguridad**, necesario si la Organización trata datos de carácter personal, deberá ser elaborado por el Responsable STIC y aprobado por el Comité STIC, que informará al Comité de Seguridad Corporativa.

## 6.8. PROYECTOS



256. La realización de proyectos supone la existencia temporal de dominios de seguridad específicos en los que la seguridad debe ser gestionada de forma acorde a las políticas de seguridad y, además, el resultado de los proyectos debe facilitar una explotación acorde a dichas políticas de seguridad. Para cada proyecto se designará un **Responsable de Seguridad del Proyecto**. Este responsable reportará a los Responsables de Seguridad STIC y SI, según corresponda.
257. El Responsable de Seguridad del Proyecto se hará cargo de los **procedimientos de trabajo** durante el desarrollo, en particular del tratamiento de la información empleada: especificaciones, diseños, datos de prueba y manuales de explotación. Realizará un **análisis de riesgos** del entorno de desarrollo y del resultado del proyecto, análisis que será reportado a los Comités STIC y SI para su conocimiento, aprobación y toma de decisiones relativas a las salvaguardas y controles que se incluirán en el sistema para su adecuada explotación; el Responsable de Seguridad del Proyecto será responsable de la adecuada ejecución de dichas decisiones.
258. El Responsable de Seguridad del Proyecto informará de los **incidentes y del progreso** en general del proyecto a los Comités STIC y SI.

## 7. INSPECCIÓN DE SEGURIDAD DE LAS TIC

### 7.1. INTRODUCCIÓN

259. La adecuada protección de los Sistemas de las Tecnologías de la Información y Comunicaciones (TIC) es una actividad crítica para cualquier Organización, debido a la criticidad de la información manejada por dichos entornos tecnológicos y su papel operativo en la Organización, que hacen indispensable garantizar el acceso a la información en cualquier momento (disponibilidad), que la misma sea sólo accesible a personas autorizadas (confidencialidad) y que no sea modificada o destruida sin autorización (integridad).
260. Con objeto de conseguir esta protección adecuada de los Sistemas, se hace necesario implantar un conjunto adecuado de medidas de seguridad, tanto técnicas como organizativas, que permitan la creación de un entorno seguro para la información, como para las aplicaciones y los sistemas que sustentan a todos ellos. De esta forma, todos los Sistemas dispondrán, donde sea conveniente, de un medio para **valorar y verificar el funcionamiento apropiado de los mecanismos de protección** relacionados con la Seguridad de las Tecnologías de la Información y Comunicaciones (STIC)<sup>2</sup> durante todo el ciclo de vida del sistema. El medio necesario que permite verificar la seguridad implementada en el Sistema y que los servicios y recursos utilizados cumplen con los requisitos especificados viene determinado por las **inspecciones de seguridad**.

### 7.2. INSPECCIONES DE SEGURIDAD

261. La Autoridad responsable del Sistema tiene que tener la certeza de que éste satisface los requisitos fijados en la documentación de seguridad según su concepto de operación y el riesgo residual aceptado. Las inspecciones de seguridad constituyen el medio que permite valorar el estado de la información manejada por los sistemas contra la pérdida de confidencialidad, integridad o disponibilidad, ya sea accidental o intencionada, así como la protección de la integridad y disponibilidad de los propios sistemas que sustentan dicha información.
262. Hay que tener en cuenta que las vulnerabilidades no son sólo de tipo técnico (bugs, configuraciones erróneas, servicios inesperados, puertas traseras, etc.), sino que pueden existir vulnerabilidades de tipo humano (falta de concienciación, de formación, etc.), de tipo procedimental (falta de documentación, acciones incorrectas o fuera de procedimiento definido, inexistencia de administrador, ausencia de verificaciones, etc.) o de tipo legislativo o normativo (desviación frente a unos requisitos definidos de obligado cumplimiento).
263. Muchas variables afectan al resultado de una inspección, por lo que es importante definir el modo correcto de evaluar un sistema, una metodología basada en las mejores prácticas y en un amplio consenso. Es fundamental

---

<sup>2</sup> La Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) es la capacidad de dichas tecnologías para evitar, hasta un determinado nivel de confianza, el compromiso de la confidencialidad, integridad y disponibilidad de la información que procesan, almacenan o transmiten los sistemas y la integridad y disponibilidad de los propios sistemas.

reducir posibles prejuicios, parcialidades y subjetividades en las inspecciones, ya que de esta manera se evitan resultados incorrectos o incompletos. Además, no se puede olvidar que una metodología constituye una guía no sólo para personal experto sino que constituye el punto de partida para principiantes en el campo de las inspecciones de seguridad. Para que una inspección de seguridad sea considerada como tal, ésta debe cumplir las siguientes propiedades:

- a. Basada en un estándar, referente o código de buenas prácticas aceptado sectorial, nacional o internacional y adecuado a los requisitos de seguridad de la Organización. La inspección debe basarse en un método adecuado y no en el empleo de un determinado producto comercial
- b. Cuantificable.
- c. Consistente y repetible.
- d. Válida mas allá de un período de tiempo determinado.
- e. Exhaustiva, realizada en profundidad según el marco previamente acordado.
- f. Dentro de la legalidad establecida.

#### 7.2.1. ACTIVIDADES A DESARROLLAR

264. La evaluación exhaustiva de la eficacia de las medidas de seguridad de un Sistema a través de técnicas y procedimientos de verificación constituye una actividad crítica llevada a cabo por la propia Organización o por una tercera parte independiente en nombre de la Organización, y busca garantizar que se han adoptado las contramedidas y salvaguardas adecuadas para la protección de los Sistemas. Las acciones a llevar a cabo para ejecutar dicha evaluación, de acuerdo con la política de seguridad, se centran en:
  - a. Análisis de sistemas y vulnerabilidades.
  - b. Análisis radioeléctricos relacionados con emisiones electromagnéticas no intencionadas (TEMPEST)<sup>3</sup>.
265. Además de la eficacia de los controles de seguridad implementados, la inspección debe servir para actualizar al Sistema respecto a las últimas vulnerabilidades conocidas.
266. Las siguientes actividades determinan el tipo de inspección de seguridad:
  - a. **Análisis.** Supervisión del proceso de valoración y gestión de riesgos llevado a cabo en el Sistema, comprobando que la documentación de seguridad (Declaración de Requisitos de Seguridad, DRS, y Procedimientos Operativos de Seguridad, POS) es fiel reflejo del mismo. El riesgo residual aceptado debe ser acorde con el tipo de información que va a manejar el Sistema. Contempla las siguientes tareas:
  - b. Revisión de la documentación.

---

<sup>3</sup> Por TEMPEST (Transient Electro Magnetic Pulse Emanation Standard) se entiende el fenómeno relacionado con la emisión electromagnética no intencionada producida por los equipos eléctricos y electrónicos que, detectada y analizada, puede llevar a la obtención de información.

- c. Visitas in situ.
- d. Entrevistas con los usuarios y responsables de seguridad del Sistema.
- e. **Verificación.** Comprobación de la implementación de controles de seguridad recogidos en la documentación de seguridad y en el análisis de vulnerabilidades sobre la operación del Sistema. Contempla las siguientes tareas:
  - f. Análisis del flujo de información en el Sistema (análisis de tráfico).
  - g. Grado de cumplimiento de la lista de comprobación aprobada para el Sistema.
  - h. Empleo de herramientas de seguridad (verificación automática) para determinar el estado de seguridad del Sistema ante vulnerabilidades conocidas.
  - i. Análisis manual del sistema operativo y aplicaciones en busca de agujeros de seguridad (verificación manual).
  - j. Gestión del software del Sistema.
  - k. Evaluación TEMPEST del Sistema.
- l. **Test de intrusión.** Ataque activo a un Sistema basado en pruebas de intrusión realizadas por personal experto contra un determinado objetivo de seguridad del mismo, cuyo objetivo primordial es medir el nivel de acceso al Sistema. Agrupa las siguientes tareas:
  - m. Ataque, conocido por los responsables de la Organización, intentando penetrar en el Sistema a pesar de las defensas implementadas.
  - n. Ataque, sin conocimiento por parte de los responsables de la Organización, intentando penetrar en las defensas del Sistema.

#### 7.2.2. TIPOS DE INSPECCIÓN

267. Las inspecciones de seguridad deben abarcar todo el hardware y software relacionado con la seguridad del entorno; esto incluye, donde sea apropiado, las opciones básicas de sistemas operativos, servidores y clientes de correo, servidores y navegadores web, servicios interpersonales (Chat, NetMeeting, Voz sobre IP, etc.), elementos de comunicaciones (switch y router) y dispositivos de protección de perímetro incluyendo herramientas de seguridad, sistemas de detección de intrusos (IDS) y dispositivos trampa. De forma genérica, se pueden distinguir los siguientes tipos de inspección:
- a. **Nivel 1.** Búsqueda de vulnerabilidades o debilidades técnicas del Sistema, lo cual incluye desde el análisis hasta verificaciones manuales de falsos positivos. Se realiza una distinción, separación y examen de los componentes del Sistema para llegar a conocer sus respectivas propiedades y funciones de seguridad.
  - b. **Nivel 2.** Adicionalmente a lo contemplado en el Nivel 1 implica la verificación manual con privilegios administrativos del sistema operativo, aplicaciones y entorno de red que conforman el Sistema. Se determina el nivel de seguridad del Sistema y su grado de cumplimiento

con respecto a la política de seguridad, proporcionando información relevante sobre la seguridad del mismo.

- c. **Nivel 3.** Evaluación del riesgo de los Sistemas mediante el empleo de verificaciones de seguridad, donde los tests de intrusión se utilizan a menudo para confirmar tanto falsos positivos como negativos. Se trata de comprobar que se mantienen las condiciones de acreditación, es decir, que el nivel de seguridad otorgado a un Sistema no ha sufrido merma.

268. A continuación se muestra una comparativa entre los distintos tipos de inspección:

	Nivel 1	Nivel 2	Nivel 3
<b>ÁMBITO</b>	Elemento (producto, servicio, dispositivo, aplicación...) y Sistema	Elemento (producto, servicio, dispositivo, aplicación...) y Sistema	Elemento (producto, servicio, dispositivo, aplicación,...), Sistema e Interconexión
<b>OBJETIVO</b>	Identificar vulnerabilidades para llegar a conocer las respectivas propiedades y funciones de seguridad del Sistema	Determinar el nivel de seguridad de un Sistema y su grado de cumplimiento con la política de seguridad.	Verificar que se mantienen las condiciones de Acreditación otorgadas al Sistema
<b>ACTIVIDADES</b>	- Análisis - Verificación Automática	- Análisis - Verificación Automática - Verificación Manual	- Análisis - Verificación Automática - Verificación Manual - Test de Intrusión
<b>MEDIOS Y TÉCNICAS</b>	- Cuestionarios - Entrevistas - Herramientas de Seguridad	- Cuestionarios - Entrevistas - Herramientas de Seguridad - Verificación Manual	Herramientas y técnicas de explotación de vulnerabilidades
<b>REALIZACIÓN</b>	Continua, especialmente tras la adición de un nuevo componente al Sistema	Periódica y acorde con el Procedimiento de Acreditación	Periódica y con carácter excepcional dependiendo de la sensibilidad del Sistema
<b>RESULTADO</b>	Mejora en la gestión global de la seguridad	Conocimiento real del riesgo del Sistema	Reconocimiento objetivo de que el Sistema opera dentro del marco de seguridad definido

### 7.2.3. RESPONSABILIDADES

269. La responsabilidad en la realización de las inspecciones de seguridad es del personal evaluador, el cual está constituido por un **analista** y por varios **técnicos especialistas** en diferentes campos (sistemas operativos, bases de datos, elementos de comunicaciones, dispositivos de protección de perímetro, etc.). El analista ejerce la dirección del equipo asumiendo la redacción final del informe de inspección y todas las decisiones relacionadas.

270. El equipo de inspección actuará en el marco de algunas de las actividades que a continuación se relacionan:

- a. Inspección de un Sistema que se encuentre en proceso de acreditación.

- b. Inspección de un Sistema que se halle dentro del calendario de inspecciones correspondiente.
  - c. Inspección de un Sistema a petición de un Organismo.
  - d. Inspección de un Sistema como consecuencia de un incidente de seguridad.
  - e. Cualquier otra razón que venga determinada por la Dirección de la Organización.
271. Dependiendo del tipo de información que maneja el Sistema, el proceso de inspección puede variar. Para Sistemas que manejen información con un nivel de **clasificación sensible**, la inspección tiene carácter obligatorio como requisito previo para la explotación del Sistema, contemplará el cumplimiento de los requisitos de seguridad recogidos en la documentación del Sistema (DRS y POS) y será periódica durante todo el ciclo de vida del Sistema. Para sistemas que manejen información con un **nivel de clasificación inferior** al anterior, la inspección debe establecerse con una periodicidad adecuada durante todo el ciclo de vida del Sistema, no siendo obligada para su puesta en explotación y contemplará el cumplimiento de los requisitos de seguridad recogidos en la documentación del Sistema. Finalmente, para Sistemas que se conecten con otros Sistemas o redes, los tests de intrusión se realizarán desde los Sistemas que manejen información con un nivel de clasificación inferior o serán llevados a cabo desde ambos Sistemas, si estos manejan información de un mismo nivel de clasificación.

### 7.3. PROCESO DE INSPECCIÓN

272. Durante la fase inicial del ciclo de vida del Sistema (desarrollo) se determinan los requisitos de seguridad, se establecen los controles de seguridad y se aprueba el plan de seguridad del Sistema. Con las inspecciones se persigue la mejora, desde el punto de vista STIC, de los mecanismos de seguridad del Sistema y de los procedimientos que le son de aplicación, lo que permite establecer y mejorar la estrategia de implantación de contramedidas que mitiguen las amenazas más importantes según el riesgo residual aceptado en el proceso de gestión de riesgos.
273. El proceso de inspección de seguridad busca complementar al menos los siguientes objetivos:
- a. Tener la certeza de que se aplican y continúan aplicando los mínimos criterios de seguridad requeridos (DRS).
  - b. Mantener centrada la atención de la Organización en la importancia de la seguridad.
  - c. Recomendar la contramedida más adecuada contra impactos concretos por la pérdida de un objetivo de seguridad relacionado con la misión de la Organización.
  - d. Impulsar el programa de educación y concienciación en seguridad de la Organización.

### 7.3.1. MEDIOS NECESARIOS

274. Antes de realizar una inspección sobre un Sistema es necesario disponer de unos **medios** que garanticen la eficiencia del proceso y la veracidad de los resultados generados en el proceso de inspección. Estos medios serán de tipo humano, procedimental, técnico y organizativo.
275. Por otro lado, es imprescindible contar con una **metodología** que asegure la consistencia de los resultados obtenidos, definiendo un conjunto ordenado de acciones y procedimientos de actuación que definan el qué y el cómo de los equipos de inspección.

### 7.3.2. REQUISITOS INICIALES

276. A continuación, se detallan una serie de tareas previas a la inspección de seguridad que deben realizar los equipos evaluadores; el objetivo es recoger la información pertinente para poder realizar una planificación temporal y establecer los recursos necesarios para el desarrollo de una inspección de forma eficaz y eficiente.
277. En primer lugar es necesario obtener las **autorizaciones** y habilitaciones pertinentes para llevar a cabo el proceso de inspección en el Sistema. Adicionalmente se debe recoger e identificar la siguiente información relativa a la **Organización**:

Localización	Identificación del centro u organismo al que pertenece el Sistema a inspeccionar Teléfono / Fax
	Datos de contacto del responsable del centro u organismo
Estructura y Organización STIC	Datos de contacto del Responsable STIC en la Organización a la que pertenece el Sistema Datos de contacto de los miembros (si existen) que dependan jerárquicamente de la citada Autoridad.

278. También se debe recoger e identificar la información relativa al **Sistema**:

Ubicación	Identificación del Sistema a inspeccionar Dirección postal donde se ubica el Sistema
Descripción del Sistema	Descripción del objeto o función del Sistema junto con la identificación de los servicios y/o recursos que presta Tipo de información y niveles de clasificación de la información que maneja el Sistema tanto en formato electrónico como en papel Identificación de las diferentes áreas, plantas, salas, etc. donde se ubica el Sistema Diagrama de arquitectura de red
Estructura y Organización del Sistema	Datos de contacto del responsable del Sistema



	<p>Datos de contacto del Administrador de Seguridad del Sistema.</p> <p>Datos de contacto del Administrador del Sistema.</p> <p>Número y tipo de usuarios del Sistema</p>
Inspecciones STIC	<p>Si existe, fecha de la última inspección y referencia del informe (registro)</p> <p>Si existe, fecha de la última declaración de acreditación</p>
Riesgos del Sistema	<p>Verificar la existencia de un análisis de riesgos, y en caso afirmativo, comprobar la fecha de realización</p> <p>Identificar el método y herramienta utilizada para realizar el análisis de riesgos</p>
Principios y Requisitos de Seguridad	<p>Identificar los requisitos de seguridad que el Sistema deba cumplir y obtener y analizar la documentación de seguridad elaborada por los responsables del Sistema</p>

279. Se debe delimitar el **alcance** de la inspección mediante la identificación de los dispositivos hardware, software, aplicaciones, tecnología usada, etc., con el fin de determinar los medios técnicos (herramientas, cuestionarios, guías, etc.) a emplear. A partir de este alcance será posible la **planificación** e identificación de **necesidades** por parte del equipo de inspección:

- Desarrollo de la adecuada planificación que incluya un calendario de las tareas a realizar, las herramientas y personal involucrado en la inspección.
- Identificación de las necesidades que debe proporcionar el Sistema durante la inspección: acceso a salas, presencia de administradores, acceso al Sistema con derechos específicos, cumplimentación de cuestionarios, espacio de trabajo, etc.
- Comunicación de la planificación inicial y de las necesidades.

280. Finalmente es necesario identificar las **limitaciones** del Sistema objetivo y estudiar la **viabilidad** de la realización del proceso de inspección en las condiciones reales de trabajo.

### 7.3.3. ESTIMACIÓN DE TIEMPO

281. Como en cualquier proyecto, en las inspecciones de seguridad se debe establecer un calendario teniendo en cuenta que el tiempo total de una inspección nunca debe exceder de tres (3) meses. El calendario debe realizarse considerando los siguientes aspectos generales:

- Tiempo de enumeración y descubrimiento de elementos activos (horas-máquina).
- Tiempo de análisis técnico (horas-hombre).
- El análisis puede empezar en una fase inicial, pero nunca antes de que haya transcurrido la mitad del tiempo necesario para la enumeración.
- El tiempo de análisis (horas-hombre) disminuirá proporcionalmente con el número de evaluadores, pero hay que tener en cuenta que el análisis y

la generación de informes llegará a ser más complejo e implicará más tiempo cuando se empleen a más de 5 evaluadores.

- e. Se deben reservar aproximadamente dos días-hombre (16 horas-hombre) por cada persona y semana para dedicarlo a investigación y desarrollo, lo cual incluye mantenimiento y verificación de herramientas de seguridad.
- f. Aproximadamente la mitad del tiempo invertido en la inspección de seguridad es necesario para la generación de informes.

#### 7.3.4. INFORME DE RESULTADOS

- 282. Una de las partes más importantes del proceso de inspección y que constituye un resumen del mismo es el **informe de la inspección realizada**. Este informe constituye la fase final de la inspección de seguridad junto con la reunión en grupo descrita en el punto siguiente y debe ser entregado como mínimo tres (3) días antes de esta reunión.
- 283. El lenguaje de este informe debe ser claro para cada uno de los públicos objetivos y debe ser positivo, destacando tanto los aspectos correctos encontrados como aquellos susceptibles de ser mejorados; en este último caso el informe de inspección debe recoger de forma estructurada cualquier deficiencia detectada en la implementación de las medidas de seguridad y las acciones correctivas a llevar a cabo, incluyendo fechas de cumplimentación.
- 284. La clasificación del informe de resultados será como mínimo de CONFIDENCIAL debiendo remitirse a la Autoridad competente dentro de los 60 días posteriores a la inspección, o 30 días si se han identificado problemas graves, para que la Organización objeto de la inspección pueda llevar a cabo las pertinentes acciones correctivas.
- 285. El informe de la inspección realizada debe constar al menos de un resumen ejecutivo y un informe técnico. En el **resumen ejecutivo** se mostrarán, en términos de probabilidades, impactos y riesgos estimados, los resultados globales obtenidos durante la inspección. Este informe no debe sobrepasar, en términos generales, las dos hojas de extensión, y debe ser capaz de sintetizar en este espacio al menos los siguientes aspectos y su justificación:
  - a. Estado global de seguridad de la Organización en el ámbito de la inspección y nivel de riesgo estimado en dicho ámbito.
  - b. Aspectos generales, positivos y negativos, determinados durante la inspección.
  - c. Problemas especialmente relevantes que puedan poner en riesgo la seguridad corporativa.
  - d. Líneas de trabajo recomendadas para subsanar las principales debilidades del sistema.
  - e. Fechas, propósito, entidad que realiza la inspección, personal de contacto (solamente los responsables)...
- 286. Por su parte, en el **informe técnico** deben presentarse, como su nombre indica, los resultados técnicos de la inspección ejecutada. Para cada uno de los elementos tecnológicos analizados, se presentará su resumen de estado, las

vulnerabilidades encontradas y las pruebas de concepto correspondientes en los casos en los que aplique. Además, se detallarán con el suficiente nivel aquellas directrices para la corrección de vulnerabilidades que el equipo auditor considere necesario aplicar, debiendo contener al menos la siguiente información para cada vulnerabilidad relevante detectada:

- a. **Identificación** de la vulnerabilidad.
  - b. Descripción de las **acciones ejecutadas** para identificar la vulnerabilidad.
  - c. **Evidencia**. Demostración de que la vulnerabilidad realmente existe.
  - d. **Impacto**. Descripción del tipo de compromiso (confidencialidad, integridad, disponibilidad) que supone para el Sistema la existencia de la vulnerabilidad.
  - e. **Solución**. Propuesta de acciones para eliminar la vulnerabilidad o mitigarla. En caso de no ser posible la eliminación o mitigación directa es necesario detallar alternativas que impliquen la disminución del riesgo por otras vías, como la eliminación de la amenaza o la identificación de controles compensatorios.
  - f. **Gravedad**. Valoración de la vulnerabilidad.
287. Con independencia del informe asociado a la inspección, hay que realizar notificaciones extraordinarias cuando el evaluador modifique el plan de trabajo, se cambie la procedencia/origen de los análisis, se identifiquen problemas graves, antes de la ejecución de una prueba de alto riesgo o de gran generación de tráfico o cuando se hayan originado problemas en el proceso de inspección.
288. En la redacción y entrega de informes se deben tener en cuenta los siguientes aspectos:
- a. Incluir soluciones prácticas orientadas a resolver los problemas de seguridad detectados.
  - b. Englobar todos los hallazgos desconocidos e identificarlos claramente como tales.
  - c. Especificar con claridad todos los estados de seguridad del Sistema y no sólo centrarse en las medidas de seguridad inapropiadas.
  - d. Usar indicadores cualitativos para medir los riesgos siguiendo métodos comúnmente aceptados y no simplemente basados en la intuición del equipo evaluador.
  - e. Notificar a la Organización el envío del informe, confirmándose la recepción del mismo.
  - f. Todos los canales de comunicación para la entrega de informes deben ser confidenciales.

#### 7.3.5. REUNIÓN EN GRUPO

289. La reunión en grupo o *workshop* es la reunión final de presentación de resultados de una inspección de seguridad y con la misma se culmina todo el

proceso. Estos resultados deben ser presentados de forma directa por el analista, como responsable de la inspección, participando además en la reunión al menos un técnico evaluador. El número de asistentes por parte de la Organización no debe ser superado por el número de responsables de la inspección a menos que únicamente asista a esta reunión una persona por parte de la Organización, caso en el cual estarán presentes dos evaluadores (analista y técnico).

290. En la reunión en grupo se deben tratar los principales hallazgos realizados durante las pruebas, así como cualquier situación o resultado destacable o relevante para la seguridad del entorno inspeccionado. El foro que asistirá a esta reunión no tiene por qué ser exclusivamente técnico, por lo que el contenido de la presentación de resultados no tiene que estar centrado en la parte técnica de la inspección, sino en términos de riesgos estimados para el entorno analizado.

#### 7.4. LISTA DE COMPROBACIÓN

291. Las listas de comprobación deben reflejar la estrecha relación que debe existir entre las inspecciones de seguridad y la documentación de seguridad del Sistema (DRS, POS, etc.), de tal manera que se puedan verificar todos los aspectos de seguridad en una inspección. Sirven como evidencia de la inspección, responsabilizan al evaluador de los resultados obtenidos, proporcionan una visión adecuada y general de la inspección y, adicionalmente, sirven como guía al evaluador en futuras inspecciones.
292. Estas listas de comprobación deben cubrir al menos los siguientes ámbitos:
- a. Aspectos Generales.
  - b. Administración y Organización de Seguridad.
  - c. Seguridad de las Tecnologías de la Información y Comunicaciones.
  - d. Seguridad Criptológica.
  - e. Seguridad TEMPEST.
  - f. Gestión de la Configuración.
  - g. Planes de Emergencia y Contingencia.
293. Con las listas de comprobación se contribuye a fundamentar con más detalle las recomendaciones/observaciones proporcionadas por la inspección de seguridad. Se deben incluir en el informe de resultados con la firma del evaluador responsable de su cumplimentación.

#### 7.5. HERRAMIENTAS DE SEGURIDAD

294. Las herramientas de seguridad son aquellos productos hardware y software que proporcionan una capacidad más automatizada de control, operación y/o gestión de diferentes aspectos de seguridad en un Sistema. Aunque no todas las herramientas desempeñen funciones específicas de seguridad, su empleo proporciona una operación y gestión del Sistema más efectiva y adecuada que repercute indirectamente en la seguridad.
295. La instalación de las herramientas de seguridad en los Sistemas podrá realizarse de forma permanente o circunstancial; en el primer caso, la configuración,

operación y control del uso de las herramientas estará indicado en la documentación de seguridad (DRS y POS), mientras que en el segundo caso se elaborará un documento específico que deberá ser aprobado por la Autoridad de acreditación del Sistema.

296. Todas aquellas herramientas directamente vinculadas a procesos de inspección o auditoría, por ejemplo las que son capaces de explotar vulnerabilidades de los Sistemas, como analizadores de vulnerabilidades, escáneres de puertos, rompedores de contraseñas, etc. deberán ser utilizadas únicamente por personal experto y expresamente autorizado por la Autoridad responsable de la acreditación del Sistema.
297. Finalmente, toda la información recopilada por las herramientas de seguridad deberá ser clasificada y tratada como CONFIDENCIAL o superior.

## 7.6. PERIODICIDAD

298. Las inspecciones de seguridad muestran, en un momento dado, el estado de seguridad de un Sistema. Por tanto, las medidas de seguridad deben ser continuamente revisadas llevando a cabo continuos análisis de riesgos e inspecciones periódicas de acuerdo con la política de seguridad del Sistema.
299. El resultado de una inspección STIC debe tener una fecha de caducidad, un tiempo límite tras el cual la confianza depositada en el Sistema para que maneje información desaparezca. La metodología empleada debe definir un tiempo de caducidad de los resultados obtenidos y disponer de los parámetros adecuados que midan la evolución del Sistema a partir de los resultados de varias inspecciones periódicas.
300. A continuación, se proporciona una referencia de la frecuencia con que deben de realizarse las inspecciones de seguridad para un Sistema que almacena, procesa o transmite información clasificada:
  - a. Para Sistemas que manejan información clasificada como SECRETO, una inspección de seguridad debería de llevarse a cabo cada dieciocho (18) meses.
  - b. Para Sistemas que manejan información clasificada y que están conectados a Internet o redes públicas similares, al menos una inspección de seguridad debería de llevarse a cabo cada dieciocho (18) meses.
  - c. Para el resto de Sistemas, los requisitos para una inspección de seguridad, incluyendo la frecuencia y el nivel de detalle, serán establecidos como parte del análisis y proceso continuo de gestión de riesgos.
301. La sensibilidad del Sistema en el desarrollo de la misión de la Organización, es uno de los principales factores a tener en cuenta respecto a la periodicidad con que deben efectuarse las inspecciones de seguridad. Es también necesario considerar la velocidad de cambio del Sistema, entendiendo por ésta la introducción de nuevos dispositivos, productos, servicios, conexiones, usuarios, procedimientos, requisitos, etc.

302. En cualquier caso, las inspecciones de seguridad estarán apoyadas por revisiones periódicas centradas en aspectos de seguridad específicos allí donde sea fundamental mantener el estado de seguridad del Sistema.

## **7.7. CONCLUSIONES**

303. Un elevado porcentaje de los compromisos de seguridad denunciados son resultado de la explotación de vulnerabilidades conocidas o errores de configuración, para los cuales había salvaguardas y contramedidas disponibles. Consecuentemente, es primordial efectuar inspecciones de seguridad para poder asegurar que la información y los Sistemas que la soportan están protegidos adecuadamente durante todo el ciclo de vida del Sistema.
304. La calidad en el resultado de una inspección de seguridad es difícil de juzgar sin una metodología, un estándar de referencia; por tanto es necesario definir y aplicar un método ampliamente aceptado donde haya que seguir una serie de pasos convenientemente actualizados para llevar a cabo la inspección.
305. Por último, es necesario destacar que las inspecciones de seguridad no se pueden considerar simplemente como una simple imagen, en un momento dado, del estado de seguridad de un Sistema y presentar los resultados como una instantánea de la seguridad. Aunque se trate de vulnerabilidades, debilidades y configuraciones conocidas en ese instante, las inspecciones de seguridad se basan en una periodicidad y en un análisis de riesgos constante que constituyen un proceso continuo en el estado de seguridad del Sistema. La frecuencia de las inspecciones y el grado de detalle asociado a cada una de ellas dependerán de la importancia del Sistema en el cumplimiento de la misión asignada dentro de la Organización.

## 8. ACREDITACIÓN DE SISTEMAS

### 8.1. INTRODUCCIÓN

306. La información clasificada manejada en un Sistema debe protegerse contra la pérdida de confidencialidad, integridad y disponibilidad, sea accidental o intencionada, y debe impedirse la pérdida de integridad y disponibilidad de los propios Sistemas que sustentan dicha información. Al objeto de conseguir la protección de seguridad adecuada se deberán aplicar un conjunto equilibrado de medidas de seguridad de distinta naturaleza que permitan la creación de un entorno seguro en el que opere el Sistema.
307. Se entiende por **Acreditación** la certificación otorgada a un Sistema de las TIC por la Autoridad responsable de la Acreditación de la capacidad para manejar información clasificada hasta un grado determinado o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su Concepto de Operación (CO).

### 8.2. CONDICIONES PARA LA ACREDITACIÓN

308. Como condición previa a la concesión de la autorización para manejar información clasificada, las Autoridades responsables de la acreditación someterán a todos los Sistemas de su ámbito de competencia a un proceso de acreditación que garantice el adecuado nivel de protección y su mantenimiento. Dicho proceso revisará al menos los aspectos detallados en la presente guía CCN-STIC.

#### 8.2.1. DOCUMENTACIÓN DE SEGURIDAD

309. Todo Sistema que maneje información clasificada deberá tener actualizada la correspondiente documentación de seguridad, dado el carácter dinámico de la misma. Dicha documentación debe comprender al menos los siguientes aspectos:
- a. **Concepto de Operación (CO)**. Declaración expresa que se realiza sobre el objeto o función de un Sistema o de una interconexión de Sistemas, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación...) y las amenazas a las que estará sometido.
  - b. **Análisis de Riesgos (AR)**. Proceso consistente en identificar amenazas y vulnerabilidades determinando su magnitud y las áreas que necesitan salvaguardas y contramedidas, plasmando todo ello en el correspondiente documento de análisis.
  - c. **Declaración de Requisitos de Seguridad (DRS)**. Documento base para la acreditación, consistente en una exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implementar. Constituye el resultado del análisis de riesgos realizado en función de la Política de Seguridad vigente.



- d. **Procedimientos Operativos de Seguridad (POS).** Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. Los POS son la aplicación práctica de los DRS sobre el Sistema, por lo que constituyen el manual de seguridad que todo usuario está obligado no sólo a leer sino a comprender y a aplicar, ya que describe cómo debe interactuar un usuario con el sistema para mantener la seguridad del mismo.

#### 8.2.2. SEGURIDAD DEL PERSONAL

310. Todas las personas que tengan acceso a los Sistemas donde se maneje información clasificada deberán poseer la correspondiente autorización por la Autoridad responsable del Sistema, de acuerdo con las normas establecidas por el propietario de la información clasificada, que ponderará la necesidad de conocer y la posesión de algún tipo de autorización para acceder a este tipo de información.
311. La relación de personas autorizadas a acceder al Sistema y a la información en él contenida deberá figurar como anexo adjunto a la documentación de seguridad (POS), detallando no sólo su identificación única sino también los derechos y permisos de las mismas.

#### 8.2.3. SEGURIDAD FÍSICA

312. Aquellas áreas dónde se pueda acceder a información clasificada a través de un Sistema deberán estar certificadas de acuerdo al nivel de clasificación de la información manejada y a los requisitos de integridad y disponibilidad requeridos.

#### 8.2.4. SEGURIDAD DOCUMENTAL

313. Los documentos que contienen información clasificada, así como sus soportes informáticos, serán protegidos de acuerdo con las Leyes y Normas en vigor (por ejemplo, Decreto 242/1969 de 20 de febrero por el que se desarrolla la Ley 9/1968, sobre Secretos Oficiales, modificada por la Ley 48/1978 de 7 de octubre). En los casos no contemplados por dicha normativa, para la protección de los documentos que contienen información clasificada, así como de sus soportes informáticos, será de aplicación la normativa interna de cada Organismo.

#### 8.2.5. SEGURIDAD DE EMANACIONES

314. Para la protección de la información clasificada contra los fenómenos basados en radiaciones electromagnéticas no deseadas, se aplicará la normativa establecida por la Autoridad correspondiente. En la documentación de seguridad del Sistema deberán figurar los certificados de las áreas donde se ubiquen los elementos del Sistema y, en su caso, de los certificados de Seguridad de Emanaciones (TEMPEST) de estos últimos.

### 8.2.6. SEGURIDAD CRIPTOLÓGICA

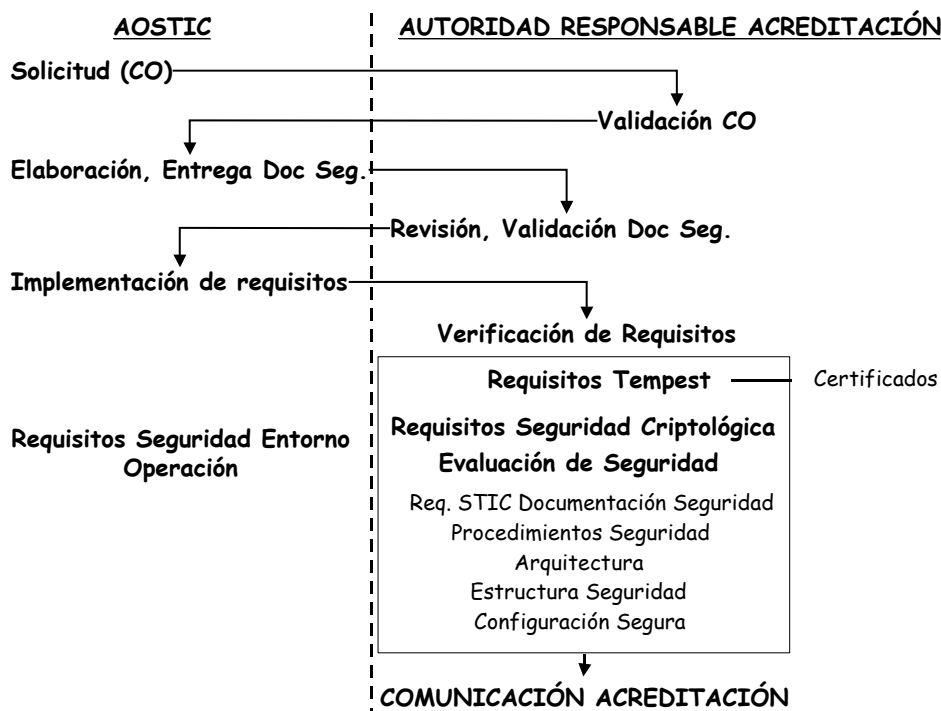
315. En aquellos Sistemas que manejen información clasificada y empleen medios o procedimientos de cifra será de obligado cumplimiento la normativa vigente y el empleo de productos con certificación criptológica, incluidos en el pertinente catálogo actualizado y publicado por la Autoridad correspondiente.

### 8.2.7. SEGURIDAD DE LAS TIC (STIC)

316. Todos los Sistemas que manejen información clasificada deberán disponer de un conjunto equilibrado de servicios de seguridad que permitan alcanzar los objetivos de seguridad requeridos. Estos servicios de seguridad permitirán, cuando sea apropiado, lo siguiente:
- a. Identificar y autenticar a las personas con acceso autorizado.
  - b. Controlar los accesos a la información a partir del principio de necesidad de conocer.
  - c. Verificar la integridad y el origen de la información y de los elementos del Sistema.
  - d. Mantener la integridad de la información clasificada y de los elementos del Sistema.
  - e. Mantener la disponibilidad requerida para la información y los elementos del Sistema.
  - f. Garantizar y verificar el funcionamiento de los mecanismos de seguridad del Sistema.
  - g. Registrar y auditar la actividad de los usuarios del Sistema.
  - h. Controlar las conexiones y los enlaces de los Sistemas.
  - i. Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información o la integridad y disponibilidad del Sistema que la soporta.
317. Las Autoridades responsables de la acreditación velarán para que estos requisitos aparezcan reflejados en la documentación de seguridad del Sistema y se satisfagan en las diferentes fases del ciclo de vida del mismo.

## 8.3. PROCESO DE ACREDITACIÓN

318. Antes de conceder la autorización a un Sistema, las Autoridades responsables deberán ejecutar las inspecciones de seguridad correspondientes para verificar el cumplimiento de las condiciones de acreditación, así como los requisitos de seguridad descritos en la documentación de seguridad y su correcta implementación.



319. En la figura anterior se representa gráficamente el proceso de acreditación, que consta de las siguientes tareas:

- Envío de la solicitud de acreditación y del Concepto de Operación (CO). La Autoridad Operativa del Sistema remitirá a la Autoridad competente en la acreditación el Concepto de Operación del Sistema como documento adjunto a la solicitud de acreditación.
- Validación del Concepto de Operación e inicio del proceso de acreditación. La Autoridad responsable de la acreditación, una vez validado el CO, comunicará a la Autoridad Operativa del Sistema el inicio del proceso de acreditación.
- Entrega de la documentación de seguridad. La Autoridad Operativa del Sistema elaborará la documentación de seguridad del Sistema y la remitirá a la Autoridad responsable de la acreditación.
- Revisión y validación de la documentación de seguridad. Como acción previa a la inspección de seguridad es necesario validar la documentación de seguridad por parte de la Autoridad responsable de la acreditación correspondiente.
- Implementación de requisitos. La Autoridad Operativa del Sistema, con anterioridad a la inspección de seguridad preceptiva debe implementar todos los requisitos indicados en la documentación de seguridad del Sistema.
- Verificación del cumplimiento de los requisitos de seguridad física, documental, de emanaciones y de personal. La Autoridad responsable de la acreditación verificará que se cumplen los requisitos de seguridad física, documental, de emanaciones y de personal. Previamente, la

Autoridad Operativa del Sistema remitirá los certificados relacionados con la seguridad física y de emanaciones.

- g. Verificación del cumplimiento de los requisitos de seguridad criptológica. La Autoridad responsable de la acreditación verificará que se cumplen los requisitos de seguridad criptológica, basados en el empleo de productos con certificación criptológica incluidos en el pertinente catálogo actualizado y publicado por la Autoridad correspondiente.
- h. Verificación del cumplimiento de los requisitos STIC. La verificación de requisitos de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) se realizará mediante la correspondiente inspección STIC por la Autoridad responsable de la acreditación o por quién ésta haya establecido. En concreto se verificará la exactitud de los siguientes aspectos tal y como son descritos en la documentación de seguridad:
  - i. La implementación de los requisitos STIC.
  - j. Los procedimientos de seguridad del Sistema.
  - k. La arquitectura del Sistema con las interconexiones del mismo.
  - l. La estructura de seguridad (responsables de seguridad) que soporta el Sistema.
  - m. Las configuraciones de los elementos del Sistema, verificando que se implementa lo prescrito por los planes de evaluación y chequeo de la seguridad (ST&E Plan) y guías STIC correspondientes.
  - n. La Autoridad responsable de la acreditación remitirá a la Autoridad Operativa del Sistema el resultado de la inspección STIC acompañado del preceptivo informe donde se reflejen las deficiencias detectadas.
  - o. Comunicación de la acreditación: la Autoridad responsable de la acreditación emitirá la declaración de cumplimiento (acreditación) una vez se hayan cumplimentado los puntos citados previamente y el resultado sea positivo.

#### 8.4. INTERCONEXIÓN DE SISTEMAS ACREDITADOS

- 320. Se produce una conexión cuando se proveen los medios físicos y lógicos de transmisión adecuados (por ejemplo enlace satélite, fibra óptica, etc.) susceptibles de ser empleados para el intercambio de información. La interconexión entre Sistemas tiene lugar cuando existe una conexión y se habilitan flujos de información entre tales Sistemas con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes Autoridades Operativas o una combinación de las anteriores.
- 321. Todos los Sistemas que manejen información clasificada, como paso previo a la solicitud de acreditación de su interconexión a otro Sistema o a redes públicas o similares, deben estar acreditados al nivel correspondiente de la información que manejen. La responsabilidad de la acreditación para la interconexión de un Sistema acreditado a otro u otros Sistemas, será de una única Autoridad cuando

los Sistemas recaigan dentro de su ámbito de actuación o, en caso contrario, corresponderá a un Comité de Acreditación formado por todas las Autoridades afectadas por dicha interconexión.

322. La acreditación se realizará mediante la validación de la correspondiente documentación de seguridad y las inspecciones STIC que verifiquen el cumplimiento de los requisitos establecidos en la citada documentación y aquellos otros establecidos por la normativa correspondiente.

## 8.5. SITUACIONES POSIBLES DE LA ACREDITACIÓN

323. En el proceso de acreditación se podrán dar las siguientes situaciones:

- a. **Autorización para Pruebas (AP).** Esta situación es utilizada como paso previo a manejar información clasificada con objeto de realizar las pertinentes pruebas técnicas (funcionales y de seguridad), de comunicaciones e intercambio de información sin clasificar. En este punto es necesario tener redactada la documentación de seguridad.
  - b. **Autorización Temporal con Propósitos Operacionales (ATPO).** Esta autorización es apropiada para situaciones en las que no se haya llevado a cabo un proceso de acreditación. La Autoridad responsable de la acreditación puede otorgar esta situación en circunstancias excepcionales y su validez será limitada (por ejemplo, seis meses que pueden ser prorrogables). La solicitud de esta ATPO debe ser realizada por la Autoridad Operativa del Sistema basándose en el concepto de operación, siendo importante indicar que **esta situación se limitará a causas muy justificadas** y en cualquier caso, estos Sistemas o interconexiones deben figurar en el registro de Sistemas acreditados.
  - c. **Autorización Provisional para Operar (APO).** Esta situación es utilizada para Sistemas o interconexiones en proceso de acreditación que no hayan superado completamente éste (pendiente de la resolución de deficiencias) o como paso previo para la concesión de la acreditación definitiva. En esta situación cada uno de los elementos del Sistema, incluidas las interconexiones, puedan intercambiar información clasificada. La documentación de seguridad debe estar redactada y la validez máxima de esta situación será limitada. Se podrán imponer limitaciones a los Sistemas o interconexiones que se encuentren en esta situación.
  - d. **Acreditación.** Situación alcanzada por los Sistemas e interconexiones que hayan superado con éxito el proceso de acreditación. La validez de la misma estará fijada en la comunicación de acreditación.
324. Si un Sistema o una interconexión no superan el proceso de acreditación, pero por necesidades operativas es necesario que manejen información clasificada, la Autoridad responsable de la acreditación podrá conceder la APO correspondiente. Los Sistemas y las interconexiones que se establezcan con carácter temporal, exclusivamente para la realización de operaciones y ejercicios, y que precisen manejar información clasificada, deberán contar con la correspondiente ATPO por el periodo que dure dicha operación o ejercicio.

## 8.6. INSPECCIONES

325. Deberán realizarse inspecciones de los Sistemas y de las interconexiones acreditadas para verificar el mantenimiento de las condiciones de acreditación; el período máximo entre inspecciones para los diferentes Sistemas acreditados vendrá determinado por el mayor grado de clasificación de la información manejada y la Autoridad responsable de la acreditación establecerá el calendario de inspecciones, siempre dentro de los plazos máximos establecidos. La continuidad de la acreditación otorgada dependerá del resultado de las inspecciones y podrá requerir de la Autoridad Operativa del Sistema la adopción de una serie de medidas correctivas así como un plazo para implantarlas.
326. La no implementación de tales medidas correctivas en el plazo requerido podrá ocasionar la pérdida de la acreditación, lo que implicará la eliminación de la información clasificada según el proceso que establezca la Autoridad responsable de la acreditación.
327. El resultado de una inspección puede, en algunos casos, requerir la necesidad de reacreditar.

## 8.7. VALIDEZ DE LA ACREDITACIÓN

328. La clasificación de la información que manejan los Sistemas acreditados determina el período máximo de validez de una acreditación, independientemente de las inspecciones que puedan sufrir.
329. En el caso de la interconexión de Sistemas, el período máximo de validez de una acreditación vendrá determinado por el mayor grado de clasificación de la información manejada por los Sistemas interconectados.

### 8.7.1. REACREDITACIÓN

330. La reacreditación es la renovación de la autorización para manejar información clasificada una vez expirada la autorización concedida o tras un cambio significativo de la configuración hardware y/o software, de la ubicación del Sistema, del tipo o nivel de clasificación de la información manejada u otras circunstancias que lo aconsejen.
331. La Autoridad Operativa del Sistema valorará las implicaciones de seguridad de todos los cambios sufridos por el Sistema durante su ciclo de vida. Los cambios que afecten a las características de seguridad deberán ser aprobados previamente por la Autoridad Operativa y acreditados por la Autoridad responsable de la acreditación.

### 8.7.2. INFORMES A REMITIR EN EL PERÍODO ENTRE ACREDITACIONES

332. Una vez concedida la acreditación, la Autoridad Operativa del Sistema deberá remitir un **informe anual** a la Autoridad responsable de la acreditación dónde se expresen las vicisitudes ocurridas en el mismo. Este informe debe recoger los siguientes aspectos:
  - a. Altas y bajas del personal responsable de la seguridad del Sistema.

- b. Modificaciones del hardware, del software o de ubicación previstas durante el año que puedan tener impacto en la seguridad del Sistema.
  - c. Estado de cumplimiento de los DRS y POS.
  - d. Incidentes que hayan afectado o comprometido la seguridad del Sistema.
333. Cualquier otro cambio que sufra el Sistema (de emplazamiento, de configuración hardware/software...) no previsto en el informe remitido será comunicado por la Autoridad Operativa del Sistema a la Autoridad responsable de la acreditación para reiniciar, en su caso, el proceso de acreditación.

#### 8.7.3. REGISTRO DE SISTEMAS ACREDITADOS

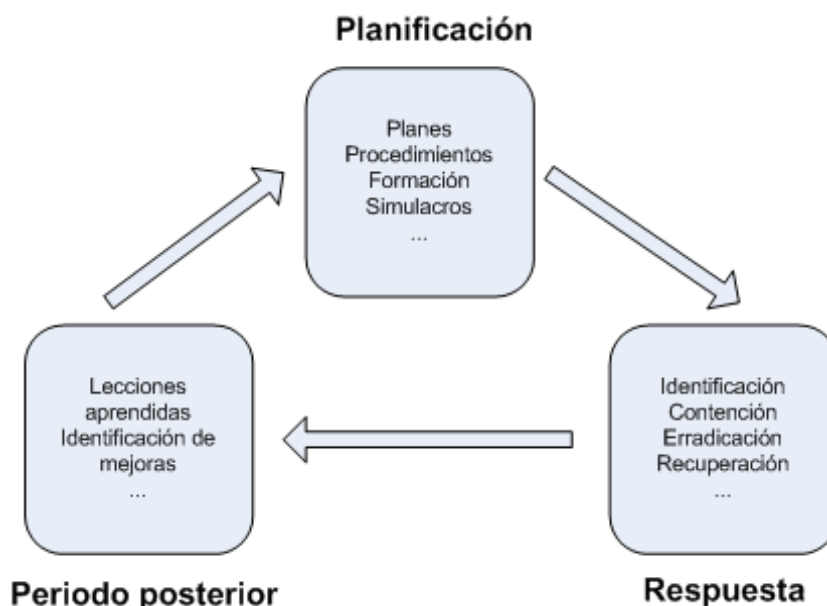
334. Las Autoridades responsables de la acreditación mantendrán un registro actualizado de los Sistemas que hayan finalizado su proceso de acreditación.



## 9. GESTIÓN DE INCIDENTES DE SEGURIDAD

### 9.1. INTRODUCCIÓN

335. Para tratar de proteger adecuadamente la información corporativa es imprescindible ser capaz de gestionar la seguridad de forma correcta, y dicha gestión pasa obligatoriamente por el establecimiento de una **capacidad de gestión de incidentes de seguridad**. Dicha capacidad debe permitir a las Organizaciones responder de forma adecuada a los incidentes que puedan producirse con respecto a su información, con el objetivo de disponer de un enfoque coherente y efectivo en dicha gestión. Esta respuesta adecuada debe ser **correcta, ágil y proporcional**, en este orden.
336. Dado que, como se suele decir, la seguridad total no existe, es necesaria una preparación conveniente ante la materialización de incidentes de seguridad que afecten en mayor o menor medida. Y ya que no se puede evitar que éstos se produzcan, sí se debe tratar de reducir al mínimo tanto su frecuencia como su impacto, garantizando que en caso de incidente la Organización sabrá responder de forma correcta ante el mismo, incluyendo la adquisición de conocimiento para que problemas similares no se produzcan en el futuro o si se producen su impacto sea mínimo.
337. La gestión de incidentes de seguridad, y en esto se hará hincapié en la presente guía, no se basa únicamente en la respuesta cuando se produce un incidente, sino que es un **proceso continuo** que debe ser implantado correctamente en las Organizaciones y que presenta actividades **antes, durante y después** de que un incidente ocurra. Ya que es imposible evitar con total garantía la materialización de incidentes, la Organización debe aprender de ellos para mejorar los mecanismos de seguridad desplegados e incrementar así su seguridad global. Aunque existen diferentes aproximaciones para identificar y diferenciar las etapas del ciclo de vida de la gestión de incidentes, todas tienen en común la separación entre los aspectos a abordar **antes** de que ocurra un incidente, los que es necesario realizar en la fase de **respuesta** pura y, finalmente, las tareas que corresponden a las **lecciones aprendidas**, a la **revisión y mejora** del proceso de gestión de incidentes y de la seguridad corporativa en su conjunto.
338. Diferentes modelos de gestión de incidentes definen fases en el ciclo de vida de la gestión, sin que exista un esquema único y comúnmente aceptado. No obstante, todos estos modelos tienen en común, tal y como se ha indicado, la identificación de tres grandes fases, las correspondientes a planificación, respuesta y periodo posterior (*aftermath*), tal y como se muestra en la figura siguiente:



339. Aunque se hablará en detalle de cada una de estas etapas a lo largo de la presente guía, es necesario destacar que en la primera de las fases del ciclo de vida de la gestión de incidentes, la correspondiente a **planificación**, se organizan las actividades de preparación ante la ocurrencia de incidentes: todas las tareas que la Organización debe ejecutar antes de dicho incidente. En la segunda etapa de **respuesta** pura al incidente de seguridad, se debe en primera instancia identificarlo para poder abordar su resolución de forma satisfactoria. Por último, en la etapa correspondiente al **periodo posterior** se engloban aquellas tareas relativas a las lecciones aprendidas en la gestión de incidente y a la mejora de la seguridad corporativa en su conjunto, incluyendo algunas actividades que habitualmente quedan fuera de la gestión de incidentes pura, como las denuncias o los peritajes.

## 9.2. DEFINICIONES

340. Un **incidente de seguridad** es un conjunto de uno o más eventos de seguridad no planificados y con una probabilidad significativa de comprometer las operaciones del negocio y amenazar a la seguridad corporativa. De esta definición se derivan dos consideraciones fundamentales a la hora de hablar de incidentes de seguridad:
- Es imposible predecir un incidente.
  - Es muy posible que el impacto asociado a un incidente sea alto.
341. Un incidente no tiene por qué constituir de forma obligatoria la materialización de un daño, sino puede que sencillamente sea una situación en la que ese daño puede materializarse con una probabilidad significativa según la definición anterior. De esta forma, el incremento relevante del nivel de amenaza o de impacto asociados a una situación concreta pueden ser considerados incidentes para la Organización, con independencia de que el impacto llegue efectivamente a materializarse.

342. Para hacer frente a los incidentes de seguridad las organizaciones deben establecer una **capacidad de respuesta** que les permita gestionar los incidentes de una forma acorde a sus políticas y requisitos de seguridad, con un ámbito, estructura y composición del equipo de gestión de incidentes adecuados. En el caso de las Administraciones Públicas españolas, a quienes va dirigida esta guía, es necesario destacar la existencia y trabajo del **CCN-CERT**, la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, cuyo objetivo principal es contribuir a la mejora del nivel de seguridad de los sistemas de información de las tres administraciones públicas existentes en España (general, autonómica y local) y entre cuyos servicios destaca el soporte y coordinación para la resolución de incidentes de seguridad que tengan la Administración General del Estado, las administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas, tal y como se indica en su propia página web (<http://www.ccn-cert.cni.es/>).

### 9.3. GESTIÓN DE INCIDENTES DE SEGURIDAD

343. La gestión de incidentes en la Organización es un proceso que debe comenzar mucho antes de que se materialice un incidente concreto; así, la primera etapa de la gestión de incidentes corresponde a la **preparación**, en la que la Organización debe realizar las tareas necesarias para detectar posibles incidentes y poderlos gestionar de forma adecuada si se materializan. Es necesario destacar que la fase de preparación y planificación es vital en una gestión correcta de incidentes, repercutiendo no únicamente en la minimización de un posible impacto sino también en una mejora global de la seguridad corporativa.
344. Tras la fase de preparación en la gestión de incidentes entra en juego la fase de **respuesta** pura, donde en una fase caliente –respuesta inmediata- y una fase fría se deben ejecutar las tareas destinadas a la identificación, contención, erradicación y recuperación del incidente, sus causas y sus efectos. Para finalizar la gestión, es necesario definir un **periodo posterior** donde, con las lecciones aprendidas en primer lugar y acciones que exceden el ámbito de la gestión pura de incidentes –como el análisis forense- en segundo lugar, se pueda realimentar de nuevo la fase de preparación, cerrando así el ciclo y garantizando la mejora continua de la gestión de incidentes corporativa.
345. Todo el proceso de gestión de incidentes, desde la notificación y detección tempranas hasta el periodo posterior a la respuesta, debe estar convenientemente documentado en la Organización. Debe definirse un procedimiento de gestión de incidentes que marque la operativa de al menos los siguientes aspectos:
- Responsabilidades y autorizaciones.
  - Notificación.
  - Clasificación.
  - Determinación de criticidad.
  - Respuesta.
  - Lecciones aprendidas.

346. Para coordinar la gestión de un incidente la Organización debe asignar un **responsable de la gestión**, un miembro del equipo de gestión de incidentes que será el máximo responsable de la respuesta proporcionada y actuará también como interlocutor entre la Organización y terceros cualesquiera involucrados en la resolución del incidente. Para poder asumir estas funciones, el responsable de la gestión centralizará toda la información y actuaciones relativas al incidente, actuando como punto único de contacto y obteniendo una visión global de la situación que le permita tomar las decisiones adecuadas para la resolución del problema.

### 9.3.1. DETECCIÓN DEL INCIDENTE

347. El primer paso necesario para lograr una gestión de incidentes adecuada a las necesidades de cualquier Organización pasa obligatoriamente por **monitorizar** los posibles elementos que puedan generar situaciones que comprometan la seguridad, detectando dichas situaciones y permitiendo a un equipo de personas actuar de la forma conveniente en cada caso. Aunque los elementos a monitorizar son muchos, debe considerarse obligatoria al menos la monitorización del entorno tecnológico propio, sobre los elementos necesarios para garantizar los servicios que la Organización presta y en los términos y umbrales necesarios para garantizar la calidad del servicio ofrecido.
348. Los eventos de seguridad deben ser registrados en la Organización según lo expuesto con anterioridad, a la hora de hablar del registro de los incidentes. Sobre este registro, realizado habitualmente de forma centralizada y con un producto de los denominados SIEM, un equipo humano concreto procesará los diferentes eventos, determinando en un análisis *first cut*, si son o no relevantes para la seguridad corporativa. Este equipo no tiene por qué ser el propio equipo de gestión de incidentes de la Organización, sino que con frecuencia es un grupo de Service Desk u Operación 24x7 que procesa no únicamente eventos de seguridad, sino todo tipo de incidencias, consultas, problemas... resolviendo algunos de ellos de forma directa y escalando el resto a áreas especialistas, en el caso de los posibles incidentes mediante diferentes mecanismos de notificación.

### 9.3.2. NOTIFICACIÓN DEL INCIDENTE

349. La Organización debe implantar canales que permitan al personal de la Organización (se debe evaluar además la conveniencia de extender estos canales a personal ajeno, en determinadas ocasiones) la notificación de posibles incidentes de una forma adecuada. Este mecanismo de notificación será de aplicación para notificar incidentes tanto por parte de equipos de Service Desk u Operación 24x7 –que como se ha indicado, habitualmente son los primeros en procesar un evento de seguridad y determinar en primera instancia si puede estar asociado a un incidente relevante- como por parte del resto de la Organización o por terceros autorizados.
350. Los canales de notificación de incidentes deben ser especialmente **ágiles**, ya que la detección y alerta temprana es vital para que el impacto asociado a un incidente sea el menor posible. La Organización debe ser capaz de ofrecer a su personal diferentes canales para notificar una situación anómala que pueda estar ligada a un incidente: correo electrónico, teléfonos, aplicaciones *ad hoc*, FAX...

Además, estos medios deben estar convenientemente publicitados en la Organización y ser conocidos por todo el personal relevante, de forma que cualquier persona que requiera realizar una notificación sepa en todo momento cómo hacerlo y deben ser probados regularmente, al menos de forma trimestral, para garantizar que su funcionamiento, en caso de requerirse, es correcto.

### 9.3.3. RESPUESTA AL INCIDENTE

351. Una vez el equipo de gestión de incidentes determina tras un análisis inicial que un evento o notificación debe categorizarse como relevante y debe llevar asociada una actuación ante el incidente comienza la etapa de **respuesta**, compuesta por acciones encaminadas a identificar, contener y erradicar el incidente, para recuperar después la operativa estándar del entorno afectado.
352. Las primeras actuaciones que debe realizar el equipo de gestión de incidentes en la fase de respuesta pasan por conocer la situación e intentar obtener una primera impresión del origen del incidente, en lo que se denomina la etapa de **identificación**. La primera tarea de esta etapa debe ser determinar si realmente el equipo se enfrenta a un incidente. Aunque se haya realizado un análisis inicial, el responsable debe **confirmar** que el evento detectado o la notificación que se ha hecho al equipo constituyen realmente un incidente que requiere de una gestión determinada, ya que en ocasiones el equipo se enfrenta a falsos positivos a pesar de haber realizado ese análisis *first cut*.
353. Una vez confirmada la materialización de un incidente de seguridad comienza en la gestión del mismo la etapa de **contención**, cuyo objetivo es evitar que el alcance de un incidente se incremente, y por tanto lo haga el impacto de dicho incidente en el servicio afectado. Habitualmente la fase de contención se divide en dos partes: la contención a corto plazo, que pretende detener la propagación sin alterar los elementos afectados (esto es, preservando evidencias) y la contención a largo plazo, etapa en la que ya se introducen cambios en los elementos afectados por el incidente y que debe ser abordada una vez se ha tomado la información necesaria para posibles análisis forenses posteriores.
354. Se debe conservar una descripción detallada de cada evidencia recogida, incluyendo:
  - a. Datos de identificación (localización, número de serie del equipo, nombre, modelo, dirección IP, MAC, etc.).
  - b. Nombre, cargo y número de teléfono de la persona o personas que han recogido la prueba.
  - c. Fecha y hora de aparición de la prueba.
  - d. Lugar de almacenamiento de la evidencia.
355. Tras la contención del incidente comienza la fase de **erradicación**, esto es, la eliminación total de los elementos que han posibilitado o potenciado el incidente o pueden volver a generarlo: cuentas de usuario generadas por un tercero durante el incidente, aplicaciones instaladas por un atacante, código malicioso instalado en los sistemas afectados, etc. En definitiva, en esta fase el equipo de respuesta debe “limpiar” los entornos afectados antes de devolverlos a su operativa estándar, tarea para la cual será necesario reinstalar por completo sistemas y

aplicaciones afectados y bastionarlos convenientemente antes de devolverlos al entorno de producción. Además, deberá realizarse una verificación funcional y otra verificación de seguridad para dar la fase de erradicación por concluida.

356. Una vez erradicado el incidente y una vez el equipo de respuesta dispone de entornos de trabajo limpios y verificados, comienza la fase de **recuperación**, cuyo objetivo es devolver a los entornos afectados por el incidente a su operativa estándar, de forma segura y recuperando el funcionamiento normal de la Organización. Adicionalmente, dado que los entornos se han visto afectados por un incidente, en esta etapa deberán aplicarse salvaguardas adicionales (temporales o permanentes) con el objeto de garantizar que el incidente no vuelve a producirse.

#### 9.3.4. PERIODO POSTERIOR

357. La primera tarea en la fase de periodo posterior o *aftermath*, y de hecho la única que obligatoriamente deberá ser abordada por la Organización durante la gestión de un incidente, corresponde con lo que se denomina **lecciones aprendidas**. En esta etapa, el equipo de gestión de incidentes debe generar un **informe de actuación** que recopile todos los datos relativos a la gestión, las acciones emprendidas en cada etapa de la respuesta, las conclusiones obtenidas y, en especial, las directrices de mejora a abordar para que incidentes similares no vuelvan a producirse o si se producen su impacto sea menor para la Organización.
358. La Organización debe definir la estructura concreta y la información a reflejar en el informe, contemplando al menos la siguiente información:
- Datos de registro inicial especificados en el apartado correspondiente de la presente guía (identificador, originador, criticidad, clasificación...).
  - Resumen ejecutivo.
  - Relación con eventos de seguridad registrados por la Organización.
  - Identificación del responsable de gestión del incidente.
  - Datos generales del incidente:
  - Descripción.
  - Causas.
  - Catalizadores.
  - Impacto en la Organización.
  - Bitácora de la gestión del incidente.
  - Informe del GIR, especificando Jefe de Equipo y acciones emprendidas con el detalle suficiente en cada caso.
  - Resumen de la resolución del incidente:
  - Acciones ejecutadas, identificando responsables si es necesario.
  - Notificaciones realizadas, tanto internas a la Organización como externas.

- o. Fecha y hora de cierre del incidente.
  - p. Análisis posterior:
  - q. Costes asociados al incidente.
  - r. Relaciones con otros incidentes en la Organización.
  - s. Directrices de actuación.
  - t. Opciones de mejora:
  - u. Identificación de controles.
  - v. Planificación de la implantación.
  - w. Responsables.
  - x. Verificación de controles.
359. Las lecciones aprendidas, tal y como se ha indicado previamente, realimentan a la fase inicial del ciclo de vida de la gestión de incidentes, la correspondiente a la preparación para la respuesta, de forma que se mejoren en especial los procedimientos operativos de gestión de incidentes y las capacidades de monitorización de la Organización, reforzando así la seguridad corporativa y cerrando el ciclo de la gestión de incidentes

#### **9.4. INCIDENTES EN SISTEMAS QUE MANEJAN INFORMACIÓN CLASIFICADA**

360. En la gestión de incidentes en Sistemas que manejan información clasificada, se debe comunicar inmediatamente la aparición del mismo a la Autoridad Operativa del Sistema y éste, dependiendo del tipo de información involucrada, a la Autoridad responsable de la acreditación. El equipo involucrado en la resolución del incidente debe disponer de la habilitación de seguridad correspondiente.
361. Se debe determinar si ha sido comprometida información clasificada y, en su caso, de qué información se trata, su clasificación, número, fecha, originador, objeto y alcance. Adicionalmente, se debe indicar el período durante el cual ha sido expuesta o comprometida así como una estimación, si es posible, del número de personas que han accedido a ella. El originador de la información debe ser notificado del incidente.
362. Durante la gestión del incidente, la Autoridad Operativa del Sistema debe ser informada periódicamente. Una vez resuelto o si han transcurrido noventa (90) días desde la aparición del mismo, se debe elaborar y entregar un informe a la Autoridad Operativa del Sistema.
363. Toda la información relativa al incidente debe ser mantenida y almacenada de acuerdo con la clasificación de la información comprometida.

#### **9.5. ACTORES Y RESPONSABILIDADES**

364. El proceso de gestión de incidentes debe venir liderado por un grupo de trabajo que con toda probabilidad se enmarcará en un departamento o área de Seguridad, con la nomenclatura correspondiente en cada Organización. Este equipo puede estar compuesto por personal interno a la Organización, externo o



una combinación de ambos, tal y como se muestra más adelante en esta misma guía.

365. Para que la gestión de incidentes sea eficiente y completa en la Organización, el equipo de gestión de incidentes debe tener el apoyo de una serie de áreas o grupos de trabajo internos a la Organización, así como relaciones habituales o puntuales con actores ajenos a ésta pero relevantes, por uno u otro motivo, en la gestión de incidentes de seguridad. En este punto se exponen algunos de los actores –de nuevo, con independencia de la denominación o estructura organizativa en cada caso- con los que el equipo de gestión de incidentes debe trabajar, indicando para cada uno de ellos el tipo de interacción requerido:

#### 9.5.1. ACTORES INTERNOS

##### 9.5.1.1. Dirección corporativa

366. Como cualquier área dentro de la Organización, el trabajo del equipo de gestión de incidentes viene marcado por las prioridades y requisitos del servicio establecidos desde la Dirección, y por tanto será ésta quien defina aspectos como el presupuesto, composición o política a alto nivel del equipo. Adicionalmente, en la gestión de incidentes especialmente relevantes es habitual el *reporting* periódico a la Dirección, que será en muchas ocasiones quien deba asumir la responsabilidad en relación a iniciativas emprendidas, impacto causado, etc.

##### 9.5.1.2. Departamento de Seguridad

367. Como se ha indicado previamente, el equipo de gestión de incidentes estará englobado en un Departamento de Seguridad, departamento que a su vez tendrá otros servicios hacia la Organización, por ejemplo los relativos a protección física. El responsable de la gestión de un incidente debe disponer durante la fase de respuesta de autoridad sobre otros grupos del departamento para, en caso de ser requerido, obtener de éstos apoyo inmediato en esta fase de respuesta: seguridad física para acceso a ubicaciones protegidas, seguridad lógica para habilitación o deshabilitación temporal de controles, protección de negocio para investigaciones...

##### 9.5.1.3. Departamentos TI

368. Los departamentos tecnológicos constituyen un apoyo elemental en la gestión de un incidente en el que entre en juego un componente técnico –no en todos será así-. Áreas como Sistemas, Comunicaciones, Desarrollo... poseen, además de unos conocimientos técnicos muy específicos, un conocimiento también profundo de la tecnología en la Organización desde el punto de vista del servicio ofrecido: criticidades de los diferentes activos, horarios de mínimo impacto... Ambas capacidades son de especial utilidad en la fase caliente de la respuesta, en la que es posible que se interrumpan ciertos servicios o que haya que tomar decisiones en relación a cambios tecnológicos sobre activos relevantes (apagado, cambios de políticas de seguridad, bloqueo de usuarios...).

##### 9.5.1.4. Departamento Jurídico

369. Tal y como se expone en la presente guía, la gestión de incidentes debe tener un soporte legal muy amplio en todas sus fases, desde la monitorización y el análisis de datos hasta posibles denuncias o peritajes en periodos posteriores de la gestión. Por este motivo, la relación entre el equipo de gestión de incidentes – en realidad, del Departamento de Seguridad en su conjunto- y el Departamento Jurídico debe ser muy fluida, revisando éste todos los procedimientos, instrucciones, políticas... de trabajo del equipo para garantizar que respetan la legislación vigente en cada caso, y transmitiendo además al equipo de gestión las implicaciones de nueva legislación o modificaciones de la actual que puedan repercutir en su trabajo.

#### 9.5.1.5. Recursos Humanos

370. En ocasiones los incidentes vienen motivados o potenciados por atacantes internos, *insiders*, que con o sin mala fe causan un impacto en la Organización. Por este motivo, sin perjuicio de posibles actuaciones legales, la Organización puede decidir emprender procedimientos disciplinarios contra personal interno, proceso en el que se puede requerir del apoyo del Departamento de Recursos Humanos corporativo.

#### 9.5.1.6. Comunicación

371. Ciertos incidentes tienen una repercusión en medios de comunicación o en el público en general que escapa al ámbito técnico del equipo de gestión de incidentes. Los departamentos de Prensa o Comunicación pueden ser relevantes en estas situaciones, canalizando –en coordinación con el responsable de la gestión del incidente- cualquier comunicación a terceros relativa a la situación, impacto, orígenes, etc.

### 9.5.2. ACTORES EXTERNOS

#### 9.5.2.1. FFCCSE

372. El Departamento de Seguridad donde se engloba el equipo de gestión de incidentes debe mantener una comunicación bidireccional con las Fuerzas y Cuerpos de Seguridad del Estado con competencias en el ámbito de la Organización. Dicha comunicación debe servir, entre otros, para que la Organización acceda a información relevante que pueda ser indicativa de una nueva amenaza o de la modificación de riesgo asociado a una amenaza existente, para facilitar a FFCCSE información relativa a delitos en el ámbito de la Organización y para coordinar cualquier actuación con los cuerpos de seguridad por parte del Departamento, obteniendo así una respuesta más eficiente, todo ello a través de los canales formales habilitados a tal efecto (con independencia de cualesquiera relaciones personales).

#### 9.5.2.2. CERT/CSIRT

373. El equipo de gestión de incidentes debe establecer relación con equipos de respuesta a incidentes externos a la Organización, en especial con aquellos en cuyo ámbito de actuación pueda encontrarse la Organización o parte de ella. De

estos equipos se obtiene información relevante en la gestión de incidentes de seguridad, así como apoyo operativo bajo ciertas circunstancias, por lo que la Organización debe analizar qué centros de respuesta están en su ámbito de actuación y establecer las relaciones apropiadas en cada caso.

374. En el ámbito de las Administraciones Públicas españolas, público de la presente guía, es especialmente relevante la relación de los equipos de gestión de incidentes con el CCN-CERT, el CERT gubernamental español. En este caso concreto, los equipos de gestión de incidentes deben mantener un contacto formal y periódico con el CCN-CERT, además de una notificación extraordinaria ante la gestión de diferentes incidentes considerados relevantes.

#### 9.5.2.3. Fabricantes/proveedores

375. Dentro de la fase de preparación de la gestión de incidentes, los equipos de gestión deben establecer contacto con proveedores o fabricantes de productos y sistemas de uso en la Organización, con el objetivo de tener acceso a información relativa a su seguridad –en especial a sus vulnerabilidades–, soporte para bastionado, acceso a parches y actualizaciones, etc. Habitualmente esta relación se mantiene a través del propio contrato de soporte entre la Organización y el proveedor concreto en cada caso.
376. Aparte del acceso a información significativa, es relevante el papel del proveedor en la respuesta a incidentes que puedan afectar de una u otra forma a sus productos o sistemas, ya que es dicho proveedor el que habitualmente dispone de los mayores expertos en sus productos y por tanto el que nos puede proporcionar un apoyo técnico muy especializado en caso de ser necesario.

## IV. SEGURIDAD LÓGICA

## 10. SOFTWARE MALICIOSO

### 10.1. INTRODUCCIÓN

377. El software malicioso, en inglés *malicious software* (comúnmente conocido como *malware*, *badware* o software malintencionado), es un término general muy utilizado por profesionales de la informática y las telecomunicaciones para definir una variedad de software o programas de códigos hostiles o intrusivos cuya función es dañar el sistema o causar un mal funcionamiento, tanto por pérdida de datos como por pérdida de productividad.
378. A día de hoy, la expresión **virus informático** es utilizada incorrectamente en el lenguaje cotidiano, a menudo incluso en los medios de comunicación para describir todos los tipos de amenazas asociadas al *malware*, cuando en realidad un virus informático es un tipo de *malware* concreto. Dentro del software, hace unos años, los virus constituían la principal amenaza para los equipos informáticos, pero hoy en día han quedado relegados a un segundo plano ya que otros tipos de *malware* han cobrado importancia. El comportamiento de los virus se puede resumir en que son programas que se reproducen infectando otros ficheros o aplicaciones (necesitan un huésped, como un virus biológico) y realizan acciones perjudiciales para el usuario. Con posterioridad aparecieron los **gusanos** (otro tipo de *malware*), programas que no necesitan infectar otros ficheros para reproducirse y que se propagan realizando copias de sí mismos, con el fin de colapsar las redes en las que se infiltran. También aparecieron otros tipos de *malware*, como los **troyanos** (similares al Caballo de Troya, aparentemente inofensivos pero con una función oculta, generalmente introducirse en un sistema para robar información o generar un acceso no autorizado) o las puertas traseras (**backdoors**, *malware* que evita los controles de acceso e identificación y autenticación de usuarios, permitiendo accesos no controlados a un entorno).
379. Por tanto, se denomina *software* malicioso o *malware* a todo aquel *software* que tiene como objetivo degradar la seguridad de un entorno sin el conocimiento de su propietario y con finalidades muy diversas, ya que en esta categoría se puede encontrar desde un virus tradicional hasta un *spyware*. Los objetivos del *malware* actualmente son muy variados, pero entre ellos destacan la obtención de información sensible, el daño a la máquina donde se encuentra instalado el software o la ejecución de estafas online, por poner unos ejemplos.
380. La evolución del malware ha sufrido un cambio a lo largo de los últimos años, en los que ha pasado de ser *software* creado a título individual o por un pequeño grupo de piratas informáticos con fines reivindicativos, egocéntricos o de simple satisfacción personal, a ser producido por mafias organizadas (ciberdelincuencia) cuyo único fin es el lucro económico. Debido a estos nuevos fines, a lo que se une la generalización del uso de la informática y del acceso a Internet, en estos años se han generado diversos tipos de *malware* nuevo para lograr el objetivo de estas mafias: ganar dinero. Estos nuevos tipos de malware cada día están más perfeccionados y son más abundantes en la red, razón por la cual existen más programas nocivos y cada vez más peligrosos. La creación de *software* malicioso ya no requiere un elevado conocimiento sobre informática y el *malware* es cada vez más fácil de crear. El intercambio de información en

redes sociales, el uso creciente del correo electrónico, la compartición de ficheros en redes P2P o la navegación web a través de Internet hacen que su distribución sea cada vez más rápida, constituyendo a día de hoy una de las principales vías de infección en los sistemas de información. Así, aparte de los ya conocidos virus, gusanos, troyanos o puertas traseras, cabe incluir dentro del malware **nuevas amenazas** como las siguientes:

- a. Dialer. *Malware* que trata de establecer una conexión telefónica con un número de tarificación especial.
- b. Programa espía (*spyware*). Programa que recoge datos acerca de hábitos de uso de Internet y los envía a empresas de publicidad.
- c. Hoax. Envío de mensajes de correo electrónico con advertencias sobre falsos virus u otro tipo de engaños (bulos).
- d. Spam. Envío indiscriminado de mensajes publicitarios no solicitados a través del correo electrónico.

## 10.2. CÓDIGO MALICIOSO O MALWARE

381. Tal y como se ha indicado, cuando se habla de código malicioso o malware se está haciendo referencia a programas que se instalan en un sistema TIC, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los sistemas operativos, aplicaciones y datos de dicho sistema, o bien simplemente para molestar o perjudicar al usuario.
382. Puesto que no todo el código malicioso es igual, establecer una clasificación es complicado. Cada día surgen nuevas muestras de *malware* susceptibles de mutar o transformarse adquiriendo nuevas funcionalidades y capacidades de ocultación. Aún así se establecerá una clasificación básica a continuación sobre los tipos de malware más comunes que se pueden encontrar en el panorama actual.

### 10.2.1. VIRUS

383. Los virus son programas que se reproducen infectando ficheros e intentando que esos ficheros sean accedidos en otro entorno para que éste también sea infectado. Los virus pueden ser desde cómicos o bromistas hasta programas destructivos. Estas dos características son las fundamentales para denominar virus a un malware: la infección de archivos –denominados huésped- y la ejecución de acciones dañinas o molestas.
384. Pese a que existe un gran número de tipos de virus, principalmente se pueden clasificar en tres grandes familias:
  - a. Aquellos que se encargan de dañar el arranque de una máquina impidiendo que ésta pueda iniciarse correctamente. Su objetivo es puramente destructivo.
  - b. Aquellos que residen en la memoria de la máquina y son capaces de funcionar en segundo plano sin que el usuario conozca la existencia de dicho virus.

- c. Por último, pero no por ello menos peligrosos, existen los virus de macros o *script*, que suelen aprovechar la capacidad de ejecutar diferentes lenguajes de programación de algunos de los visores de documentos más utilizados: XLS (Excel), DOC (Word), PPS (PowerPoint), PDF (Acrobat Reader), etc., para infectar el equipo.
385. Del mismo modo que los virus biológicos se introducen en el cuerpo humano e infectan una célula, que a su vez infectará nuevas células al inyectar su contenido en ellas, los virus informáticos se introducen en los sistemas e infectan ficheros insertando en ellos su código. Cuando el programa infectado se ejecuta, el código entra en funcionamiento y sigue extendiéndose. Además, ambos tipos de virus (biológico e informático) suelen presentar síntomas que avisan de su presencia.
386. Como se ha indicado, una infección vírica tiene lugar cuando se ejecuta el código que contiene el virus. Cabe destacar diferentes vías de infección, como el uso de software pirata, las aplicaciones descargadas de sitios no oficiales en Internet, las redes de compartición de información (como las P2P) o el intercambio de documentos (archivos ofimáticos, PDF, etc.) infectados, normalmente adjuntos a correos electrónicos. En un entorno corporativo, este último problema es especialmente grave, considerando que uno de los principales riesgos proviene de los virus que están encubiertos en ficheros facilitados por personas conocidas, ya sea por correo electrónico, *pendrives* o cualquier otro medio de intercambio de datos. Por ejemplo, alguien conocido puede enviar un correo electrónico con un documento malicioso, sin ninguna mala intención -ya que desconoce que el documento está contaminado-, y al abrirlo en otro equipo éste quedará contaminado y repetirá el proceso, sin saberlo, enviando de nuevo el documento contaminado a otras personas e infectando así a otros usuarios. El reenvío de cadenas de correos, que suelen ser de humor o curiosidades que se envían mediante ficheros adjuntos de PowerPoint, supone un peligro potencial muy considerable, ya que muchos de estos ficheros están infectados con algún tipo de *malware* y la propagación de los mismos únicamente depende del usuario.
387. Los virus informáticos históricamente han tenido una mayor presencia en los sistemas operativos Microsoft Windows, pero esto no quiere decir que su incidencia sea nula en otros sistemas operativos: existen virus para Linux o MacOS X, por poner solo unos ejemplos. Aunque existe un buen número de productos comerciales que detectan virus (los conocidos antivirus), éstos no son infalibles, ya que en su mayor parte sólo son capaces de detectar virus o patrones víricos conocidos. Por tanto, es necesario que para mitigar el riesgo asociado a la contaminación vírica se cuente, además de con un antivirus continuamente actualizado, con medidas y procedimientos para proteger, reaccionar y actuar contra incidentes asociados a malware. Adicionalmente, se debe concienciar a los usuarios del entorno de que el mejor antivirus es la prevención y el sentido común.

#### 10.2.2. CABALLOS DE TROYA

388. De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocían, y que tenía una



función muy diferente a la que ellos pensaban, un troyano o caballo de Troya actual es un programa que aparentemente realiza una función útil para quien lo ejecuta, pero que en realidad ejecuta una acción que el usuario desconoce, generalmente dañina. A diferencia de los virus, un troyano no se reproduce infectando otros ficheros ni se propaga haciendo copias de sí mismo como hacen los gusanos.

389. Los efectos de los troyanos **pueden ser muy peligrosos**. Permiten realizar intrusiones o ataques contra el sistema afectado que pueden causar un serio impacto en la seguridad corporativa, pudiendo permitir, entre otras acciones, las siguientes:
- Tener acceso a información sensible (contraseñas, datos bancarios, etc.)
  - Realizar cambios en el registro y archivos de configuración.
  - Tomar el control del sistema de manera parcial o completa.
  - Utilizar el sistema comprometido para atacar a otros sistemas.
  - Acceder a otra información almacenada o transmitida por la red.
  - Instalar canales encubiertos (*covert channels*).
390. La primera acción que realiza un Caballo de Troya habitualmente es mantenerse oculto mediante la modificación de parámetros del sistema y propiedades de ficheros, como la fecha, el tamaño o incluso el *checksum* para aparentar ser idéntico a un programa legítimo, a la vez que reemplaza los programas de sistema con sus propias versiones para impedir la detección.
391. Las firmas de los troyanos conocidos suelen estar incluidos en los antivirus. El riesgo adicional es que este tipo de malware suele modificar el comportamiento de los antivirus incluso si la búsqueda heurística está activa. Este riesgo solo puede ser contrarrestado observando estrictamente reglas para uso de software autorizado e instalando programas de control de integridad.
392. Algunos ejemplos de troyanos muy conocidos son *Autorooter*, *Zasi*, *Webber* o *Zeus*.

### 10.2.3. GUSANOS

393. El término gusano, acuñado en 1975 en la obra de ciencia ficción de John Brunner *The Shockwave Rider*, hace referencia a programas capaces de viajar por sí mismos a través de redes de computadores para realizar cualquier actividad una vez alcanzada una máquina. Aunque esta actividad no tiene por qué entrañar peligro, el concepto de gusano actual –sobre todo cuando se habla de *malware*– es obviamente negativo. Los gusanos son programas muy similares a los virus, ya que también se auto replican y tienen efectos dañinos para los sistemas, pero se diferencian de éstos en que no necesitan infectar otros ficheros para reproducirse.
394. Básicamente, los gusanos se limitan a realizar copias de sí mismos, sin alterar necesariamente ningún otro fichero, pero se reproducen a tal velocidad que pueden colapsar por saturación las redes en las que se infiltran. Los gusanos pueden acceder al sistema utilizando métodos como el *password cracking*, explotando un mecanismo de puerta trasera (*backdoor*) o explotando

vulnerabilidades en las aplicaciones utilizadas en el sistema que permitan el acceso al mismo, por poner solo unos ejemplos.

395. El 2 de noviembre de 1988, Robert T. Morris saltó a la fama cuando uno de sus programas se convirtió en “el Gusano” con mayúsculas, en el *Worm* de Internet. Este *malware* aprovechaba vulnerabilidades en programas muy utilizados en el entorno Unix de la época y motivó que en pocas horas miles de equipos conectados a Internet dejaran de funcionar. Fueron necesarias muchas horas de trabajo para detener esta infección, y a partir de este incidente se instauró el primer CERT con el objetivo de hacer frente a este tipo de situaciones. En la actualidad, los gusanos se extienden principalmente a través del correo electrónico o de dispositivos extraíbles, como los conocidos *I Love You*, *Navidad*, *Pretty Park*, *Happy99*, *ExploreZip*, *Conficker* o *Stuxnet*.

#### 10.2.4. BOMBAS LÓGICAS

396. Una bomba lógica es un programa que se activa bajo ciertas circunstancias, como una determinada fecha, la existencia de un fichero con un nombre dado, o el alcance de cierto número de ejecuciones de un programa que contiene la bomba. Así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba se materializa. En muchas ocasiones las bombas lógicas se encuentran embebidas en otros programas que son ejecutados internamente por personal con acceso directo al sistema.
397. Algunas acciones que puede realizar una bomba lógica al ser activada son las siguientes:
- Borrar información del disco duro.
  - Enviar información a un tercero.
  - Apagar el monitor.
  - Mostrar un mensaje por pantalla.
398. Las contramedidas frente a bombas lógicas se deben basar en una configuración adecuada de software y en procedimientos de control empleando software cuyo uso esté aprobado en la Organización y haya sido obtenido de fuentes confiables; debido a que en muchos casos se trata de *malware* dirigido, las bombas lógicas son muy difíciles de detectar sin indicaciones previas de actividad.

#### 10.2.5. CÓDIGO MÓVIL MALICIOSO

399. El denominado código móvil malicioso es *software* que es transmitido desde un sistema remoto para ser ejecutado en un sistema local, típicamente sin consentimiento explícito del usuario. Se han convertido en un medio popular de escribir programas que pueden ser utilizados por diferentes sistemas operativos y aplicaciones como navegadores web y clientes de correo.
400. Aunque el código móvil puede ser benigno, los atacantes han aprendido a utilizarlo como medio efectivo para atacar sistemas y también como mecanismo para transmitir virus, gusanos y troyanos a otras estaciones de trabajo. Este tipo

de código malicioso difiere significativamente de virus y gusanos en que no infectan archivos o intentan propagarse por sí mismos; en su lugar, explotan vulnerabilidades particulares al aprovecharse de los privilegios por defecto asignados al código móvil.

401. Entre los lenguajes populares para el desarrollo de código móvil malicioso se incluye Java, ActiveX, JavaScript y VBScript.

#### 10.2.6. PUERTAS TRASERAS

402. Las puertas traseras son trozos de código en un programa que permiten a quien conoce su funcionamiento saltarse los métodos usuales de autenticación para realizar cierta tarea. Habitualmente son insertados por los programadores para agilizar la tarea de probar su código durante la fase de desarrollo del mismo y se eliminan en el producto final, pero en ciertas situaciones el programador puede mantener estas puertas traseras en el programa funcional, ya sea deliberada o involuntariamente. Por ejemplo, una aplicación que para realizar cualquier tarea de seguridad solicita a quien lo ejecuta cinco claves diferentes. Evidentemente, durante la fase de desarrollo es muy incómodo para el programador teclear estas contraseñas antes de ver si el producto funciona correctamente, por lo que es muy común que esta persona decida incluir una rutina en el código de forma que si la primera clave proporcionada es una determinada no se soliciten las cuatro restantes. Esta situación, aceptable durante la fase de desarrollo, se convierte en una amenaza a la seguridad si se mantiene una vez el producto está instalado en el entorno de producción: cualquiera que conozca la clave inicial puede saltarse todo el mecanismo de protección del programa.
403. En la actualidad las puertas traseras habituales suelen permitir el control total del equipo afectado. Una vez contaminado un sistema –a través de los medios habituales: ejecución de código malicioso, correo electrónico...- las acciones permitidas por las *backdoors* pueden resultar muy perjudiciales. Entre ellas se encuentran la eliminación de ficheros o la destrucción de la información del disco duro, capturar y reenviar datos confidenciales a un actor externo o abrir puertos de comunicaciones, permitiendo que un posible intruso controle el sistema de forma remota.
404. Algunos ejemplos de backdoors conocidos son Orifice2K.sfx, Bionet.318, Antilam o Subseven.213.

#### 10.2.7. HOAXES

405. Los *hoaxes* son correos electrónicos cuyo contenido es falso -aunque el remitente sea legítimo- y son enviados de forma masiva por parte de usuarios que consideran como verdadero dicho contenido, generando así ruido en la red y en el buzón de quien lo recibe, y facilitando la captación de direcciones de correo electrónico por parte de un tercero malintencionado que, posteriormente, las podría utilizar para atacar a dichos usuarios. Aunque se trata de un *malware* especial que no realiza un daño directo sobre el equipo del usuario, sí que se considera nocivo por los motivos expuestos con anterioridad.

406. Ejemplos típicos de hoax son las cadenas de correo electrónico que proporcionan datos falsos sobre atentados, campañas benéficas de grandes empresas a cambio de un simple correo electrónico o niños con enfermedades gravísimas que buscan apoyo. Obviamente, se trata de datos falsos o rumores que, aprovechando la buena fe de los usuarios, se propagan por la red a través del correo electrónico y permiten a un atacante planificar un daño más directo contra los usuarios. Por supuesto, se debe desconfiar de cualquier información de este tipo que llegue al correo -incluso si proviene de personas conocidas- y notificar a estas personas que están enviando un hoax, un falso rumor en la red. Si se recibe un *hoax*, no hay que hacer caso de sus advertencias e instrucciones: lo más aconsejable es borrarlo sin prestarle la más mínima atención y, por supuesto, no reenviarlo a otras personas.

#### 10.2.8. PHISHING

407. El *phishing* (del inglés *fishing*, "pescando") no es en sí un *malware* puro, aunque hay que citarlo como elemento *software* que causa un daño ejecutando acciones sin que el usuario las perciba. Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.
408. Existe un amplio abanico de software y aplicaciones de toda índole que quedan clasificados dentro de la categoría de robo de información personal o financiera, algunas de ellas realmente complejas, como el uso de una ventana Javascript flotante sobre la barra de direcciones del navegador con el fin de confundir al usuario.
409. Algunas de las características más comunes que presentan los mensajes de correo electrónico utilizados para realizar phishing son las siguientes:
- Uso de nombres de compañías existentes y de confianza.
  - Utilizar el nombre de un empleado, o departamento, real de una empresa como remitente del correo falso.
  - Direcciones web con la apariencia correcta.
  - Factor miedo.
410. Para lograr su objetivo, este tipo de malware, además de la ocultación de la URL fraudulenta en un correo electrónico aparentemente real, también utiliza otras técnicas más sofisticadas:
- Man-in-the-middle* (hombre en el medio). En esta técnica, el atacante se sitúa entre el usuario y el sitio web real, actuando a modo de *proxy*.
  - Aprovechamiento de vulnerabilidades de tipo *Cross-Site Scripting* que permiten simular una página web segura de una entidad bancaria.
  - Aprovechamiento de vulnerabilidades del navegador en el cliente, que permiten mediante el uso de *exploits* falsear la dirección que aparece en dicho navegador.

- d. Algunos ataques de este tipo también hacen uso de *exploits* en sitios web fraudulentos que, aprovechando alguna vulnerabilidad del navegador o del sistema operativo del cliente, permiten descargar troyanos de tipo *keylogger* que robarán información confidencial del usuario.
- e. Otra técnica más sofisticada es la denominada **pharming**. Se trata de una táctica fraudulenta que consiste en cambiar los contenidos del DNS (*Domain Name Server*, Servidor de Nombres de Dominio) ya sea a través de la configuración del protocolo TCP/IP o del archivo correspondiente en cada sistema operativo, para redirigir los navegadores a páginas falsas.

#### 10.2.9. ROGUE SOFTWARE

- 411. El *rogue software* es un *malware* que aparenta ser una herramienta de desinfección (como un antivirus), pero que realmente no es más que un troyano que engaña al usuario haciéndole creer que primero tiene una infección y a continuación que este antivirus falso desinfecta la máquina. En la práctica, el *rogue software* no realiza ninguna acción beneficiosa para el usuario y es un *malware* tan perjudicial como un troyano o un virus -o más-.
- 412. Estas aplicaciones maliciosas tienen un gran auge y están generando una gran cantidad de dinero en la actualidad. Hay que tener en cuenta que el beneficio para la entidad que ha creado dicho *malware* es doble, ya que por un lado cobra por una falsa herramienta de desinfección y por otro instala *malware* para obtener información confidencial, pudiendo así, por ejemplo, obtener todas las contraseñas y datos que introduzca el usuario.
- 413. Normalmente este *software* se crea puntualmente incluyendo publicidad en páginas web para simular ante el cliente que realmente es un *software* legítimo y correcto. Además, se intentan modificar las opciones de los buscadores más importantes para que, al buscar el nombre del *malware* acompañado de palabras clave (por ejemplo “antivirus”), salga esta falsa herramienta de desinfección como la primera en la búsqueda. Por ello es importante comprobar que se instala software reconocido, que no es nuevo en el sector y que proviene de una fuente confiable.

#### 10.2.10. ADWARE

- 414. El *adware* es un *malware* que, más que dañar la máquina u obtener información confidencial del usuario, tiene como objetivo generar publicidad en el equipo de la víctima mediante múltiples ventanas sin que el usuario tenga ningún control sobre éstas.
- 415. Habitualmente, el *adware* se instala en el equipo al acceder a webs de contenido sexual, software pirata o publicidad (aunque técnicamente puede instalarse al acceder a cualquier tipo de página web). Es fácilmente reconocible, ya que cuando se navega por Internet, se generan un gran número de ventanas publicitarias en el sistema infectado.
- 416. Las recomendaciones para evitar este *malware* de forma preventiva es que nunca se instale ni se acepte ningún tipo de *plugin* o complemento cuando se navegue por páginas web de dudosa reputación o no confiables. De forma defensiva, se

recomienda emplear herramientas de desinfección de *adware* o antivirus de propósito general.

#### 10.2.11. OTRO SOFTWARE MALICIOSO

417. Hay que considerar la existencia de *software*, a menudo utilizado en combinación con *malware* puro, que constituye una seria amenaza para los Sistemas de las TIC. Se citan en este apartado algunos de estos programas:

- a. **Sniffer de red.** Se trata de programas que analizan el tráfico que pasa a través de una red de comunicaciones. Los atacantes suelen utilizar estas herramientas para capturar información de autenticación u otra información sensible.
- b. **Rootkit.** Colección de herramientas utilizadas para ocultar una intrusión y obtener acceso con privilegios de administrador a un sistema.
- c. **Spam.** El *spam* es un conjunto de correos publicitarios enviados de forma masiva a miles de usuarios de todo el mundo, usuarios que obviamente no han autorizado el envío de dicha publicidad a sus buzones de correo. La recepción de *spam*, tan habitual hoy en día, puede evitarse mediante filtros y listas negras bien en el servidor de correo, bien en el propio cliente.
- d. **Spyware.** *Malware* similar a los troyanos, de tal manera que los usuarios añaden este *software* malicioso a su sistema sin saberlo cuando instalan otras aplicaciones. Los programas *spyware* actúan como programas independientes y ejecutables teniendo capacidad para:
  - e. Monitorizar el uso del teclado.
  - f. Analizar archivos del disco de forma arbitraria.
  - g. Espiar a otras aplicaciones como procesadores de texto o programas de chat.
  - h. Leer *cookies* y cambiar la página por defecto del navegador web.
  - i. Monitorizar diversos aspectos del comportamiento del usuario.
- j. **Cookies.** Una cookie es un archivo de pequeño tamaño que conserva información acerca del uso de un sitio web, bien de forma temporal para una sesión bien de forma persistente para identificar a un usuario en visitas sucesivas. Desafortunadamente, las *cookies* persistentes pueden ser utilizadas como *spyware* para rastrear la navegación web del usuario (*tracking cookies*).
- k. **Keyloggers.** Son programas espía, que toman el control de los equipos, para espiar y robar información registrando las pulsaciones del teclado, para robar información como contraseñas de páginas financieras o sistemas de correo electrónico.
- l. **Jokes.** Un *joke* es un programa inofensivo que simula las acciones de un virus informático en el ordenador. Su objetivo no es atacar, sino gastar una broma a los usuarios, haciéndoles creer que están infectados por un



virus y que se están poniendo de manifiesto sus efectos. Aunque su actividad llega a ser molesta, no produce por sí mismo efectos dañinos.

### 10.3. SALVAGUARDAS

418. Para mitigar los riesgos asociados a *malware* es necesario un conjunto de medidas y procedimientos denominados genéricamente antivirus (aunque como se ha indicado anteriormente el *malware* es mucho más que un virus) para proteger, reaccionar y recuperarse de incidentes basados en *software* malicioso.

#### 10.3.1. ESTRATEGIAS DE PREVENCIÓN

419. La protección contra código malicioso debe basarse, al menos, en la implementación de las siguientes estrategias:
- Instalación de software antivirus con actualizaciones regulares de fabricantes reconocidos (las actualizaciones se deben aplicar a la mayor brevedad posible). Los sistemas antivirus son tal vez la herramienta de seguridad más empleada por los usuarios, puesto que además de eliminar virus suelen incluir defensa contra todo tipo de *malware* actual. Los antivirus deben permitir una combinación de los siguientes métodos de análisis:
  - Escáner de acceso. Análisis de los archivos cuando éstos son abiertos.
  - Escáner bajo demanda. Análisis de *malware* que se lleva a cabo en función de un calendario previamente establecido.
  - Escáner de correos electrónicos. Ejecución de software de protección instalado en los dispositivos de protección de perímetro o los servidores de correo, que deben chequear los mensajes antes de ser tratados por la aplicación de correo.
  - Control de firmas. Funcionalidad, a menudo incluida en los productos antivirus, que permite detectar cambios no legítimos en el contenido de un archivo.
  - Métodos heurísticos. Componente habitual en soluciones antivirus que busca firmas de virus modelo en archivos ejecutables.
  - Implementación efectiva de control de configuración y gestión de software, tratando de asegurar que los sistemas operativos y aplicaciones son actualizados de forma correcta tras la publicación de los parches preceptivos. Es muy importante tener habilitada la actualización automática de *software* en el sistema y aplicar las actualizaciones siempre que se informe de que existe una nueva versión (especialmente, en las actualizaciones referentes a seguridad). Si se solicita reiniciar el sistema, este reinicio debe hacerse lo antes posible, puesto que muchos parches sólo se aplican tras un reinicio del equipo (antes del mismo no tendrán efecto, aunque estén instalados correctamente). Además es necesario tener en cuenta que no sólo es importante actualizar el sistema operativo, sino que también se deben actualizar el resto de aplicaciones de trabajo, sobre todo el navegador web y sus complementos, puesto que



- si no están actualizados pueden ser un punto de infección al visitar páginas web maliciosas.
- h. Se debe disponer de la última versión del sistema operativo empleado en la Organización, ya que habitualmente estas nuevas versiones introducen mejoras significativas en la seguridad.
  - i. Implementación de medidas de control que restrinjan al mínimo el riesgo por introducción de *software* no verificado con soluciones antivirus.
  - j. Copias de respaldo. Es fundamental realizar copias de respaldo de manera regular para asegurar la integridad del sistema. La información se debe almacenar en un medio protegido contra escritura que debe ser ubicado en un lugar seguro de acuerdo con los requisitos establecidos por la Organización.
  - k. Programas de formación y concienciación. Se trata del factor más importante en cualquier política *antimalware*, ya que como se ha dicho el mejor antivirus es la prevención. Los usuarios deben ser conscientes en todo momento de que la ejecución de software no autorizado puede causar la infección del sistema más protegido. La formación del usuario es una medida esencial de protección contra incidentes provocados por *software* malicioso y uso no autorizado de aplicaciones. Los usuarios deben estar advertidos constantemente de la aplicación de las buenas prácticas expuestas a continuación en esta misma guía.
420. Para evitar la infección por malware en el entorno se deben seguir unas **pautas de trabajo generales**, sin importar el rol del usuario en la Organización:
- a. Trabajar habitualmente en el sistema como usuario sin privilegios, no como administrador salvo que las tareas operativas lo requieran en un momento concreto.
  - b. No ejecutar nunca programas de origen dudoso o desconocido.
  - c. Es necesario prestar especial atención a todos los adjuntos incluidos en los correos electrónicos.
  - d. Analizar y escanear antes de su uso cualquier información introducida o distribuida mediante dispositivos de almacenamiento extraíbles.
  - e. Utilizar *software* original.
  - f. Si se emplea un paquete ofimático capaz de ejecutar macros, desactivar la ejecución automática de éstas; si no se puede desactivar, la Organización debe plantear el uso de otro programa.
  - g. Evitar la ejecución automática de archivos, desactivando la capacidad *autorun* de memorias USB, CD, DVD... y desactivando la vista previa de los mensajes de correo electrónico.
  - h. En los sistemas de mensajería instantánea o al recibir un mensaje de correo electrónico, no pulsar nunca directamente sobre ningún vínculo, especialmente si es de procedencia desconocida.
421. A continuación se exponen una serie de buenas prácticas adicionales para los administradores de sistemas y redes. Aparte de las pautas generales, se debe

tener presente que estos perfiles disponen habitualmente de privilegios en el entorno de trabajo, hecho que los convierte en un objetivo para los atacantes y un punto débil para la seguridad de la Organización. Así, es necesario considerar al menos las siguientes directrices de trabajo:

- a. Tener un buen *antimalware* instalado y actualizado, protegiendo todos los puntos de la red.
- b. Si el *antimalware* no incluye firewall, se debe instalar uno, tanto en los puestos como en los servidores, con un doble objetivo: evitar que un equipo sea plenamente accesible desde el resto de la red (para un *malware* o una persona que trate de atacar) y evitar también que un malware que ha contaminado pueda abrir puertos no controlados, accesibles desde otras zonas de red, al explotar alguna vulnerabilidad del sistema.
- c. Solamente los administradores del sistema deben estar autorizados para instalar software.
- d. Se debe disponer de una adecuada política de establecimiento y mantenimiento de contraseñas.
- e. Se deben realizar auditorías de seguridad en profundidad periódicamente.
- f. Es necesario proteger adecuadamente el perímetro de la red, para asegurarse de que los empleados no se infectan al navegar por la web.
- g. Se deben aplicar todos los parches de seguridad que publican los fabricantes de software utilizados en la Organización (Microsoft, Adobe, etc.).
- h. Es necesario que los equipos técnicos se mantengan informados sobre nuevas estrategias de infección.

### 10.3.2. ESTRATEGIAS DE RESPUESTA

422. Una vez que se ha detectado una infección por *malware*, hay que seguir los siguientes pasos:
  - a. Identificar y aislar los equipos y medios infectados.
  - b. Desconectar físicamente de la red los elementos infectados a partir del tipo y lugar donde se ha detectado el virus.
  - c. Suspender cualquier intercambio de información entre el elemento infectado y el resto del sistema.
  - d. Rastrear y alertar a potenciales receptores de información de la presencia de máquinas infectadas en el entorno.
423. La Organización debe definir, implantar y probar procedimientos organizativos y técnicos de respuesta ante incidentes causados por *malware*.

### 10.3.3. ESTRATEGIAS DE RECUPERACIÓN

424. La recuperación ante un ataque causado por *malware* implica las siguientes acciones:
- a. Borrar y eliminar el *malware* de los medios infectado.
  - b. Recuperar el área afectada por la infección mediante la utilización de copias de respaldo. El alcance y escala de daño dependerá del tipo de *malware*.
  - c. Prestar especial atención a posibles reinfecciones en el entorno.
  - d. Considerar el impacto de que el ataque aparezca en los medios de comunicación social y definir una estrategia de comunicación.

## 11. PROTOCOLOS DE RED

### 11.1. INTRODUCCIÓN

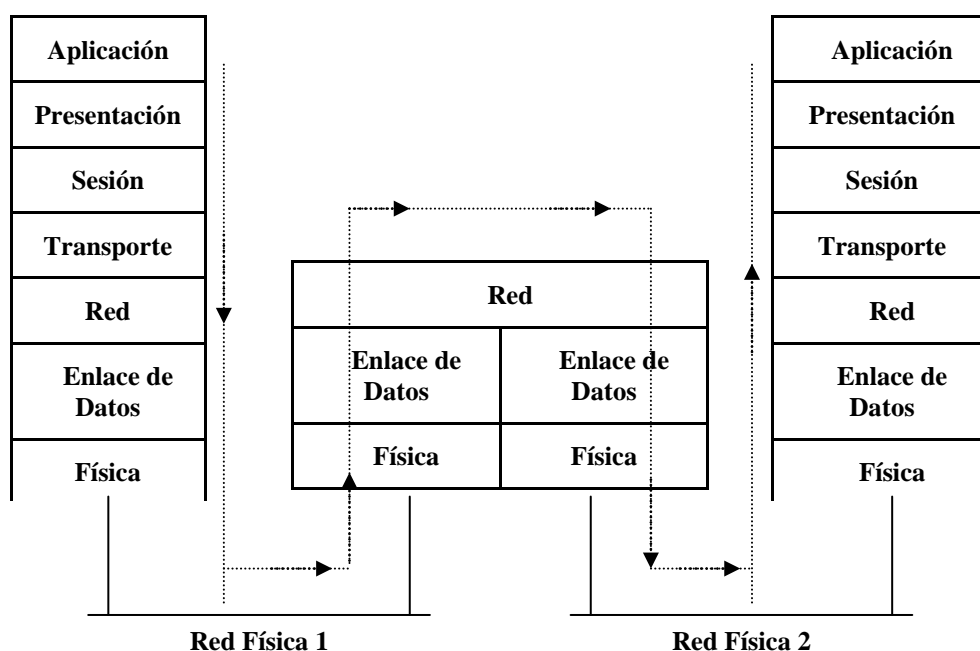
425. Es fundamental que los equipos de seguridad o técnica de la red y los sistemas conozcan cada uno de los protocolos de red utilizados por la tecnología de la Organización, tanto para poder realizar una configuración y mantenimiento adecuado de los mismos como para poder resolver los problemas e incidentes de seguridad que pueden presentarse. Por este motivo, en el presente capítulo se van a describir brevemente los principales protocolos de la pila TCP/IP, la más utilizada en los entornos habituales.

### 11.2. MODELOS OSI Y TCP/IP

426. El modelo de referencia OSI es un modelo conceptual de comunicaciones basado en una abstracción de siete capas donde se especifican las diferentes funcionalidades de red de los dispositivos. Este enfoque permite independizar las implementaciones de manera que un cambio en una de las capas no afecta a las restantes.
427. El flujo de información entre capas circula de manera vertical, de manera que las capas superiores encapsulan la información en las denominadas “*Protocol Data Units*” (PDU: cabecera + datos) pasándolas a las capas inferiores. Del mismo modo, las capas inferiores hacen llegar la información a las superiores desencapsulando las PDU y posteriormente pasándolas hacia la capa superior. En un mismo dispositivo las capas deben obligatoriamente pasar por las capas adyacentes para llegar a las restantes en un modelo del tipo cliente/servidor donde las capas inferiores ofrecen servicios a las superiores.
428. Las siete capas del modelo OSI son las siguientes:
- Física: transmisión física de la información dependiente del portador (fibra óptica, cobre, acceso inalámbrico, etc.) y de diferentes especificaciones físicas y eléctricas.
  - Enlace de Datos: estándar para transmitir en el medio físico (Ethernet, Token Ring, etc.).
  - Red: responsable del direccionamiento y entrega de la información entre nodos de la red. (IP, ICMP, IPX,...)
  - Transporte: primera capa en proporcionar un mecanismo de comunicaciones lógicas extremo a extremo (circuitos virtuales) y opcionalmente de entrega fiable (completa y ordenada) (TCP, UDP,...).
  - Sesión: capa encargada de establecer sesiones lógicas entre programas o procesos superiores.

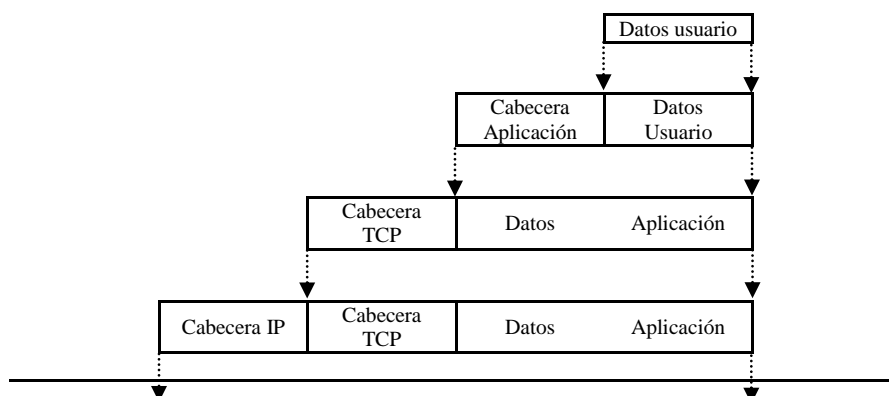
<b>Aplicación</b>	<b>7</b>
<b>Presentación</b>	<b>6</b>
<b>Sesión</b>	<b>5</b>
<b>Transporte</b>	<b>4</b>
<b>Red</b>	<b>3</b>
<b>Enlace de Datos</b>	<b>2</b>
<b>Física</b>	<b>1</b>

- f. Presentación: permite el marcado y adaptación de los contenidos de manera que se pueda identificar el formato de los datos y representarlos de una forma adecuada.
- g. Aplicación: capa de abstracción superior donde residen las aplicaciones y protocolos de aplicación donde se generan, reciben y tratan los datos de la comunicación: (SMTP, FTP, HTTP, etc.).
429. Los dispositivos pueden tener las diferentes capas implementadas parcialmente o en su totalidad. Por ejemplo, una estación de trabajo habitualmente cubre las siete capas mientras que un dispositivo enrutador debido a sus funcionalidades cubre habitualmente hasta la capa tres.



**Figura 1.- Comunicación a través de un dispositivo enrutador**

430. El proceso de la comunicación pasa por transferir los datos de nivel superior a la capa inferior, quien le añadirá información de control en forma de una cabecera (y en ocasiones una cola) y transferirá el resultado a la capa inferior, repitiendo este proceso hasta que los datos son transmitidos físicamente. En el receptor, el proceso se invertirá permitiendo obtener los datos de forma íntegra tal y como existían originalmente.



Cabecera Ethernet	Cabecera IP	Cabecera TCP	Datos	Aplicación	Cola Ethernet
-------------------	-------------	--------------	-------	------------	---------------

**Figura 2.- Proceso de Encapsulación**

431. Como puede verse en la figura anterior, los datos de usuario se lastran con bits de cabecera del protocolo de aplicación; a su vez, el nivel inferior (transporte) añade su propia cabecera, conformando lo que en el caso de TCP se denomina un segmento. Este segmento se envía al nivel inferior (red), formando un paquete, y finalmente el paquete se lastra en la capa más baja (enlace) dando así lugar a un datagrama.
432. Por otra parte, la pila de protocolos TCP/IP es una implementación que no coincide exactamente con el marco de referencia OSI, en la que se pueden encontrar de forma diferenciada sólo cuatro niveles de interacción:
- Enlace de datos: ARP/RARP, etc.
  - Red: IP, ICMP, IGMP, etc.
  - Transporte: TCP, UDP
  - Aplicación: HTTP, FTP, SMTP, etc.

Modelo OSI		Modelo TCP/IP	
Aplicación	7	Aplicación	
Presentación	6		
Sesión	5		
Transporte	4	Transporte	
Red	3	Red	
Enlace de Datos	2	Enlace de Datos	
Física	1		

**Figura 3.- Comparativa del Modelo OSI con la pila de Protocolos TCP/IP**

433. Como se puede apreciar las dos capas más importantes son la de red, donde el protocolo IP intenta ser el protocolo que permite transportar la información por la red y la de Transporte, donde los protocolos TCP/UDP intentan permitir comunicaciones lógicas entre los dispositivos extremos.
434. Además, se puede encontrar la particularidad de protocolos que participan en más de una capa, como el protocolo “ARP” que sirve de nexo de unión entre las capas de red (3) y enlace de datos (2).

### 11.3. PROTOCOLOS MÁS COMUNES

435. Queda totalmente fuera del alcance de la presente guía CCN-STIC hacer un análisis en profundidad de los protocolos de red. No obstante, es fundamental que los equipos técnicos de la Organización sí estén familiarizados con ellos, tanto desde un punto de vista funcional como desde un punto de vista de seguridad. Los protocolos con los que cualquier personal técnico debe estar perfectamente familiarizado como mínimo son ARP, IP, ICMP, TCP y UDP, pues son los que soportan el grueso de las comunicaciones de red. Además de estos protocolos básicos, es necesario también estar familiarizado con los protocolos específicos del entorno concreto de la Organización, entre los que se encuentran habitualmente protocolos de enrutamiento como RIP, OSPF o BGP, los protocolos utilizados para crear redes privadas virtuales, protocolos de voz sobre IP (VoIP) o similares. Y por supuesto será conveniente también estar familiarizado con los protocolos correspondientes a servicios estándar tales como SMTP, FTP, DNS, HTTP/HTTPS, NTP, etc.
436. Las especificaciones de los protocolos de red suelen estar contenidas en documentos conocidos como RFC (*Request For Comments*). Los RFC detallan los detalles de los protocolos y marcan las pautas que han de seguirse para su implementación en el mundo real. Aún así, siempre existirán diferencias de implementación entre distintos fabricantes debidos a los grados de libertad o resquicios que puedan existir en los RFC, aunque al menos la compatibilidad debería estar garantizada. Los RFC son por tanto el lugar donde se debe acudir cuando se desea conocer las características de un protocolo concreto; no obstante, en la presente guía se realizará una pequeña introducción de los protocolos más comunes basándonos en la pila de protocolos TCP/IP.

#### 11.3.1. CAPA DE ENLACE DE DATOS

##### 11.3.1.1. PROTOCOLO ARP

437. El protocolo ARP (*Address Resolution Protocol*) se encarga de permitir a los distintos dispositivos de red encontrar dinámicamente mediante mensajes de difusión su dirección de nivel dos (dirección hardware o MAC) dada su dirección de nivel tres correspondiente (dirección IP). El tráfico ARP es tráfico local a un segmento de red determinado, aunque es posible el uso de un *proxy* ARP para contestar peticiones ARP de otras redes. Los dispositivos suelen ser capaces de almacenar la información ARP durante un cierto periodo de tiempo en una caché interna para evitar problemas de retardos y sobrecargas de red.
438. El protocolo ARP viene definido en el RFC 826.

##### 11.3.1.2. PROTOCOLO RARP

439. El protocolo RARP (*Reverse Address Resolution Protocol*), al contrario que el protocolo ARP, se encarga de permitir a los distintos dispositivos de red encontrar, dada la dirección de nivel dos correspondiente (dirección MAC), su dirección de nivel tres (dirección IP). Al igual que el tráfico ARP, el tráfico RARP es tráfico local a un segmento de red determinado y los distintos



dispositivos suelen ser capaces de almacenar dicha información durante un cierto período de tiempo.

440. El protocolo RARP viene definido en el RFC 903.

#### 11.3.1.3. PROTOCOLO PPP

441. PPP (*Point-to-Point Protocol*) es un protocolo desarrollado por IETF (*Internet Engineering Task Force*) para corregir y mejorar el protocolo SLIP (*Serial Line Internet Protocol*), creando un estándar internacional. PPP permite establecer una conexión entre dos nodos garantizando autenticación y asignación dinámica de IP y negociando parámetros de autenticación y compresión. Habitualmente es usado para establecer la conexión con un proveedor de servicio a través de un módem telefónico.

442. El protocolo PPP viene definido en el RFC 1661.

#### 11.3.1.4. PROTOCOLO L2TP

443. El protocolo L2TP (*Layer 2 Tunneling Protocol*) fue desarrollado por IETF como extensión del protocolo PPP, combinando los protocolos PPTP (*Point to Point Tunneling Protocol*) de Microsoft y L2F (*Layer Two Forwarding*) de Cisco Systems, para proporcionar acceso multiprotocolo a través de una comunicación tunelizada. Este protocolo es usado para crear redes privadas virtuales, no obstante, puesto que L2TP no realiza comprobaciones de integridad ni cifrado nativo de datos, debe ser usado junto con el *framework* IPSec que se verá más adelante

444. El protocolo L2TP viene descrito en el RFC 2661.

#### 11.3.1.5. PROTOCOLO STP

445. El protocolo STP (*Spanning Tree Protocol*) es un protocolo estandarizado por el IEEE como 802.1d<sup>4</sup> que garantiza la eliminación de bucles en la red debido a conexiones redundantes, creando una topología libre de bucles y calculando una ruta única entre los dispositivos de la red pero manteniendo los enlaces redundantes desactivados para activarlos en caso de necesidad.

446. En la actualidad existen distintas variantes del protocolo STP.

### 11.3.2. CAPA DE RED

#### 11.3.2.1. PROTOCOLO IP V4

447. El protocolo IP (*Internet Protocol*), cuya especificación se puede encontrar en el RFC 791, es el estándar de facto en las comunicaciones de hoy en día. Existen dos versiones del mismo, la versión 4, que es la que se encuentra desplegada de forma mayoritaria en la actualidad y la versión 6, que viene a solventar algunos de los problemas de la versión 4 relativos a escalabilidad y seguridad y que se encuentra en una fase de implantación lenta.

---

<sup>4</sup> Puesto que existe otra versión de STP no compatible con la estandarizada por el IEEE, se recomienda el uso de ésta última.

448. Los paquetes IP constan de una cabecera, típicamente de 20 bytes, y un cuerpo de datos variable. La cabecera incluye distintos parámetros que permiten que el protocolo IP sea resistente a algunos problemas encontrados en la red, como bucles de enrutamiento, gracias al campo "tiempo de vida" (*Time To Live, TTL*), el cambio del tamaño máximo de trama (*Maximum Transmission Unit, MTU*) permitido en el medio físico a través de diversos campos relacionados con la fragmentación o la corrupción de los paquetes en tránsito gracias al campo de chequeo de integridad (*checksum*).
449. Los parámetros más importantes contenidos en la cabecera IP desde el punto de vista funcional son las direcciones de origen y destino (por ejemplo, 192.168.1.1 en IPv4), que permiten enrutar los paquetes a través de las distintas redes hasta alcanzar su destino y el protocolo de nivel superior (transporte) que se encuentra embebido en el cuerpo de datos.
450. Las direcciones IP en la versión 4 del protocolo constan de 4 bytes (32 bits) y se suelen representar de la forma "xxx.xxx.xxx.xxx" donde cada "xxx" puede tomar un valor de 0 a 255. El direccionamiento IP se halla lógicamente fragmentado en tramos, dando lugar a lo que se conoce como direcciones de clases A, B, C, D y E, que originalmente fueron pensadas para ser asignadas a organizaciones de mayor tamaño (clases A) a menor tamaño (clases C). La clase D, con direcciones comprendidas entre 224.0.0.0 a 239.255.255.255, está destinada a un tipo especial de direccionamiento llamado *multicast*, que permite llevar a cabo comunicaciones de uno a varios. Por último, la clase E fue originalmente reservada para uso futuro.
451. Dentro de estos rangos de direccionamiento, hay ciertos subrangos de direcciones reservadas para uso privado, es decir, para uso interno de las Organizaciones y que no deberían nunca salir a Internet. Estos son (en notación CIDR, *Classless Inter-Domain Routing*) los siguientes: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Adicionalmente, el rango 169.254.0.0/16 está destinado a la autoconfiguración de sistemas en ausencia de un servidor DHCP.

#### 11.3.2.2. Protocolo IP V6

452. La versión 4 del protocolo IP, presente desde hace más de 20 años, presenta una serie de problemas, siendo el mayor de ellos la limitación en el número de direcciones IP disponibles. Por lo tanto, como evolución natural apareció la versión 6 como una nueva *suite* del protocolo IP. IPv6 viene definido principalmente en el RFC 2460
453. Entre las principales diferencias de la nueva versión, cabe destacar las siguientes:
- Ampliación de las direcciones IP, de 32 bits a 128 bits, lo cual permite un mayor número de nodos en la red.
  - Simplificación de la cabecera IP, pasando a 40 bits fijos, mejorando la eficiencia y permitiendo cabeceras de extensión.
  - Mejoras directas en la seguridad, proporcionando autenticación, integridad y confidencialidad mediante el *framework* IPsec.
  - Mecanismos de calidad de servicio (QoS).

- e. Eliminación de la dirección de *broadcast* y creación de la dirección de red *anycast*, similar a las direcciones *multicast* pero en la que el paquete enviado, en lugar de enviarse a todos los nodos del grupo, se selecciona para un único nodo, habitualmente el más cercano según los protocolos de enrutamiento, como destino del paquete.

454. Debido a la complejidad de la migración a IPv6, aunque la mayor parte de los protocolos de capas superiores no necesitan grandes cambios para operar sobre IPv6, han aparecido distintas soluciones para llevar a cabo dicha migración, como la creación de islas que funcionan con IPv6 pero establecen comunicaciones tunelizadas como backbone con IPv4 con otras islas, o la traducción entre ambas versiones del protocolo o la doble pila en cada *host* de la red.

#### 11.3.2.3. PROTOCOLO ICMP

- 455. El protocolo ICMP (*Internet Control Message Protocol*), tremendamente importante para el correcto funcionamiento de las comunicaciones IP y definido en el RFC 792, es un protocolo de nivel 3 a pesar de estar encapsulado en paquetes IP.
- 456. Existen dos tipos de paquetes ICMP: informativos y de error. A través de ICMP es posible informar de eventos de red tales como la imposibilidad para un paquete de alcanzar su destino debido a un problema temporal en la red, a la prohibición de tránsito a través de un enrutador o a que el sistema remoto no se encuentra disponible y también permite interrogar a los sistemas finales o intermedios acerca de características de configuración tales como máscara de red o tiempo, o de *status* o si el sistema se encuentra disponible.
- 457. Al igual que sucedía en el caso de IP, el paquete ICMP está compuesto por cabecera y cuerpo de datos. La primera indicará de qué tipo de mensaje se trata, mientras que el cuerpo de datos contendrá información relacionada con el mensaje en cuestión.
- 458. Es relativamente frecuente encontrar configuraciones de cortafuegos que deniegan todos los paquetes ICMP y esto no es recomendable. Si bien es cierto, que permitir el tránsito de todos los paquetes ICMP en las redes puede permitir a un potencial atacante obtener información de las características de las mismas, también lo es que filtrar todos los paquetes ICMP puede causar serios problemas en la red. La solución más aconsejable suele ser por tanto llegar a un equilibrio en el que se dejen pasar los paquetes críticos para la comunicación de errores y bloquear aquellos que permitan obtener información. No obstante es siempre conveniente guardar un registro de los paquetes bloqueados y revisarlos periódicamente por si eventualmente se introdujeran en la red servicios que utilizaran algún tipo de mensaje ICMP bloqueado que sea necesario para funcionar correctamente.

#### 11.3.2.4. PROTOCOLO IGMP

- 459. Existen tres tipos de direcciones IP: *unicast*, *broadcast* y *multicast*; las direcciones *multicast* (multidifusión) permiten el envío de información,

encapsulada principalmente como UDP, a distintos destinos de forma simultánea, de forma que reduce la carga con respecto a *broadcast*.

460. *Multicast* emplea direcciones IP de la clase D, las cuales van desde 224.0.0.0 a 239.255.255.255. El protocolo IGMP (*Internet Group Management Protocol*) es el encargado de la gestión dinámica de grupos de multidifusión, añadiendo o eliminando a los distintos dispositivos de dichos grupos, entre otras funciones.
461. La versión 3 de IGMP, la más utilizada hoy en día, viene definida en el RFC 3376.

#### 11.3.2.5. FRAMEWORK IPSEC

462. El Framework IPSEC (*Internet Protocol Security*) es un conjunto de protocolos cuyo objetivo es asegurar las comunicaciones, autenticando y cifrando cada paquete IP. IPSec dispone de dos modos de funcionamiento, túnel y transporte.
463. Dentro del *framework* se encuentran los siguientes protocolos:
- a. AH (*Authentication Header*), protocolo que garantiza la integridad y autenticación de datos.
  - b. ESP (*Encapsulating Security Payload*), protocolo que proporciona autenticidad de origen, integridad y protección de confidencialidad.
  - c. IKE/ISAKMP (*Internet Key Exchange/Internet Security Association and Key Management Protocol*), protocolos encargados del intercambio de claves, negociación de parámetros y establecimiento de asociaciones de seguridad (SA) de IPSec.

#### 11.3.2.6. PROTOCOLOS DE ENRUTAMIENTO

464. Los protocolos de enrutamiento son los encargados del intercambio de información entre los *routers* para crear y mantener las tablas de enrutamiento, de forma que permiten conocer la mejor ruta para llegar a un destino.
465. Dentro de los protocolos de enrutamiento hay dos familias de protocolos totalmente diferenciadas, la familia IGP (*Interior Gateway Protocols*), la cual permite el enrutamiento dentro de sistema autónomo, administrado por una única entidad y EGP (*Exterior Gateway Protocols*), que permite el enrutamiento fuera de la red interna, es decir, permite enrutar el tráfico con otros sistemas autónomos, los cuales son administrados por distintas entidades.
466. En la familia IGP, cabe destacar los protocolos RIP (*Routing Information Protocol*) u OSPF (*Open Shortest Path First*), y dentro de la familia EGP destaca el protocolo BGP (*Border Gateway Protocol*)<sup>5</sup>.
467. Un punto a tener en cuenta en los protocolos de enrutamiento es que son usados para el intercambio de información en la capa de red; no obstante, no todos pertenecen a dicha capa: por ejemplo RIP o BGP usan información de capas superiores para intercambiar las tablas de enrutamiento.

#### 11.3.3. CAPA DE TRANSPORTE

---

<sup>5</sup> Existen otros protocolos de enrutamiento propietarios como EIGRP o IS-IS

### 11.3.3.1. PROTOCOLO TCP

468. El protocolo TCP (*Transmission Control Protocol*), especificado en el RFC 793, proporciona mecanismos para asegurar la entrega de forma fiable de los datos de nivel superior, así como para gestionar de forma eficiente la conexión establecida. Para ello incorpora en su cabecera parámetros como los números de secuencia y de *acknowledgement*, que permiten determinar si algún paquete se ha perdido y facilitar la retransmisión y establecer un mínimo de seguridad en la conexión, o parámetros como el tamaño de ventana o las banderas (flags), que permiten gestionar adecuadamente el tráfico de información y el establecimiento, cierre y gestión de la conexión.
469. El precio a pagar por estas características de fiabilidad y seguridad es un cierto exceso en la transmisión de datos, que puede ser proporcionalmente bastante notable si la cantidad de datos a transmitir es importante o si los paquetes individuales son pequeños.
470. Tanto TCP como UDP, tratado a continuación, utilizan el concepto de puertos para permitir establecer la unicidad de conexiones en Internet. Así, en un momento concreto sólo puede haber una conexión establecida entre el sistema A y el sistema B con puerto de origen X y puerto de destino Y. Los puertos de origen suelen ser seleccionados aleatoriamente, salvo en el caso de notables excepciones como IKE, pero los puertos de destino suelen ser asignados estáticamente a un protocolo determinado, como método para permitir localizar fácilmente los servicios proporcionados por un sistema, aunque también existen en este caso notables excepciones como es el caso de las llamadas a procedimientos remotos (RPC). De esta forma, el protocolo DNS utilizará el puerto 53 (tanto TCP como UDP), el protocolo SMTP el puerto TCP 25 y así sucesivamente<sup>6</sup>.
471. IANA (*Internet Assigned Numbers Authority*) es la encargada de la asignación de los distintos tipos de números de puertos.

### 11.3.3.2. PROTOCOLO UDP

472. UDP (*User Datagram Protocol*), el cual viene definido en el RFC 768, es un protocolo relativamente simple comparado con TCP y no goza de las características de fiabilidad y seguridad propias de éste. No se encarga de determinar si los paquetes han llegado adecuadamente a su destino, ni de retransmitirlos en caso contrario, a pesar de lo cual sí puede incorporar un cierto nivel de chequeo de integridad a través del *checksum*. Si un protocolo de nivel superior que utiliza UDP como medio de transporte requiere estas características de fiabilidad y seguridad, deberá implementarlas él mismo.
473. La ventaja, al contrario de lo que sucedía en TCP, es que la sobrecarga es muy baja, por lo que UDP es un protocolo ideal para servicios que intercambien mensajes mayoritariamente cortos (como DNS) o servicios en los que no sea relevante la pérdida de algunos paquetes (como streaming de audio o vídeo).

---

<sup>6</sup> Se pueden consultar buena parte de los protocolos y puertos definidos en <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>

474. Como se ha indicado anteriormente, UDP hace uso del mismo concepto de puertos que TCP. Algunos servicios críticos para el funcionamiento de Internet, tales como DNS, funcionan fundamentalmente utilizando paquetes UDP.

#### 11.3.4. CAPA DE APLICACIÓN

475. A continuación se describirán brevemente algunos de los protocolos de la capa de aplicación más habituales.

##### 11.3.4.1. PROTOCOLO SMTP

476. El protocolo SMTP (*Simple Mail Transfer Protocol*) es un protocolo basado en texto y utilizado para el intercambio de mensajes de correo electrónico entre distintos MTA (*Mail Transfer Agents*).
477. El protocolo SMTP utiliza por defecto el puerto TCP/25 y viene descrito en el RFC 821. Existe una versión extendida del protocolo llamada ESMTP definida en el RFC 1425.

##### 11.3.4.2. PROTOCOLO POP

478. El protocolo POP (*Post Office Protocol*), permite recoger el correo electrónico almacenado en un servidor, almacenándolo en un sistema local para su posterior revisión offline, mediante un MUA (*Mail User Agent*)
479. La versión actual de este protocolo es la 3, la cual viene definida en última instancia en el RFC 1939. POP3 usa el puerto TCP/110

##### 11.3.4.3. PROTOCOLO IMAP

480. El protocolo IMAP (*Internet Message Access Protocol*) es un protocolo de acceso a mensajes electrónicos almacenados en un servidor. IMAP es más complejo y tiene varias ventajas sobre POP; por ejemplo, permite visualizar online los mensajes de manera remota y no descargando los mensajes como lo hace POP.
481. La versión actual de este protocolo es la 4, que viene definida por el RFC 3501. IMAP usa el puerto TCP/143

##### 11.3.4.4. PROTOCOLO FTP

482. FTP (*File Transfer Protocol*) es un protocolo basado en texto de transferencia de archivos entre sistemas basado en una arquitectura cliente-servidor. Toda la comunicación entre ambos extremos, incluida la autenticación, se realiza en texto claro.
483. El protocolo está definido en el RFC 959. FTP usa el puerto TCP/21 para la conexión de control y el puerto TCP/20 para la transferencia de datos

##### 11.3.4.5. PROTOCOLO DNS

484. El protocolo DNS (*Domain Name System*) es una base de datos jerárquica distribuida la cual tiene como función principal la traducción de los nombres en



direcciones IP y viceversa, así como proporcionar información para el enrutamiento de los correos electrónicos. Para reducir el tráfico DNS en la red, los dispositivos pueden almacenar información en una caché interna.

485. El protocolo DNS está definido en los RFC 1034 y 1035 y utiliza principalmente el puerto UDP/53.

#### 11.3.4.6. PROTOCOLO HTTP

486. HTTP (*Hypertext Transfer Protocol*) es un protocolo cliente-servidor sin estado, basado en transacciones en texto, que define el contenido y el formato usado en la comunicación entre navegadores y servidores web para la descarga de documentos principalmente en lenguaje HTML (*Hypertext Markup Language*) y direccionados mediante el uso de URI (*Uniform Resource Identifiers*).
487. El protocolo HTTP viene definido en varios RFC, siendo el más importante el RFC 2616. HTTP usa el puerto TCP/80.

#### 11.3.4.7. PROTOCOLO HTTPS

488. El protocolo HTTPS (*Hyper Text Transfer Protocol Secure*) es la versión segura del protocolo HTTP, mediante el uso de SSL/TLS para crear un canal cifrado entre el cliente y el servidor.
489. HTTPS viene definido en RFC 2818 y usa el puerto TCP/443.

#### 11.3.4.8. PROTOCOLO SNMP

490. SNMP (*Simple Network Management Protocol*) es un protocolo de intercambio de información entre dispositivos. El protocolo tiene dos métodos de funcionamiento: mediante consultas periódicas (*polling*) sobre variables existentes en la MIB (*Management Information Base*) o mediante mensajes enviados desde el propio dispositivo (*traps*) a la estación gestora.
491. La versión actual del protocolo es la tres. No obstante, la más utilizada es la versión dos. SNMP viene definido en el RFC 1157 y utiliza habitualmente los puertos UDP/161 y UDP/162 (*traps*).

#### 11.3.4.9. PROTOCOLO SIP

492. SIP (*Session Initiation Protocol*) es un protocolo desarrollado por IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el vídeo, voz, mensajería instantánea, juegos en línea y realidad virtual, y cuya sintaxis es similar a las transacciones del protocolo HTTP.
493. El protocolo es utilizado principalmente en comunicaciones de voz sobre IP junto con otros protocolos como RTP (*Real-time Transport Protocol*).
494. SIP viene definido en el RFC 3261, y usa principalmente el puerto UDP/5060.

#### 11.3.4.10. PROTOCOLO NTP



- 495. El protocolo NTP (*Network Time Protocol*) tiene como objetivo sincronizar los relojes de los dispositivos de una red a una hora precisa. Existe una versión simplificada llamada SNTP (*Simple Network Time Protocol*).
- 496. NTP viene definido en el RFC 1305 y utiliza el puerto UDP/123

#### 11.3.4.11. PROTOCOLO DHCP

- 497. DHCP (*Dynamic Host Configuration Protocol*) es un protocolo que permite a un cliente, mediante *broadcast*, obtener los parámetros de configuración de red necesarios para comunicarse con otros clientes. La dirección IP se obtiene de un *pool* de direcciones disponibles y se asigna al cliente durante un periodo de tiempo establecido.
- 498. DHCP viene definido en el RFC 2131 y utiliza los protocolos UDP/67 y UDP/68.

## 12. SEGURIDAD PERIMETRAL

### 12.1. INTRODUCCIÓN

499. Asegurar el perímetro es una de las estrategias defensivas más eficaces y comúnmente utilizadas en el campo de la seguridad: no hay más que recordar las fortificaciones medievales en las que existía tan sólo un número restringido de puntos de entrada, en los que se aplicaba un fuerte control de acceso o, ya en la actualidad, las verjas y alambradas que marcan el perímetro de determinados centros en los que de nuevo existe un número muy concreto de puntos de entrada fuertemente controlados. Reducir la superficie de exposición, crear puntos controlados de acceso y centrar las defensas en esos puntos permite optimizar la capacidad defensiva. Para reforzar la eficacia de la fortificación, existen además elementos añadidos de seguridad como guardias, fosos, barreras naturales o perímetros internos.
500. El mundo de las tecnologías de la información ha adoptado estas ideas a lo largo de los últimos años, creando arquitecturas y dispositivos que permitieran realizar las mismas tareas con igual eficacia. En el centro de estas tecnologías se encuentran los **cortafuegos**. Los cortafuegos son el equivalente a las murallas de la antigüedad, dispositivos que separan distintas áreas con distintos requisitos de seguridad o niveles de riesgo y que controlan el flujo de tráfico entre ellas. Además de los cortafuegos, y al igual que sucedía en el caso de las fortificaciones mencionadas anteriormente, se han incluido elementos adicionales para hacer posible el incremento de la seguridad proporcionada por el cortafuegos, ya sea aumentando la “inteligencia” de los cortafuegos en sí mismos, o a través de nuevas tecnologías y procesos como el cifrado, los certificados digitales, los sistemas de detección y prevención de intrusiones, los sistemas de análisis de contenidos, etc.

#### 12.1.1. IDENTIFICACIÓN DE AMENAZAS

501. Tanto la seguridad perimetral en general como los cortafuegos en particular son habitualmente de utilidad limitada si no se tiene previamente una idea clara de qué se quiere defender, cómo de valioso es, cuál sería el impacto de un incidente de seguridad y cuáles son las amenazas.
502. Antes de empezar por tanto a poner en marcha las tecnologías y procesos de seguridad perimetral será necesario hacer un estudio detallado de la actividad productiva de la Organización y dar respuesta a las respuestas anteriormente planteadas. El resultado final de este proceso de análisis será lo que habitualmente se conoce como "Política de Seguridad" y debe definir claramente qué está permitido y qué está prohibido dentro de la Organización.
503. Hay que ser consciente desde el primer momento de que por la naturaleza misma de las tecnologías empleadas es imposible alcanzar un 100% de seguridad. El principal objetivo de una Organización es desarrollar de forma eficiente sus actividades para lograr alcanzar unos objetivos concretos. En el mundo real, eso implica llegar a un equilibrio entre inversión y beneficios (entendidos como el grado de cumplimiento de los objetivos previstos por la Organización, sean económicos o de cualquier otro tipo). Una inversión excesiva en seguridad que

no se corresponde con una respuesta adecuada a las amenazas reales a las que una Organización se enfrenta será inadecuada desde el punto de vista de negocio.

504. Identificar las amenazas que acechan a una Organización concreta puede ser una tarea ardua. En cualquier caso, resulta obvio que Organizaciones de tipo militar o financiero estarán en general expuestas a ataques más sofisticados que pequeñas empresas. No obstante, hoy en día debe desterrarse la idea de que el nivel de amenaza para Organizaciones menos “jugosas” es bajo o inexistente. En los últimos años se ha apreciado una tendencia hacia ataques indiscriminados, que afectan y causan importantes pérdidas a todo tipo de Organizaciones. Nadie está a salvo, por pequeña que sea o por poco interesante que pueda parecer para un atacante.
505. Con el creciente uso de Internet en los últimos años y el acceso a complejas herramientas, cada vez es menor el conocimiento necesario por parte de un atacante de llevar a cabo un ataque; no obstante una posible clasificación de las amenazas es la basada en el atacante, distinguiendo entre amenazas no estructuradas, llevadas a cabo habitualmente por personas inexpertas mediante el uso de herramientas automáticas que en muchos casos quieren probar su conocimiento, y amenazas estructuradas, realizadas por personas motivadas y técnicamente competentes, con un objetivo concreto. En cualquier caso, las pérdidas económicas o de imagen corporativa de la Organización pueden ser graves.

#### 12.1.2. EVOLUCIÓN

506. Ha habido una interesante evolución en la tendencia seguida por los ataques en la última década. Antes de la implantación masiva de cortafuegos, la amplia superficie expuesta por los sistemas, la gran cantidad de servicios habilitados en las instalaciones por defecto, la debilidad de las implementaciones de los protocolos de red y otros factores posibilitaban una gran variedad de ataques desde distintos flancos. Después de dicha implantación, en la segunda mitad de la década de los noventa, la superficie eficaz se redujo considerablemente, quedando expuestos solamente un número limitado de servicios (típicamente correo electrónico, FTP, web o DNS). Esto, junto con otros factores que se describen a continuación, ha ido propiciando paulatinamente tanto un cambio en la tipología de ataques como un cambio en el perfil de los atacantes:
  - a. Interacción. Con objeto de mantener la competitividad se produce una fuerte interacción en términos de comunicación y accesibilidad con los socios de negocio, propiciando la disolución de las tradicionales fronteras “interior” y “exterior”. El caso más extremo de esta tendencia es la externalización (*outsourcing*) de servicios, que difumina en un alto grado el perímetro de la Organización.
  - b. Movilidad. Gracias a los importantes avances en las tecnologías de las TIC, es posible multiplicar la productividad de la Organización llevando todos los recursos de la misma al usuario móvil, y propiciando la descentralización en términos de centro de trabajo.

- c. La implantación de tecnologías de acceso inalámbrico (WiFi, Bluetooth, etc.), y los problemas de implementación de sus protocolos y de su implantación abren una nueva vía de acceso al interior de la Organización.
  - d. Se produce una fuerte expansión de los servicios web, en muchos casos con aplicaciones vulnerables que no están diseñadas para ser accesibles desde redes públicas pero que por requisitos del servicio acaban siéndolo sin superar las correspondientes pruebas de seguridad.
  - e. Se produce una fuerte integración de los motores de bases de datos con las aplicaciones web, lo que provoca que surjan nuevos ataques que se aprovechan de esa interacción y que puedan ser explotadas desde el exterior algunas vulnerabilidades intrínsecas a las tecnologías de bases de datos.
507. Estos factores entre otros, propician la complejidad de los entornos de producción, la difuminación de los perímetros y la aparición de nuevas familias de ataques más sencillos de perpetrar en el entorno actual que los tradicionales ataques a servicios. Debido a la reducción de la superficie de exposición, se idean asimismo nuevas y más eficaces técnicas que permitan romper el perímetro desde el interior, dado que el tráfico saliente suele estar sujeto a políticas más permisivas que el entrante. En ese sentido, se produce un auge de los ataques de ingeniería social, que intentan engañar al usuario para que ejecute código malicioso recibido en un correo electrónico o para que visite una página web maliciosa que explote alguna vulnerabilidad del sistema operativo o del propio navegador. El resultado final es que el atacante puede hacerse con el sistema utilizando conexiones salientes que burlan el perímetro de seguridad.
508. Un detalle importante a tener en cuenta a la hora de hablar de seguridad perimetral es que no ha de ser entendida en términos interno - externo, Organización - Internet, sino en términos de separación de áreas con distintos requisitos de seguridad. Es un error común centrar toda la atención en crear un perímetro externo muy reforzado, pero olvidar el resto de la Organización. Si esto es así, y un atacante consigue penetrar el perímetro de la Organización, éste podrá acceder a todos los recursos de la misma, o al menos disponer de una posición privilegiada para poder realizar ataques de una forma más eficaz. Es necesario hacer un análisis de cuántos niveles distintos de seguridad deben establecerse en la Organización y pasar a separarlos y protegerlos adecuadamente de acuerdo a su criticidad o nivel de riesgo.

### 12.1.3. PUNTOS DÉBILES

509. Existen multitud de puntos débiles en una Organización que pueden hacer efectiva una amenaza, alguno de ellos son implícitos a la tecnología (debilidades en los protocolos de comunicación) y, por supuesto, otros son atribuibles a las personas. Entre los más significativos se encuentran los siguientes:
- a. Protocolos. Todas las capas de TCP/IP presentan de forma implícita puntos débiles, como ausencia de autenticación (SNMP) o intercambio de datos en claro (HTTP, telnet, FTP...). Aunque muchos de estos protocolos están evolucionando aportando nuevas medidas de seguridad

(como SNMP versión 3) y para otros existen alternativas seguras (como SSH o SFTP), aún existen entornos donde, por diferentes motivos, se usan protocolos inseguros.

- b. Sistemas. Tanto los servidores como la electrónica de red pueden presentar servicios instalados por defecto o mal configurados o bugs en aplicaciones o en el propio sistema operativo. Es importante aplicar salvaguardas de bastionado en todos los elementos tecnológicos significativos para la Organización.
- c. Seguridad física. En ocasiones se producen debilidades dentro de las Organizaciones en ámbitos como el control de acceso a ubicaciones, la protección de la información en formato físico (documentos, soportes...) o la seguridad operativa en las instalaciones (mesas limpias, bloqueos automáticos de sesión...). Es necesario garantizar los aspectos relativos a la protección física de la información en todos los casos.
- d. Personas. Las personas suelen ser el eslabón más débil de la cadena, susceptibles a ataques como la ingeniería social o *phishing*, por lo que la Organización debe trabajar en la formación y concienciación, en el ámbito de la seguridad, de todo el personal, tanto interno como externo.

## 12.2. COMPONENTES DE LA SEGURIDAD PERIMETRAL

- 510. Se describen en este punto los elementos tecnológicos intervinientes en la seguridad perimetral corporativa. Aunque como se ha indicado previamente los cortafuegos son el elemento principal en el ámbito de la protección perimetral, existen otros elementos cada día más relevantes para dicha protección y cuyo despliegue y explotación debe ser convenientemente evaluado en la Organización.

### 12.2.1. ENRUTADORES Y REGLAS DE FILTRADO

- 511. Los enrutadores son dispositivos que permiten a los paquetes de red encontrar el camino adecuado para llegar a su destino final haciendo uso de información acerca del estado de las rutas en un momento concreto. Debido a esta función crítica, y a la posición estratégica que ocupan en la red, se convierten también en elementos fundamentales de la arquitectura de seguridad perimetral.
- 512. Si bien es cierto que gracias al aumento de potencia de las plataformas hardware actuales a menudo se entremezclan las funciones de los enrutadores y de los cortafuegos, las capacidades de los enrutadores están orientadas a realizar eficientemente su función característica y su eficiencia se puede ver seriamente perjudicada si se le fuerza a realizar tareas demasiado exhaustivas, como las típicamente realizadas por un cortafuegos (un filtrado excesivo o demasiado complejo).
- 513. Por su posición privilegiada en la infraestructura los enrutadores, especialmente los de perímetro o “*border routers*”, son un punto privilegiado donde filtrar tráfico claramente malicioso. Es por tanto una buena práctica, y aliviará a los siempre sobrecargados cortafuegos, utilizar los enrutadores para realizar un **filtrado simple** de tráfico o incluso explotar las características más avanzadas

que pueda proporcionar siempre y cuando estas tareas no perjudiquen su labor fundamental de enrutar eficientemente los paquetes.

514. A la hora de proteger la red es imprescindible conocer su tipología: protocolos autorizados, rangos de direccionamiento permitidos, etc. Hay dos estrategias fundamentales para proteger la red utilizando enrutadores:
- a. Filtrado: permitir o denegar el tráfico, generalmente mediante listas de control de acceso (ACL) aunque también es posible hacerlo mediante otros mecanismos, como filtrado de camino inverso (*Reverse Path Filtering*, RPF) o rutas de descarte (*null routes*).
  - b. Conformado/Limitado: mecanismos de calidad de servicio consistentes en la definición de umbrales de tolerancia al partir de los cuales se aplican medidas sobre el tráfico.
515. En los dispositivos de enrutamiento de perímetro suele aplicarse un filtrado conocido como de entrada/salida (*ingress/egress*) de manera que el enrutador sea el primer punto de control del tráfico. Para un rendimiento óptimo lo habitual es filtrar el tráfico en el interfaz más cercana a la entrada de éste: el tráfico de salida hacia Internet es filtrado en el interfaz interno y el tráfico de entrada de Internet se filtra en el interfaz externo.
516. A la hora de aplicar restricciones de filtrado en un enrutador –o en un cortafuegos- deben considerarse al menos los siguientes aspectos:
- a. Denegar la entrada y salida a Internet de direcciones de uso especial: RFC 1918 (*private*), RFC 3330 (*special use*). Las direcciones de uso especial y las reservadas por IANA son conocidas como “*martians*”.
  - b. Denegar la entrada y salida de tráfico originado por espacio de direcciones válido pero no utilizadas (*unallocated*).
  - c. Denegar la entrada de tráfico con direcciones propias y la salida de tráfico no originado con direcciones propias (RFC 2827, *anti-spoofing*).
  - d. Denegar el tráfico que incluye violaciones del estándar correspondiente en cada caso.<sup>7</sup>
  - e. Permitir explícitamente el tráfico de retorno hacia las direcciones propias y el tráfico de salida originado con las direcciones propias.
  - f. Permitir el tráfico de los protocolos de enrutamiento y de red estrictamente necesarios, bloqueando otros protocolos y alertando ante el uso de protocolos o servicios especialmente anómalos, como gopher, finger o NetBus.
517. Las direcciones que jamás deberían verse en Internet son la combinación de direcciones martians y unallocated que se conoce por el nombre de *bogons*<sup>8</sup>. Es

<sup>7</sup> En ocasiones dichas violaciones pueden consituir un tráfico legítimo, aunque anómalo. En este caso deberán analizarse las implicaciones de permitir este tráfico y, en caso de considerarse así, habilitar explícitamente estas anomalías en los enrutadores o cortafuegos.

<sup>8</sup> Es necesario consultar la sección “Bogon Reference Page” de la página web de Team Cymru (<http://www.cymru.com/>) para obtener información actualizada. También se puede encontrar información al respecto en las bases de datos de registro de routing, como RADB (*Routing Assets DataBase*) de la red americana MERIT, accesible mediante la herramienta *whois*: `whois.radb.net fltr-bogons / fltr-martians / fltr-unallocated`.

importante mantener esta lista, ya que repetidamente durante el año IANA asigna nuevos rangos a los registros regionales para que puedan ser utilizados.

518. Adicionalmente, es habitual proteger mediante limitación de tráfico el máximo número de tramas UDP e ICMP a transitar. Esto es muy dependiente del entorno, pero habitualmente la distribución de tráfico suele ser de un 85% TCP, 10% UDP y el restante 5% ICMP (los umbrales suelen dimensionarse en función de la capacidad del enlace). En ocasiones, si bien no se filtra directamente la superación del umbral estimado, sí se genera un evento de anomalía en caso de superar dicho umbral o, contrariamente, en caso de no alcanzar un mínimo de tráfico en la red.
519. Al igual que sucede con el resto de la tecnología corporativa, es importante verificar que los enrutadores están adecuadamente configurados –incluyendo su bastionado- cuando vayan a ponerse en producción. Se debe evitar el exceso de puertos abiertos no utilizados o de servicios no configurados con las medidas de seguridad disponibles, que ponen en peligro la seguridad de estos dispositivos críticos. Aunque la configuración por defecto de los enrutadores variará entre fabricantes, modelos y versiones, en general estos son algunos de los servicios y parámetros que suele ser necesario deshabilitar o bastionar, a no ser que exista una necesidad justificada para su utilización, con objeto de minimizar la exposición del dispositivo o de la red ante un posible ataque:
- a. TCP/UDP *small servers*. Servidores simples (chargen, daytime...) utilizados históricamente para resolver problemas de red.
  - b. Finger. Servicio que proporciona información de los usuarios conectados al sistema.
  - c. HTTP. Servidor web para gestión.
  - d. BOOTP. Servidor para la autoconfiguración de parámetros de red.
  - e. TFTP. Servicio que permite la carga y descarga de ficheros mediante protocolo TFTP.
  - f. FTP. Servicio que permite la carga y descarga de ficheros mediante protocolo FTP.
  - g. DHCP. Protocolo que permite la asignación dinámica de direcciones IP.
  - h. *Source routing*. Método de enrutado que permite modificar el camino que toma un paquete mediante la inclusión de uno o más enrutadores intermedios por los que el paquete es forzado a transitar.
  - i. SNMP. Protocolo de supervisión y gestión de dispositivos.
  - j. NTP. Servicio de sincronización de tiempo.
  - k. DNS. Servicio para asociar nombres de sistemas a direcciones IP.
  - l. Identd. Servicio de identificación.
  - m. Gratuitous ARP. Generación de datos ARP informativos no solicitados.
  - n. Cisco Discovery Protocol. Protocolo propietario de Cisco –fabricante mundial de enrutadores- utilizado para informar a los dispositivos cercanos de sus funcionalidades.



- o. Proxy-ARP. Servicio que permite la respuesta ARP a direcciones IP no pertenecientes al dispositivo.
  - p. *Directed broadcast*. Capacidad que posibilita el envío de tráfico a la dirección de *broadcast* y que puede ser utilizada para conseguir un efecto amplificador.
  - q. *Unreachable notifications*. Notificaciones ICMP generadas cuando no se puede entregar un paquete.
  - r. *Redirects*. Posibilidad de generar notificaciones ICMP indicando a un sistema que existe un mejor gateway en su red para llegar al destino.
  - s. *Mask Reply*. Capacidad de responder a consultas ICMP sobre la máscara de la red.
520. Además de los protocolos, servicios y capacidades anteriores es necesario deshabilitar todos los interfaces no utilizados y cualquier comando de autonegociación presente, realizando en su lugar la configuración manual de los parámetros necesarios. Siempre que técnicamente sea posible, se deberá gestionar el enrutador utilizando SSH v.2 frente a SSH v.1, y por supuesto evitar un protocolo en claro como TELNET.
521. Por último, tan crítico como todo lo anterior resulta mantener el dispositivo debidamente actualizado y configurado, y realizar inspecciones de seguridad periódicas sobre los enrutadores corporativos, en especial los perimetrales.

#### 12.2.2. CORTAFUEGOS

522. Un cortafuegos (*firewall*) es un sistema formado por aplicaciones, dispositivos o una combinación de éstos, encargado de hacer cumplir una política de control de acceso en las comunicaciones entre zonas de red según unos criterios de seguridad existentes. Por políticas de control de acceso se entienden las primitivas de "permitir" o "denegar" a determinados clientes el acceso a los recursos de red, expuestos como servicios, según unos privilegios de autorización. Habitualmente estos privilegios a los recursos u objetos se definen mediante listas con entradas secuenciales llamadas juegos de reglas (*rulesets*).
523. Los cortafuegos son uno de los pilares de la seguridad perimetral, constituyendo uno de los principales elementos de control para conseguir poner en práctica los distintos requisitos que impone la política de seguridad. A sus capacidades tradicionales de control de tráfico de red se han añadido multitud de funcionalidades que le permiten llevar a cabo control de acceso, filtrado de contenidos o redes privadas virtuales, así como características que entran más en el campo de la funcionalidad que de la seguridad, tales como traducción de direcciones o balanceo de carga.
524. Se pueden encontrar multitud de tipos de cortafuegos determinados por su ámbito (cortafuegos de red o de sistema), función, nivel de actuación en la torre de protocolos, inteligencia en la inspección del tráfico, etc. Además suelen diferenciarse cualitativamente y cuantitativamente por los servicios o funcionalidades añadidas que proporcionen, tales como traducción de direcciones, redes privadas virtuales, integración de mecanismos de autenticación, etc. Con independencia de esta clasificación, como dispositivo de

control de acceso es imprescindible que un cortafuegos proporcione trazas de registro (*logs*) lo más completas posible para poder auditar en cualquier momento dicha información.

525. Desde la aparición de los primeros sistemas de filtrado, el mercado ha sufrido una gran evolución y mejora, conformando distintas generaciones de sistemas cortafuegos:
- Packet Filter* (primera generación), donde se lleva a cabo un filtrado basado en información de red (direcciones IP origen y destino) y de transporte (puertos TCP/UDP y *flags* de las cabeceras)
  - Application Layer Gateway* (segunda generación), donde se realiza un filtrado a nivel de aplicación, lo que implica una total dependencia del protocolo.
  - Stateful Inspection* (tercera generación), donde se procede a filtrar el acceso usando información existente entre las capas de red y de aplicación, manteniendo información de los flujos de tráfico en una tabla de estado.
526. Actualmente el mercado está evolucionando hacia *appliances* para llevar a cabo una gestión unificada de amenazas (*Unified Threat Management*, UTM), dispositivos que además de las tareas propias de filtrado de un cortafuegos también llevan a cabo funciones de VPN, antispam, antiphishing, antispysware, filtro de contenidos, antivirus o detección y prevención de intrusiones (IDS/IPS).

### 12.2.3. SISTEMAS VPN

527. Cada vez es más habitual que las organizaciones permitan a su personal la conexión remota a su infraestructura TI a través de Internet y, por lo tanto, es necesaria una vía de conexión segura a la Organización. Para proporcionar esta conexión segura se dispone de tecnologías de redes privadas virtuales (VPN, *Virtual Private Network*), que proporcionan una capa de abstracción entre la Organización y la conexión del usuario tunelizando la conexión y aplicando una capa de cifra para garantizar la seguridad de la información transmitida.
528. Dependiendo del objetivo de la conexión se pueden distinguir dos tipos de conexiones VPN, las denominadas *site-to-site* y las denominadas *roadwarrior*. Las conexiones *site-to-site* permiten establecer un túnel entre dos sedes remotas, de forma que cualquier persona de una sede pueda tener visibilidad sobre la otra, mientras que las conexiones *roadwarrior* permiten la conexión única del equipo de trabajo de un usuario concreto a la Organización, por lo que si existen varios usuarios que necesitan acceder de forma remota cada uno de ellos necesitará una conexión VPN independiente.
529. Dentro de las tecnologías VPN existen multitud de soluciones y protocolos implicados, como PPTP (*Point to Point Tunneling Protocol*), L2F (*Layer 2 Forwarding*), L2TP (*Layer 2 Tunneling Protocol*) o IPSec (*IP Security*), siendo ésta última la más extendida actualmente.
530. IPSec presenta dos cabeceras, la cabecera AH (autenticación), que proporciona funciones de autenticación, integridad y no repudio, y la cabecera ESP (encapsulación), que proporciona confidencialidad de los datos. A su vez,

presenta dos modos de funcionamiento, el modo transporte, donde únicamente se cifran los datos enviados dejando intactas las cabeceras originales, y el modo túnel, en el que aparte de cifrar los datos enviados se cifra la cabecera IP original, añadiendo una nueva.

531. El uso de IPSec o de protocolos equivalentes de redes privadas virtuales, que aporten la seguridad necesaria a las conexiones remotas a la Organización, debe considerarse obligatorio en cualquier solución de acceso remoto a los sistemas corporativos a través de Internet.

#### 12.2.4. DISPOSITIVOS DE RED

532. La interconexión de los distintos elementos de la seguridad perimetral entre sí y con las distintas subredes de una Organización se realiza a través de dispositivos de red, habitualmente *switches*. El uso de dispositivos de red más antiguos, de tipos *hub*, debe considerarse prohibido en cualquier Organización, debido a los riesgos que introduce la utilización de estos elementos.
533. Los *switches*, especialmente los de gama baja y media, adolecen de problemas ampliamente conocidos y son susceptibles de errores de configuración que pueden permitir a un atacante que ha conseguido comprometer uno de los sistemas conectados al *switch* perpetrar diversos tipos de ataques contra el propio dispositivo u otros que se encuentren conectados a él. De forma añadida, y debido a las características de flexibilidad y potencia que permiten los switches, es práctica habitual el concentrar todas las conexiones de red en un switch común, empleando por ejemplo redes locales virtuales (*Virtual Local Area Networks*, VLAN) para llevar a cabo la compartimentación necesaria para aislar segmentos con distintos requisitos de seguridad.
534. Existe la posibilidad de que las VLAN persistan entre diferentes switches, e incluso a través de redes de área extensa (*Wide Area Network*, WAN) si se puede producir encapsulado de nivel 2. Para ello se utiliza el *trunking*, consistente en permitir que una sola conexión física contenga múltiples VLANs a través de la introducción de etiquetas en las tramas, de acuerdo a las especificaciones del protocolo 802.1q.
535. Las VLANs no fueron creadas explícitamente con un objetivo de seguridad, sino con el objeto de limitar el efecto del tráfico de *broadcast* y *multicast* en redes grandes, por lo que ha existido tradicionalmente cierta controversia acerca de la seguridad proporcionada por las mismas. Se han revelado diversas vulnerabilidades en la estanqueidad proporcionada por las VLAN, permitiéndose en ocasiones introducir tráfico de forma no autorizada desde una VLAN a otra distinta (salto de VLAN o *VLAN Hopping*). Este fenómeno ha sido identificado especialmente en *switches* de gama baja o media, como se ha indicado, los más vulnerables habitualmente, cuando la configuración de los mismos no es óptima. Los *switches* de gama media y alta disponen de medidas de seguridad adicionales para detectar y mitigar en la medida de lo posible ataques a nivel de enlace de datos, como *ARP flooding*, ataques al protocolo *Spanning Tree*, tormentas *multicast/broadcast*, etc., por lo que las organizaciones deben evaluar la necesidad de implantar este tipo de dispositivos en las redes corporativas.

### 12.2.5. SERVIDORES

536. Los servidores son los elementos encargados de ofrecer servicios, ya sean estructurales o productivos, al resto de la Organización, a otras Organizaciones o al público en general. Dado que para ofrecer un servicio hay que proporcionar acceso de una u otra forma a programas corriendo en el sistema y que en general todos los programas contienen fallos de programación, el simple hecho de ofrecer estos servicios introduce un riesgo, inicialmente hacia el propio servidor, pero por extensión a cualquier otro sistema o dispositivo de su entorno.
537. No todos los servicios introducen el mismo riesgo de seguridad en la Organización, ya que éste dependerá de factores como su complejidad o su necesidad de interactuar con entornos potencialmente hostiles, como Internet. De la misma manera no todos los servicios son igual de críticos, existiendo habitualmente servicios de los cuales la Organización depende en gran medida para su correcto funcionamiento y cuya disrupción o disfunción causaría un grave perjuicio. Entre este tipo de servicios críticos se suelen encontrar habitualmente los servicios de nombres (DNS), de tiempos (NTP), de correo (SMTP) y los servicios web corporativos.
538. Después de lo expuesto resulta claro que para contar con una seguridad perimetral robusta habrá que asegurar debidamente a los servidores. Para ello será imprescindible aplicar procedimientos de buenas prácticas de instalación y configuración (bastionado), mantenimiento y operación. No hay que olvidar que tanto los sistemas operativos como las aplicaciones actuales cuentan habitualmente con un gran número de mecanismos de seguridad que pueden ser configurados para mitigar el riesgo, sumándose así a las medidas de seguridad perimetral desplegadas.
539. Algunas de estas medidas de seguridad adicionales están basadas en la instalación de un firewall o proxy dedicado en el equipo final, el cual únicamente analizará un tipo de tráfico específico, aportando una capa más de seguridad al servidor y por tanto al entorno. Dentro de este tipo de sistemas, y teniendo en cuenta la gran evolución de los servicios web, es necesario destacar los *Web Application Firewalls* (WAF) y los *firewall* de base de datos. Los WAF son sistemas de protección de tráfico web, con una base de datos de firmas de las distintas vulnerabilidades existentes, capaces de analizar el comportamiento del usuario y detectar manipulación de parámetros en cabeceras o cookies, inyecciones SQL o ataques de *Cross-site Scripting* (XSS), llegando a bloquear el tráfico anómalo detectado. Por otra parte, los firewalls de base de datos, al igual que en el caso anterior, son sistemas dedicados que se instalan como *frontend* de los servidores finales, y analizan exclusivamente el tráfico SQL, detectando posibles alteraciones y haciendo cumplir la política de acceso.

### 12.2.6. SISTEMAS DE USUARIO Y SISTEMAS MÓVILES

540. Los sistemas de usuario han de ser contemplados hoy en día dentro de las estrategias de seguridad perimetral debido a la profusión de ataques que explotan las vulnerabilidades presentes en los mismos, en muchos casos con la

ayuda de técnicas de ingeniería social, logrando de forma eficaz romper el perímetro de la Organización desde dentro hacia afuera.

541. Si bien el principal medio para actuar contra este tipo de amenazas es una buena política de actualización de sistemas operativos y aplicaciones, así como controles de software malicioso, y una formación adecuada de los usuarios en lo que a seguridad se refiere, también es cierto que se puede y se debe establecer una política de seguridad que sea tan estricta desde dentro hacia afuera como lo es desde fuera hacia dentro, incluyendo el filtrado de tráfico, la utilización de proxies, y el despliegue y operación de sistemas de detección y/o prevención de intrusiones sobre el tráfico saliente de la Organización (denominado en ocasiones sistemas de detección de extrusiones).
542. Dentro de los sistemas de usuario merecen una mención especial los sistemas móviles, tales como portátiles, *smartphones*, tabletas, etc. Cuando a dichos sistemas se les permite acceso a la Organización desde fuera de la misma están extendiendo de forma natural su perímetro, por lo que es necesario controlar especialmente todos los elementos que introduzcan movilidad en la información corporativa.

#### 12.2.7. TECNOLOGÍAS INALÁMBRICAS

543. La introducción masiva de tecnologías inalámbricas, en especial WiFi, ha propiciado la paulatina disolución del perímetro físico de la Organización. Si tradicionalmente era necesario contar con acceso físico al interior de la Organización o penetrar las capas de protección más externas para poder acceder a su núcleo, hoy basta con situarse dentro del radio de alcance de los dispositivos inalámbricos de la misma para poder contar con acceso directo a las redes internas o, en su defecto, con una situación privilegiada desde donde poder perpetrar los ataques de forma más eficaz.
544. A pesar de que estas tecnologías han incluido en las sucesivas especificaciones de sus protocolos diversas mejoras en el ámbito de la seguridad, lo cierto es que hasta el momento ninguna de ellas ha satisfecho plenamente los requisitos necesarios para asegurar una adecuada protección en términos de confidencialidad, integridad y disponibilidad de la información manejada. Diversos problemas tanto en los protocolos como en las implementaciones que los fabricantes han plasmado en sus productos han resultado en la posibilidad de poder realizar ataques de diversos tipos, rompiendo en muchos casos el perímetro, evitando los distintos controles de seguridad establecidos por dispositivos como cortafuegos o enrutadores y burlando sistemas de detección y prevención de intrusos desplegados en la Organización.
545. A la hora de implementar estas tecnologías dentro de la Organización habrá que asegurarse siempre que sea posible hacer uso de las características de seguridad incluidas en las últimas versiones de los protocolos, desechando aquellos que han sido rotos o se espera que lo sean en breve; por ejemplo, en el caso de las redes WiFi, esto implica poner en marcha medidas como el control de acceso, la regeneración de claves vía TKIP o el cifrado robusto mediante el uso de AES, por poner unos ejemplos, y por supuesto evitar el uso de protocolos como WEP o WPA. Una configuración adecuada de estos parámetros hará mucho más

compleja la tarea de penetrar en el perímetro a partir de la infraestructura inalámbrica

546. En el caso de los dispositivos que hacen uso de la tecnología Bluetooth, cada vez más extendida en todo tipo de dispositivos de uso personal y corporativo, el perfil de utilización actual de dichos dispositivos, el tipo de vulnerabilidades detectadas y su alcance nominal, normalmente del orden de unos pocos metros, no sitúa en estos momentos su uso en el mismo nivel de riesgo para la Organización que en el caso de los dispositivos WiFi.
547. Finalmente, otro riesgo a considerar de forma especial, es el uso de *smartphones* que incorporan conexión WiFi y 3G. Aunque habitualmente en la mayor parte de modelos no se permite el uso simultáneo de ambos interfaces de comunicación, un usuario malintencionado podría alterar este comportamiento, lo que podría propiciar que en un momento determinado se puentee la red corporativa directamente a Internet a través de estos dispositivos, sin pasar por un cortafuegos, con los evidentes riesgos de seguridad que esto implica para la Organización. Es por tanto obligatorio establecer los controles de seguridad necesarios en la conexión de estos dispositivos a la red de la Organización, tanto a la hora de hablar de dispositivos corporativos como de dispositivos personales, en las tendencias BYOD (*Bring Your Own Device*) actuales.



## 13. DETECCIÓN DE INTRUSOS

### 13.1. INTRODUCCIÓN

548. Se denomina **intrusión** a un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de la información o de los entornos que la manejan. A los sistemas utilizados para detectar las intrusiones se les denomina sistemas de detección de intrusiones (*Intrusion Detection Systems*, IDS) o, más habitualmente y aunque no sea la traducción literal, **sistemas de detección de intrusos**.
549. Los sistemas de detección de intrusos tienen por objeto detectar ataques desde la Organización (extrusiones), hacia la Organización (intrusiones) o en la propia Organización. En este sentido es obligatorio el análisis y despliegue de entornos que permitan esta detección, con el objetivo de poder responder a situaciones de riesgo en el menor tiempo posible. Es necesario evaluar la conveniencia de implantar un esquema mixto que contemple al menos la detección de intrusos en red y la detección de intrusos en sistemas.
550. Para cumplir sus objetivos de forma correcta, cualquier IDS considerado en la Organización debe cumplir una serie de requisitos obligatorios. En primer lugar, debe ejecutarse continuamente sin supervisión humana (con independencia de que simplemente registre posibles intrusiones o de que lance incluso respuestas automáticas). Además, debe ser aceptable en el entorno, tanto porque permita el correcto funcionamiento del resto de sistemas de la Organización (por ejemplo, desde el punto de vista de sobrecarga en el entorno) como porque la información que genera sea útil y se permita su gestión eficiente. En este sentido, las tasas de falsos positivos (detecciones que realmente no se corresponden con una intrusión) y de falsos negativos (intrusiones no detectadas por el sistema) deben ser, ambas, mínimas. Adicionalmente, debe ser lo suficientemente adaptable al entorno de trabajo, incluyendo en esta capacidad de adaptación la tolerancia a fallos o a situaciones anómalas.

### 13.2. CLASIFICACIÓN DE LOS IDS

551. Generalmente existen dos grandes enfoques a la hora de clasificar a los sistemas de detección de intrusos: o bien en función de qué sistemas monitorizan o bien en función de cómo lo hacen. En la primera de estas aproximaciones existen dos grupos de sistemas de detección de intrusos: los que analizan actividades de un único sistema en busca de posibles intrusiones, y los que lo hacen de una red, aunque se emplacen en uno sólo de los Sistemas de la misma.
552. Un IDS **basado en red** (o NIDS, *Network based IDS*) monitoriza los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. El IDS puede situarse en cualquiera de los hosts o en un elemento que analice todo el tráfico, como un switch o un enrutador. Esté donde esté, monitorizará diversas máquinas y no una sola: esta es la principal diferencia con los sistemas de detección de intrusos basados en *host*.
553. Mientras que los sistemas de detección de intrusos basados en red monitorizan toda una red, los **basados en máquina** (HIDS, *Host based IDS*) realizan su



función protegiendo un único sistema. El IDS busca patrones que puedan denotar una intrusión y alerta o toma las medidas oportunas en caso de que uno de estos patrones sea detectado. Dentro de esta categoría se suelen diferenciar los verificadores de integridad del sistema (SIV, *Sytem Integrity Verifiers*), los monitores de registros (LFM, *Log File Monitor*) y los *honeypots* o tarros de miel, también llamados sistemas de engaño. Los verificadores de integridad monitorizan archivos de un Sistema en busca de posibles modificaciones no autorizadas, los monitores de registros vigilan archivos de log en busca de patrones que puedan indicar una situación anómala y, finalmente, los sistemas de engaño son mecanismos encargados de simular objetos (servicios, ficheros, aplicaciones...) con problemas de seguridad de forma que un atacante piense que realmente el problema se puede aprovechar en beneficio propio, cuando realmente se está aprovechando para registrar todas sus actividades.

554. La segunda gran clasificación de los sistemas de detección de intrusos se realiza en función de cómo operan estos sistemas. Existen dos grandes técnicas de detección de intrusos: las basadas en la detección de anomalías (*anomaly detection*) y las basadas en la detección de usos indebidos (*misuse detection*). La primera de ellas, la detección de anomalías, se basa en la suposición de que una intrusión se puede considerar una anomalía del entorno, por lo que si el establecer un perfil del comportamiento habitual permitirá detectar las intrusiones por pura estadística. Se trata por tanto de una metodología que trata de modelar la normalidad para identificar la anormalidad. Por el contrario, la detección de usos indebidos presupone que es posible establecer patrones para los diferentes ataques conocidos y algunas de sus variaciones, identificándolos por tanto de forma directa.

### 13.3. SISTEMAS Y REDES TRAMPA

555. Los sistemas y redes trampa, conocidos como *honeypots* (tarros de miel) y *honeynets* respectivamente, se han ido introduciendo paulatinamente en las arquitecturas de seguridad durante los últimos años. Los *honeypots* se definen como recursos cuyo valor reside en ser atacado o comprometido. Habitualmente los *honeypots* simulan ser un recurso más de la infraestructura (sistema, dispositivo de red, etc.), pero no serán utilizados para propósitos de producción: de este modo, cualquier actividad detectada en este sistema será de carácter malicioso y deberá generar una alerta. Su objetivo es obtener nuevos patrones de comportamiento e información de nuevos ataques, con el objetivo de prevenirlos y detectarlos en los sistemas reales.
556. Generalmente la clasificación de los tarros de miel se realiza referenciando el grado de compromiso que éstos introducen en la red. Así, están los *honeypots* de **baja interacción**, que simulan la existencia de servicios vulnerables y escuchan y almacenan todas las peticiones recibidas en ficheros de registro, conformando un sistema pasivo que no responde a las solicitudes o interactúa con el atacante; el caso más extremo es el denominado *honeypotoken*, un tarro de miel que simplemente por ser accedido implicará una alerta directa. Por el contrario, los *honeypots* de **alta interacción** son sistemas que permiten a un atacante interactuar en un alto grado con el tarro de miel, por lo que se introducen riesgos adicionales en el entorno, ya que si un atacante consigue manipular su funcionamiento estándar puede lograr acceso no autorizado a uno o más

Sistemas. A cambio de este riesgo, ofrecen un estudio completo del comportamiento y actividades de los atacantes, ya que resultarán más atractivos y difíciles de detectar para éstos que los tarros de miel de baja interacción.

557. Las *honeynets* son redes dedicadas especialmente a albergar tarros de miel, constituyendo en sí mismas redes trampa a las que dirigir a un atacante –o a las que accederá *per se*– con el objeto de analizar en un nivel de detalle alto su comportamiento. Se trata de entornos de muy alta interacción dedicados en exclusiva a hospedar trampas y que no deben mezclarse, bajo ningún concepto, con el entorno productivo de la Organización (ni siquiera deben utilizar un direccionamiento IP asignado a la Organización).
558. Resulta obvio que, especialmente en el caso de las *honeynets*, el despliegue de sistemas trampa introducen un riesgo a considerar en la Organización, tanto por motivos reputacionales como por el hecho de que estas plataformas puedan ser posteriormente utilizada para atacar a otros elementos de la infraestructura o incluso a otras Organizaciones. La Organización debe evaluar estos riesgos antes de desplegar sistemas trampa de alta interacción, que adicionalmente implican costes de despliegue y mantenimiento mucho más elevados que los entornos de baja interacción. Por el contrario, estos últimos constituyen un arma eficaz para detectar intrusiones dentro de la Organización con un coste de despliegue y mantenimiento relativamente bajo, por lo que se debe considerar su implantación en todo tipo de organizaciones.

#### 13.4. IMPLANTACIÓN EN LA ORGANIZACIÓN

559. Tal y como se ha indicado, la Organización debe implantar mecanismos para detectar, con un nivel de confianza aceptable, ataques o situaciones anómalas, de forma que se permita responder a las mismas en el menor tiempo posible desde que se producen. En este sentido, debe considerarse obligatoria la implantación y explotación adecuada de sistemas de detección de intrusos entendidos como un control global, es decir, por encima de productos concretos, de herramientas que proporcionen a la Organización la capacidad para detectar intrusiones.
560. Así, deben implantarse sondas de detección basadas en red, al menos para los segmentos más relevantes de la Organización y sondas basadas en *host* en aquellos Sistemas críticos. De la misma forma, debe evaluarse convenientemente la necesidad y ventajas de desplegar capacidades de detección de intrusos en los sistemas cortafuegos de la Organización. Estas aproximaciones generarán alertas que deben ser correladas para evitar falsos positivos y centrar la atención del equipo de seguridad en aquellas alertas más relevantes, que serán convenientemente tratadas en la Organización.
561. En el ámbito de la detección basada en red, una de las partes fundamentales del esquema de detección la forman las sondas desplegadas en los segmentos de red a monitorizar, que tienen como objetivo determinar cuándo un usuario trata de realizar actividades sospechosas en el dominio de control de la sonda. Un sistema de este tipo desplegado, por ejemplo, en un segmento de DMZ, permitiría al administrador de seguridad, disponer de un sistema de alerta ante intrusiones a dicha red, bien sean producidas por usuarios situados en Internet como en la red interna.

562. Las sondas desplegadas permiten trabajar como un *sniffer* de red, inspeccionando el contenido de los paquetes que circulan por el medio cableado, comparándolos con un catálogo de firmas o patrones de ataque predeterminados (generalmente, esquemas basados en detección de usos indebidos). Este flujo de información capturado es inspeccionado en tiempo real, disparando inmediatamente una alerta si un patrón de tráfico coincide con el del catálogo de usos indebidos de la sonda. Adicionalmente, este catálogo debe ser actualizado de forma periódica, obteniendo así acceso a la detección de nuevos patrones de ataque en la Organización.
563. Adicionalmente a los sistemas basados en red, los sistemas de detección basados en máquina –al menos para los Sistemas críticos- deben contemplar el control de integridad de archivos (SIV), detectando cambios no controlados y alertando cuando éstos ocurren, la monitorización de registros (LFM), informando de aquellas actividades relevantes para la seguridad recogidas en los sistemas de registro de las máquinas y el despliegue de *honeytokens* para controlar el acceso a objetos (ficheros, registros de bases de datos, servicios...) que puedan suponer un riesgo para la seguridad corporativa.
564. El último aspecto del esquema de detección a contemplar es la identificación de tráfico anómalo en los entornos cortafuegos de la Organización, mediante patrones de tráfico que puedan implicar riesgos corporativos. Ejemplos de dichos patrones son las violaciones de protocolo, los tráficos entrantes con origen en una zona de red diferente a la esperada o el uso de protocolos en desuso, por citar unos cuantos.
565. Tal y como se ha indicado, las diferentes aproximaciones a la detección generarán una cantidad de alertas –a priori, elevada- que deben ser procesadas en la Organización. Dicho procesamiento pasa de forma obligatoria por una correlación que permita al menos tanto la eliminación de falsos positivos como la priorización de las alertas más significativas, para que el equipo de respuesta las trate en primera instancia. Habitualmente, tras el proceso de correlación, las alertas generadas y correladas se reflejarán y tratarán, por parte del equipo correspondiente, en un entorno SIEM/SEM desplegado en la Organización.

### 13.5. AMPLIACIÓN DEL ESQUEMA

566. El esquema técnico de detección habitual expuesto en la presente guía (esto es, NIDS+IDS, e incluso detección en cortafuegos) es necesario pero no suficiente en un entorno de monitorización global de la Organización. Hoy en día las técnicas de monitorización deben integrarse con la detección de intrusos clásica para permitir la detección, a partir de ambas fuentes de datos, de una gran variedad de elementos de riesgo para la Organización.
567. De forma adicional a la detección de intrusos sobre la infraestructura tecnológica de la Organización (enfoque clásico, expuesto en la presente guía), se deben integrar en un esquema de detección elementos como los entornos no cooperativos (foros, blogs, redes sociales...) ajenos al control de la Organización, las fuentes de información de seguridad (noticias, CERT, FFCCSE, medios de comunicaciones...) o incluso las personas. En definitiva, todo aquello que pueda causar una intrusión o derivar en un incidente de seguridad.

568. En este contexto de detección global se tratará con una gran cantidad de datos adquiridos por los sistemas de detección e imposibles de manejar por un humano. Además de las reglas de correlación estándar, basadas en parámetros técnicos (origen y destino de una trama, contenido de campos de datos o cabeceras, etc.), se debe evaluar la necesidad de aportar inteligencia por encima de la correlación pura, por ejemplo considerando parámetros como la contextualización de cadenas en los campos de datos, la geolocalización de tráficos o los flujos de entrada y salida de información corporativa.
569. Hay que tender, en definitiva, a un esquema de detección globalizado que adquiera datos de múltiples fuentes que poco o nada tienen que ver entre sí, que permita la correlación de todos estos datos aportándoles la suficiente inteligencia y que capacite así a la Organización para proporcionar una respuesta adecuada en el menor tiempo posible siempre que se considere un riesgo relevante.

### 13.6. SISTEMAS DE PREVENCIÓN DE INTRUSIONES

570. Los sistemas de prevención de intrusiones (*Intrusion Prevention Systems*, IPS) utilizan una aproximación parecida a la de los IDS para detectar ataques, pero en lugar de tan solo detectarlos y generar algún tipo de alerta, los IPS intentarán detenerlos, convirtiendo el elemento de seguridad pasiva en un elemento activo. Al igual que sucede en el caso de los IDS, existen IPS de red y de sistema.
571. Resulta evidente que los IPS no pueden permitirse la existencia de falsos positivos, ya que al ser elementos activos estarían rechazando operaciones válidas (tráfico, acciones de los usuarios, etc.). Para minimizar la tasa de falsos positivos se utilizan las estrategias más estables de las tecnologías de IDS, reglas mucho más exactas, análisis de anomalías y otros mecanismos que permiten esa reducción.
572. En general la utilización de IPS es recomendable tanto en sistemas como en red, aunque suele suponer una inversión considerable. A este respecto, será adecuado seguir las mismas pautas definidas para los IDS en cuanto a priorizar el despliegue en aquellos sistemas de mayor criticidad, bien por la información que manejan, bien por su grado de exposición a ataques.

### 13.7. ATAQUES

573. En los inicios de esta misma guía CCN-STIC se ha hablado de la confidencialidad, integridad y disponibilidad de la información como las características que conforman su seguridad y, en este sentido, se ha hablado también de amenazas a la seguridad de la información, clasificándolas en cuatro grandes familias: interrupción, interceptación, modificación y fabricación. Dentro de estas categorías, se entienden los ataques como una **amenaza intencionada**, causada por un actor que quiere generar un impacto en la Organización. Se tratarán en este punto algunos de los ataques más habituales contra los Sistemas, sin considerar ataques que quedan fuera del ámbito de la presente guía (ingeniería social, ataques semánticos, intrusiones físicas...).
574. Habitualmente, cualquier Sistema interconectado a una red (en especial redes no clasificadas) está expuesto a una serie de ataques relevantes. Se indican a continuación algunos de los más comunes, presentando una relación no

exhaustiva de ataques que todo el personal involucrado en la gestión de las TIC debe conocer.

- a. Barrido (“escaneo”) de puertos. Ataque que trata de obtener información básica acerca de qué servicios se ofrecen en un determinado Sistema, así como otros detalles técnicos del mismo. Se trata de un ataque NO severo pero que suele constituir una de las etapas iniciales de ataques más duros.
  - b. *Spoofing*. Generación de tráfico utilizando un origen falseado. Los tipos de spoofing más comunes son el IP Spoofing, el DNS Spoofing o el ARP Spoofing, por citar unos cuantos.
  - c. Denegaciones de Servicio (DoS). Ataque contra un recurso con el objetivo de degradar total o parcialmente los servicios prestados por ese recurso a sus usuarios legítimos.
  - d. Denegaciones de servicio distribuidas (DDoS). DoS causado por un ataque masivo y simultáneo a un único objetivo real, muy extendido en la actualidad.
  - e. *Sniffing*. Captura del tráfico que circula por una red, por ejemplo en un sistema intermedio.
575. Estos ataques y muchos otros no referenciados deben ser detectados, siempre que técnicamente sea posible, por el esquema de detección de intrusos de la Organización, de forma que ésta pueda proporcionar una respuesta rápida y adecuada ante los mismos antes de que se materialice un impacto relevante.

## 14. SEGURIDAD EN REDES INALÁMBRICAS

### 14.1. INTRODUCCIÓN

576. En los últimos años se ha producido un gran desarrollo en la conectividad “sin cables”. Cada vez más dispositivos (ordenadores, teléfonos, etc.) incorporan estas capacidades de forma nativa en cualquiera de sus distintas formas. En el presente capítulo se abordarán las principales especificaciones técnicas y aspectos de seguridad de las tecnologías inalámbricas más populares:
- a. **WiFi.** Mecanismo de conexión inalámbrica de área local (WLAN) de dispositivos basados en la norma IEEE 802.11.
  - b. **Bluetooth.** Especificación inalámbrica para redes de área personal (WPAN), utilizado para la comunicación de teléfonos móviles, tabletas y ordenadores personales entre otros.
  - c. **WiMAX.** Norma de transmisión de datos IEEE 802.16 para el intercambio de información en redes de área amplia (WAN), utilizada para dar cobertura inalámbrica de comunicación a entornos residenciales en la última milla.
  - d. **RFID.** Sistema de comunicación inalámbrica de corto alcance destinado a la identificación de objetos, animales o personas, a través de etiquetas con capacidades de albergar información y ser transmitida a través de ondas de radio.
577. Siendo evidentes las ventajas de portabilidad que ofrecen estas tecnologías, introducen riesgos añadidos a los ya existentes en cualquier red cableada, que deben ser tratados de forma cuidadosa y específica con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de estas infraestructuras y los datos que se transmiten haciendo uso de ellas.

### 14.2. ESPECTRO ELECTROMAGNÉTICO

578. En el siguiente diagrama se muestra el espectro electromagnético general y el uso de los diferentes rangos de frecuencias por diferentes servicios y aplicaciones.

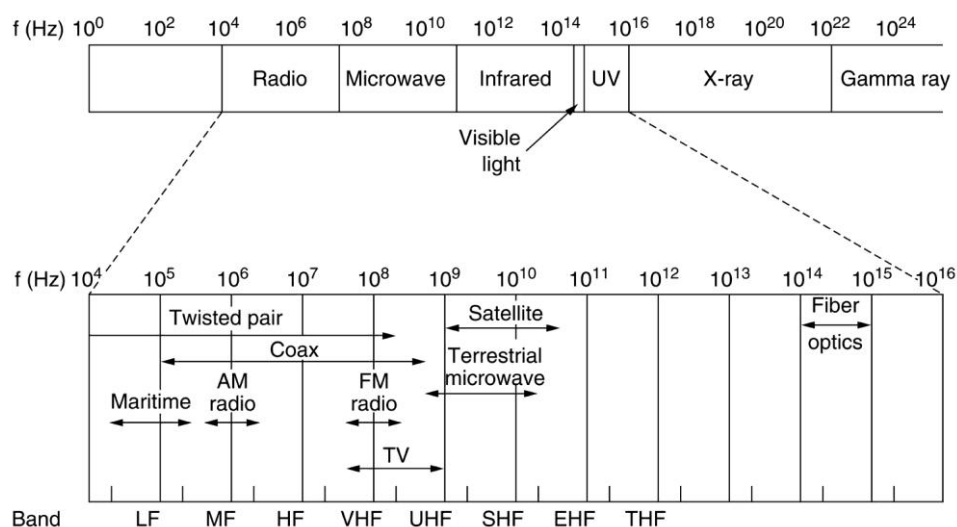
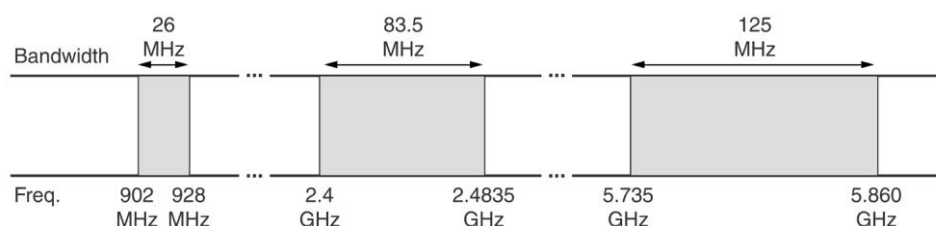


Figura 15.- Espectro Electromagnético

579. Dentro del espectro electromagnético existen varias bandas en las que no se ha contemplado la necesidad de licencias para su uso: son las llamadas bandas ISM (*Industrial, Scientific and Medical*), que se reservaron para la investigación y el desarrollo por la comunidad científica y la industria. Según el Cuadro Nacional de Atribución de Frecuencias del Ministerio de Industria, Energía y Turismo (CNAF) en su nota UN-51 y UN-128, las bandas nacionales que no requieren licencia, dentro de esta categoría son las siguientes:

- 2400 a 2500 MHz (frecuencia central 2450 MHz)
- 5725 a 5875 MHz (frecuencia central 5800 MHz)
- 24,00 a 24,25 GHz (frecuencia central 24,125 GHz)
- 61,00 a 61,50 GHz (frecuencia central 61,250 GHz)

580. Al margen de las anteriores, en la nota UN-128 se especifica un rango especial para las redes locales, que trabajan en los rangos 5150-5350 MHz y 5470-5725MHz. Estas bandas de frecuencias son las utilizadas por la industria para el desarrollo de todo tipo de elementos, desde electrodomésticos hasta redes inalámbricas.

Figura 16.- Bandas ISM (*Industrial, Scientific and Medical*)



581. Tecnologías como las redes basadas en el estándar 802.11, o WiFi (como popularmente se conocen), pueden trabajar simultáneamente dentro del espectro ISM de los 2,4 GHz y 5 GHz, tal y como muestra la ilustración anterior. Otras especificaciones como Bluetooth también lo hacen en la banda de los 2,4 GHz, pero no es el caso de las tecnologías RFID, generalmente con un rango de cobertura menor y cuya dispersión en el espectro electromagnético viene resumida por la siguiente ilustración:

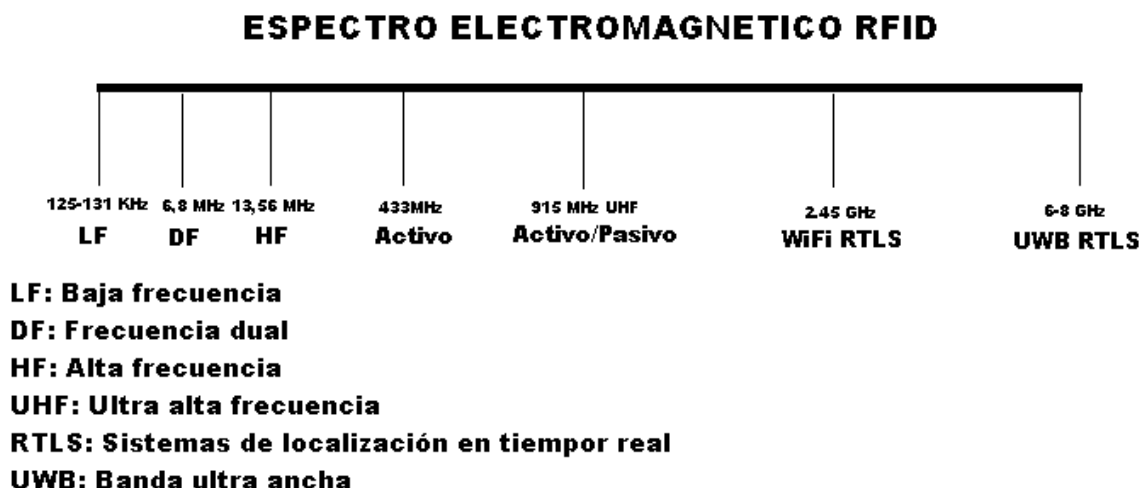


Figura 1: Espectro RFID

582. Por lo que respecta a WiMAX, existen dos perfiles de equipamiento en el mercado que trabajan respectivamente en la banda ISM de los 5,4 GHz, sin necesidad por lo tanto de licencia, y en el espectro de los 2,5 y 3,5 GHz, con su correspondiente licencia en este caso.

### 14.3. REDES IEEE 802.11 (WIFI)

#### 14.3.1. PROPIEDADES DEL ESPECTRO ELECTROMAGNÉTICO

583. Las redes inalámbricas basadas en el estándar IEEE 802.11 trabajan en el rango de 2.4 GHz para sus especificaciones IEEE 802.11abg y en el de 2.4-5GHz para IEEE 802.11n. Los principales elementos que influyen en la transmisión son el ancho de banda, las técnicas de modulación (como FDMA, TDMA o CDMA), los métodos de codificación o la potencia de emisión del dispositivo, entre otros.

	Estándares			
	802.11a	802.11b	802.11g	802.11n
Rango de Frecuencia (Ghz)	5,15-5,825 GHz	2,4-2,4835 GHz	2,4-2,4835 GHz	2,4-2,4835 GHz 5,15-5,825 GHz

Codificación	OFMD	DSSS	OFMD (manteniendo DSSS para compatibilidad con 802.11b)	OFMD
Ancho de Banda Máximo	54 Mbps	11Mbps	54Mbps	600Mbps (teóricos)

584. Además, hay que tener en cuenta en la transmisión las posibles interferencias que se pueden producir por dispositivos inalámbricos operando en el mismo canal, así como las pérdidas de señal por los distintos materiales que ésta deba atravesar. El rango de frecuencias en el que trabajan los dispositivos inalámbricos, permite la coexistencia en la misma área de cobertura de tres canales simultáneos para la banda de 2,4 Ghz.

#### 14.3.2. GRUPOS DE TRABAJO PARA LA NORMA IEEE 802.11

585. Las principales normas desarrolladas por el IEEE en el ámbito de las redes de área local inalámbricas son las siguientes:
- 802.11: Estándar original, con capacidad de 1 y 2 Mbps. (1997).
  - 802.11: Desarrollo del estándar original en la banda de los 5 Ghz, con capacidad máxima de 54 Mbps (1999).
  - 802.11b: Desarrollo del estándar original en la banda de los 2.4 Ghz, con capacidad máxima de 11 Mbps (1999).
  - 802.11c: Estándar que define las características que necesita el punto de acceso (*Access Point*, AP) para actuar como puente (*bridge*).
  - 802.11d: Estándar que permite el uso de la comunicación mediante el protocolo 802.11 en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar (2001).
  - 802.11e: Estándar sobre la introducción de calidad de servicio (*Quality of Service*, QoS) en la comunicación entre AP y clientes.
  - 802.11f: Estándar que define una práctica recomendada para el intercambio de información entre los AP. La adopción de esta práctica permitirá el *roaming* entre diferentes redes.
  - 802.11g: Desarrollo del estándar original en la banda de los 2.4 Ghz, con capacidad máxima de 54 Mbps (2004).
  - 802.11h: Estándar que permite la asignación dinámica de canales.
  - 802.11i: Estándar que define el cifrado y la autenticación en redes inalámbricas para mejorar las deficiencias de WEP (2004).
  - 802.11j: Estándar desarrollado para cumplir la normativa japonesa.
  - 802.11n: Estándar que incrementa la velocidad de transmisión hasta 600Mbit/s utilizando antenas MIMO (múltiple entrada, múltiple salida) (2009)

- m. 802.11p: Estándar destinado a cubrir las necesidades de vehículos en movimiento (2010).
  - n. 802.11s: Estándar para el funcionamiento en redes malladas (2011)
  - o. 802.11u: Desarrollo de mejoras para la implementación de puntos de acceso y autorización de clientes (2011)
  - p. 802.11v: Desarrollo de la gestión de la red inalámbrica (2011).
  - q. 802.11w: Estándar destinado a la protección de las tramas de gestión (2009).
  - r. 802.11aa: Estándar para la mejora de la comunicación en tiempo real de flujos de vídeo y audio (2012).
  - s. 802.11ad: Mejoras en la velocidad de transmisión de datos de la *Wireless Gigabit Alliance*, para la banda de los 60GHz (2012).
  - t. 802.11ae: Desarrollo de mejoras para la priorización de las tramas de gestión (2012).
586. En cuanto a la ubicación de estos estándares en las capas del modelo OSI, los mismos se encuentran en las capas física y de enlace de datos.

#### 14.3.3. DISPOSITIVOS

587. Existen dos grandes tipos de dispositivos WiFi: en primer lugar, las **tarjetas de red** integradas en los sistemas a través de diferentes protocolos (PCI, PCMCIA, USB, etc.). En ellas, la velocidad de transmisión y recepción es variable, dependiendo del fabricante y de los estándares que cumpla en cada caso.



Figura 18.- Tarjetas de red

588. En segundo lugar, los **puntos de acceso** (AP), encargados de recibir la información de las tarjetas de red cliente bien para su centralización, bien para su encaminamiento. Complementan a los *hubs*, *switches*, *bridges* o *routers* que se encuentren en la red. Se identifican frente a los clientes inalámbricos utilizando como parámetros el nombre de red (ESSID) y su dirección MAC.



Figura 19.- Punto de acceso y arquitectura de red

#### 14.3.4. FUNCIONAMIENTO

589. Todos los dispositivos, independientemente de que sean tarjetas de red o puntos de acceso, tienen tres modos de funcionamiento.
- El modo **Managed** es el modo en el que un cliente se conecta a un punto de acceso, para que éste último le sirva de concentrador, o a una red “Ad-Hoc”.
  - El modo **Master** es el modo en el que trabajan los puntos de acceso. Es posible configurar una tarjeta de red para que funcione en este modo si se dispone del *firmware* apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.
  - El modo **Monitor** permite capturar en modo promiscuo todas las tramas 802.11 en un determinado canal.
590. Estos modos de funcionamiento indican que básicamente el hardware de los dispositivos WiFi es muy similar, añadiendo cierta funcionalidad extra a los puntos de acceso vía *firmware* o *software*, para que se comporten como tal.
591. Cuando un cliente se conecta a un punto de acceso, la calidad de la conexión se ve afectada principalmente por los siguientes parámetros:
- Velocidad máxima del AP, en función de la norma que soporte (con 802.11n esta velocidad será de hasta 600Mbps teóricos).
  - Distancia al AP: a mayor distancia menor velocidad.
  - Elementos intermedios entre las tarjetas de red y el AP: las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el AP y la tarjeta de red modifican la velocidad de transmisión a la baja.
  - Saturación del espectro e interferencias: cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones, por lo que la velocidad se reducirá.

592. El alcance teórico de los puntos de acceso suele ser de aproximadamente 300 metros. En condiciones reales, el rango de alcance de una conexión varía por la infinidad de condiciones que le afectan. A los dispositivos inalámbricos se les pueden incorporar antenas externas con diferentes características que permiten extender los enlaces, estando documentados enlaces a decenas de kilómetros.

#### 14.3.5. TOPOLOGÍAS DE RED

593. Existen dos tipos principales de topologías de redes WiFi: *ad hoc* e infraestructura. En la primera de ellas, en la topología *ad hoc*, cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red de igual a igual, para lo que sólo será necesario disponer de un BSSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos en la red, que hagan bajar el rendimiento.

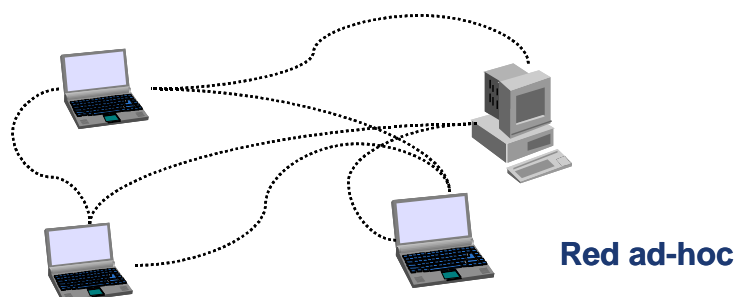


Figura 20.- Topología de red Ad-Hoc

594. Dentro de este tipo de redes se están desarrollando nuevas topologías que incluyen capacidades de encaminado (*Mobile Ad-Hoc Networks*), de modo que se puedan crear redes distribuidas sin depender de un punto central de conexión (punto de acceso), permitiendo así la comunicación entre todos los nodos de la red sin tener cobertura entre los comunicantes, utilizando para ello el resto de nodos de la red.
595. La segunda topología es la denominada **infraestructura**, en la que existe un nodo central (punto de acceso) que sirve de enlace para todos los clientes. Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del punto de acceso y conocer los parámetros de la red.

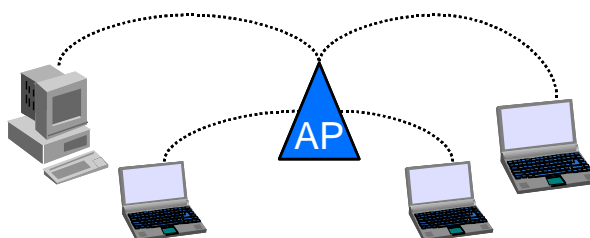


Figura 21.- Topología de red Infraestructura

#### 14.3.6. AMENAZAS Y RIESGOS PARA ESTÁNDAR 802.11

596. De forma resumida, se pueden entender los riesgos en las redes inalámbricas como la suma de todos los que afectan a una red cableada tradicional más aquellos nuevos introducidos por esta tecnología. Y como en la redes tradicionales, es imprescindible un continuo seguimiento de los nuevos desarrollos y vulnerabilidades que puedan ir apareciendo en el tiempo. En la siguiente lista se muestran los principales riesgos y amenazas que afectan a redes inalámbricas en la actualidad:

- a. Todas las vulnerabilidades que afectan a una red de cable convencional afectan a las redes inalámbricas.
- b. Puede obtenerse acceso a través de conexiones inalámbricas a otros servicios o entornos que, no siendo inalámbricos, estén conectados a éstos.
- c. La información que se transmite sin cables puede ser fácilmente interceptada incluso a kilómetros de distancia, sin posibilidad de detectar esta captura.
- d. Se pueden producir fácilmente ataques de denegación de servicio (DoS) contra este tipo de infraestructuras (perturbadores o inhibidores de señal, paquetes maliciosos, etc.).
- e. Se puede inyectar tráfico en las redes inalámbricas a gran distancia.
- f. Se pueden desplegar equipos falsos (*rogue AP*), para obtener información y realizar ataques tipo *Man in the Middle*.
- g. Se puede obtener información de conexión con sólo tener acceso a un equipo legítimo (claves guardadas en registro, ficheros, etc.).
- h. Se puede obtener acceso a Internet, utilizando las redes conectadas de terceros que no mantengan una política de seguridad adecuada.
- i. Se pueden realizar ataques internos desplegando redes inalámbricas no autorizadas.
- j. Se pueden realizar ataques desplegando redes inalámbricas con una seguridad deficiente, cuyo cometido real es conseguir que usuarios conecten con ella para capturar su tráfico.
- k. Se puede revelar información de la entidad propietaria en datos abiertos fácilmente capturables (SSID).

#### 14.3.7. ELEMENTOS DE SEGURIDAD

597. Desde la aparición de los primeros estándares en el ámbito de las redes inalámbricas se incluyeron elementos de seguridad en este tipo de infraestructuras. En este punto se expondrán las principales salvaguardas en las redes inalámbricas 802.11

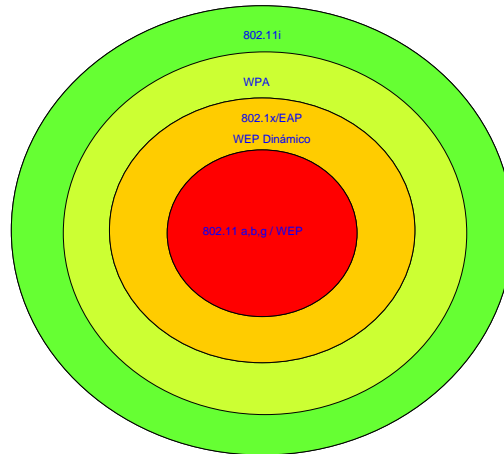
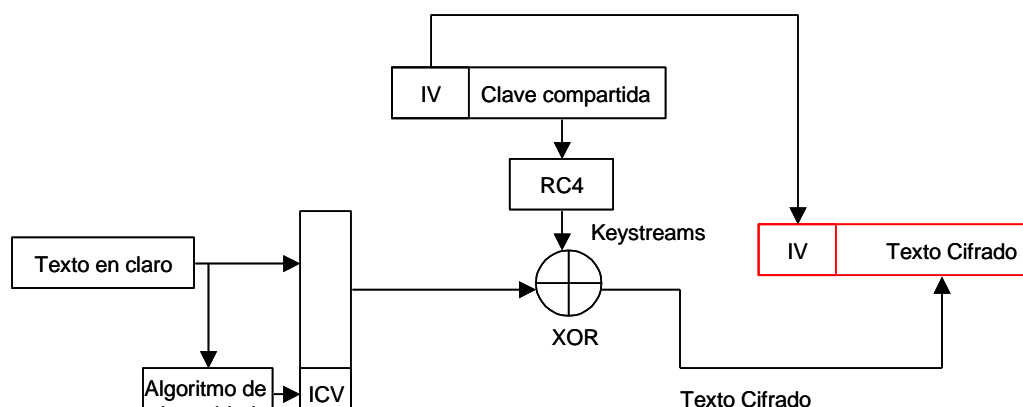


Figura 22.- Estándares y protocolos de seguridad para redes inalámbricas

#### 14.3.7.1. WEP

598. *Wired Equivalent Privacy* (WEP) es un protocolo que se diseñó para reforzar la seguridad del enlace de radio entre dispositivos en redes 802.11. Utiliza el algoritmo de cifrado simétrico RC4 y claves compartidas en las primeras implementaciones de 64 bits, siendo más adelante ampliado el estándar a 128 bits. Sus objetivos son proteger la comunicación inalámbrica de capturas externas (**confidencialidad**), prevenir los accesos no autorizados a la red (**control de acceso**) y evitar la modificación de los mensajes transmitidos (**integridad de datos**).
599. Con WEP activado, los interfaces de red inalámbricos cifran cada trama 802.11 antes de cada transmisión y descifran las tramas 802.11 que reciben. Este cifrado se realiza utilizando una clave estática que debe insertarse en todos y cada uno de los dispositivos que se quieran conectar a la infraestructura.
600. Un elemento fundamental en la implementación del algoritmo RC4 en WEP son los Vectores de Inicialización (IV), cadenas de 24 bits que forman parte de la clave secreta WEP y que se envía en claro en cada paquete, reduciendo de esta forma la longitud efectiva de la clave. Además, incorpora un control de integridad basado en CRC.





**Figura 23.- Proceso de generación de un paquete WEP**

601. Las principales vulnerabilidades que presenta WEP se resumen en los siguientes puntos:

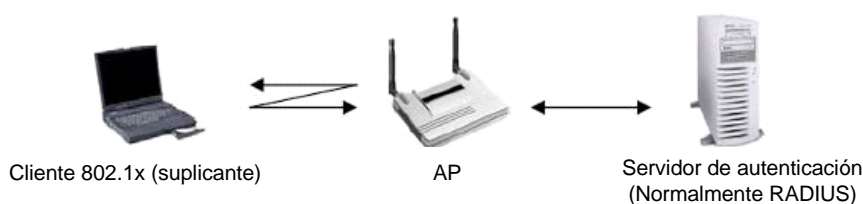
- a. Se utiliza una única clave para el acceso de todos los dispositivos (puntos de acceso y tarjetas de red) y no ofrece ningún mecanismo automático de renovación de claves, lo que hace que habitualmente éstas no se cambien nunca.
- b. CRC no depende del paquete completo, permitiendo inyectar tráfico en la red sin conocer la clave de cifrado.
- c. El vector de inicialización se agrega en las cabeceras de los paquetes y se envía en claro, lo que revela parte de la clave con la que está cifrado cada paquete, reduciendo la longitud efectiva de la clave y, de este modo, la efectividad del cifrado.
- d. Sólo hay  $2^{24}$  (16777,216) posibles valores de IV, por lo que en poco tiempo se reutilizan, lo que permite realizar ataques estadísticos contra la clave, obteniendo la contraseña establecida por cliente y punto de acceso.
- e. No se comprueba la identidad del generador de los paquetes, lo que permite que un usuario pueda inyectar en la red paquetes maliciosos.
- f. Es posible realizar ataques de diccionario y fuerza bruta. Un atacante con tan solo un único paquete de datos puede ejecutar reiteradas pruebas en busca de la clave compartida.
- g. El estándar es susceptible ataques de denegación de servicio. Este tipo de vulnerabilidad no está relacionada directamente con el protocolo WEP, es decir, no es una carencia de seguridad que haya sido aportada por la implementación de WEP, sino que es inherente al diseño e implementación del propio estándar 802.11.

602. Basándose en estas vulnerabilidades, se han desarrollado gran número de ataques a las infraestructuras inalámbricas protegidas con WEP. Los más sencillos, están basados en el acceso físico a equipos con claves WEP, ya que

los sistemas operativos de uso común y controladores de tarjetas almacenan las claves WEP sin cifrar en registros o ficheros de texto, con lo que teniendo acceso físico a un equipo configurado se tendrá acceso a la clave WEP que se esté utilizando. Pero estas acciones no son las que mayor riesgo entrañan, ya que debido a las deficiencias criptográficas del protocolo WEP es posible obtener la contraseña compartida para una red en escasos minutos y además de forma remota. Es por eso que, hoy en día, **nunca debe utilizarse este sistema de seguridad para proteger el acceso a una red inalámbrica WiFi.**

#### 14.3.7.2. WEP DINÁMICO

603. A partir de la aparición de las vulnerabilidades del protocolo WEP, la industria desarrolló una solución temporal que permitía resolver los problemas que éste presenta. La solución que se propuso está basada en el protocolo 802.1x., un estándar del IEEE (junio de 2001) para el control de acceso a red basado en puerto. Proporciona los medios para autenticar y autorizar a dispositivos conectados a un puerto físico (*switch*, AP inalámbrico, etc.).
604. Este protocolo trabaja en la capa de enlace de la pila OSI; está orientado a la conexión punto a punto entre dispositivos, definiendo únicamente un marco de autenticación y estando su desarrollo e implementación basada en el protocolo EAP (*Extensible Authentication Protocol*, definido en el RFC 2284). Define una arquitectura específica en la que se incluyen los siguientes elementos:
- a. Suplicante: elemento que solicita la autenticación al autenticador.
  - b. Autenticador: elemento al que el cliente se conecta y que pasa la información de autenticación al servidor de autenticación (*switch* o punto de acceso inalámbrico).
  - c. Servidor de Autenticación: elemento que realiza el proceso de autenticación, recibiendo las solicitudes por parte del autenticador y devolviendo a éste las respuestas positivas o negativas (servidor RADIUS).



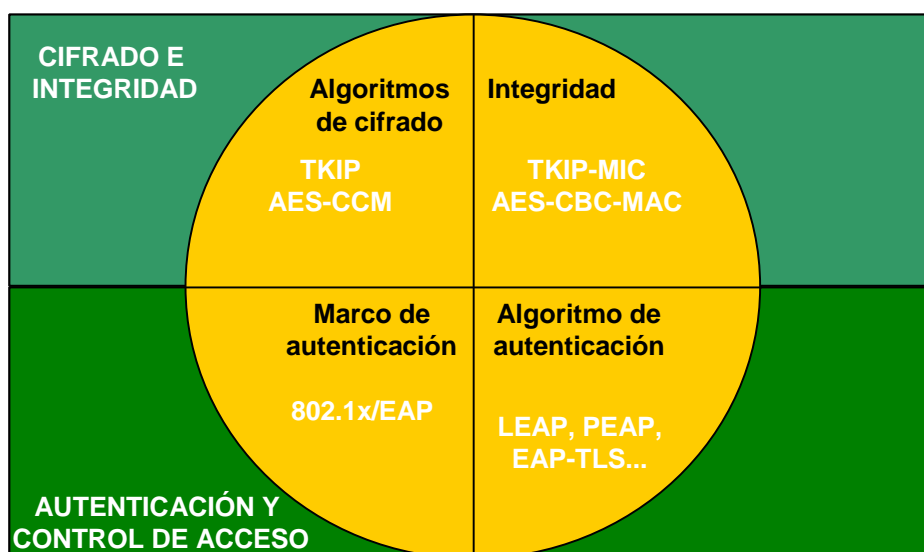
**Figura 24.- Autenticación mediante WEP dinámico**

605. EAP es el protocolo de autenticación sobre el que se ha definido 802.1x. Se desarrolló en el ámbito de las conexiones PPP y acceso telefónico remoto, permitiendo transportar diferentes protocolos de autenticación como *Transport Layer Security* (TLS) o *Tunnel Transport Layer Security* (TTLS). La especificación de EAP no define cómo se realiza el transporte de los mensajes, por lo que en el estándar 802.1x se define el protocolo EAPOL (*EAP over LAN*), que describe cómo se transportan los mensajes sobre Ethernet (IEEE 802.3).

606. Una de las deficiencias en WEP es el hecho de que no implementa ningún procedimiento de autenticación con garantías; para ello en WEP dinámico se definió el uso de protocolos en capas OSI superiores, como EAP-LEAP, EAP-MD5, EAP-PEAP, EAP-TLS, EAP-TTLS y EAP-SIM. Actualmente, se reconoce EAP-TLS como el método más seguro. Está basado en el hecho de que tanto el cliente como el servidor poseen certificados digitales X.509, ya que son éstos los que se utilizan en el proceso de autenticación mutua. El método EAP-TTLS está basado en el uso por parte de los clientes de contraseñas, utilizando certificados digitales únicamente en los servidores, evitando de este modo el despliegue de infraestructuras de clave pública.
607. Con WEP dinámico se resuelven los problemas de autenticación en la red y parcialmente la confidencialidad al realizar cambios de clave, aunque se siga utilizando WEP como protocolo de cifrado. Lo que no se resuelve es la posibilidad de inyectar tráfico en la red ni la reutilización de vectores de inicialización.

#### 14.3.7.3. WPA - 802.11i (WPA2)

608. WPA (*WiFi Protected Access*) se publicó como un subconjunto de 802.11i (conocido también como WPA2), definiendo nuevos estándares para la autenticación, cifrado e integridad de los mensajes en las comunicaciones en redes inalámbricas. WPA define dos modos de trabajo: WPA-PSK (*Pre-Shared Key*) y WPA-ENTERPRISE. El primero de ellos está pensado para su empleo por parte de usuarios domésticos, compartiendo una clave estática entre los dispositivos y eliminando la necesidad de implementar un servidor de autenticación externo (RADIUS), realizando dicha autenticación el propio punto de acceso inalámbrico. Por el contrario, WPA-ENTERPRISE está basado en el uso del protocolo 802.1x ya explicado anteriormente (suplicante, autenticador y servidor de autenticación).
609. El proceso de gestión y creación de claves es prácticamente el mismo para TKIP y AES-CCMP, los dos estándares definidos en 802.11i. La única diferencia está en el número de claves necesarias, ya que AES-CCMP combina los procesos de cifrado e integridad. En relación a los algoritmos de cifra, TKIP continua utilizando RC4, mientras que AES-CCMP utiliza AES (*Advanced Encryption Standard*); TKIP se ha mantenido dentro del estándar para dar cobertura a los dispositivos ya implantados, debido a que el uso de AES requiere hardware específico.
610. Además de los algoritmos de autenticación y cifrado, otra de las características que se han incluido tanto en WPA como en 802.11i es un mensaje de control de integridad (MIC). Dentro de TKIP es conocido como *Michael* y en el caso de 802.11i es AES-CBC, de forma que se garantice la integridad de los paquetes transmitidos y recibidos.
611. Es aceptado que la combinación de la autenticación 802.1x y AES-CCMP aportan una **solución de seguridad robusta para entornos inalámbricos**. La confidencialidad de los datos está garantizada por AES-CCMP, mientras que la integridad está garantizada por la implementación de MIC. Para casos de implementaciones sencillas en las que se necesite emplear hardware ya desplegado, se puede considerar el uso de 802.1x y TKIP (WPA).



**Figura 25.- Protocolos utilizados en WPA y WPA2**

#### 14.3.8. INFRAESTRUCTURA RECOMENDADA

612. Antes de implantar una infraestructura inalámbrica, deben analizarse detenidamente los servicios que se implantarán y se ofrecerán a los usuarios, así como los casos de uso que se darán. Para controlar los riesgos que introducen las infraestructuras de redes inalámbricas, las Organizaciones deben implantar medidas dirigidas a contrarrestar las amenazas y vulnerabilidades específicas de éstas.
613. La combinación de medidas procedimentales y técnicas constituyen una solución efectiva para el control de los riesgos asociados con este tipo de redes. Asumiendo que es imposible eliminar todos los riesgos, ni conseguir un sistema seguro al cien por cien, la implantación por una Organización de las medidas descritas en este punto ayudará a conseguir un nivel de seguridad adecuado.

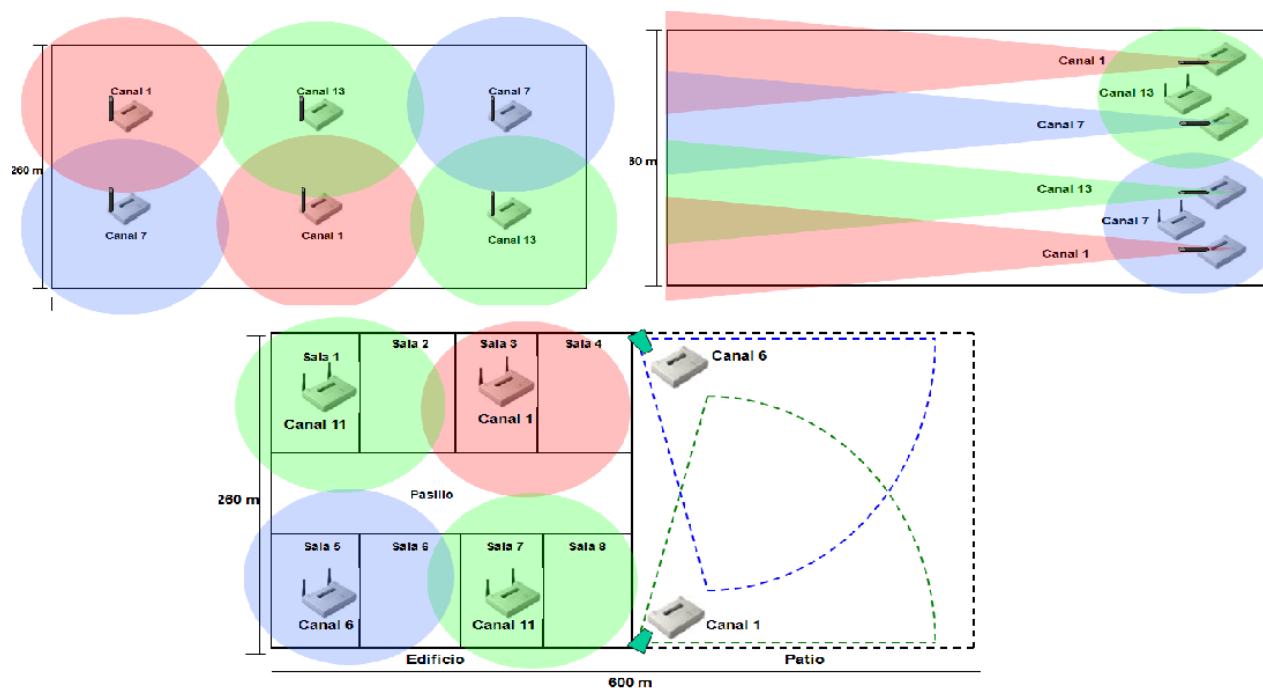
##### 14.3.8.1. MEDIDAS PROCEDIMENTALES

614. Las medidas procedimentales para el aseguramiento de redes inalámbricas deben comenzar por la definición de una política clara de despliegue y uso de la futura infraestructura. Esta política debe definirse a partir del análisis de riesgos correspondiente, que determinará las medidas técnicas a implementar. Es necesario identificar y contemplar al menos los siguientes aspectos:
- Identificación de los casos de uso de la tecnología inalámbrica en la Organización.
  - Identificación de los distintos tipos de accesos y servicios requeridos por los usuarios (LAN, WAN, Internet, correo electrónico, etc.).
  - Asignación de las responsabilidades sobre el despliegue, instalación y operación de la infraestructura.

- d. Definición de las limitaciones sobre las ubicaciones físicas, tanto de puntos de acceso como de clientes dentro de la Organización.
- e. Definición del tipo de información que podrá circular por la infraestructura.
- f. Definición de los estándares mínimos de seguridad y configuraciones a utilizar.
- g. Definición de los procedimientos de respuesta frente a pérdidas o robo de equipos inalámbricos.
- h. Definición de procedimientos para la gestión de claves en la infraestructura.
- i. Definición de procedimientos para la gestión de incidentes.
- j. Definición de procedimientos y periodicidad de análisis de seguridad de la infraestructura.
- k. Adicionalmente, la Organización debe asegurarse que todos los usuarios y personal técnico que vayan a utilizar o administrar este tipo de infraestructuras reciben la formación adecuada y son conocedores de la política de uso.
- l. Se debe definir y establecer una política de contraseñas adecuada que permita reducir los riesgos de seguridad y que determine caducidad, periodicidad de cambio, complejidad del alfabeto de entrada, longitud y almacenamiento de las claves.
- m. Se debe prestar especial atención en la definición de procedimientos para la gestión de de las llamadas “redes de cortesía” o WiFi públicas, aquellas destinadas a invitados al margen de la Organización pero gestionadas por ésta. Deben estar contempladas en rangos de red aislados o incluso totalmente al margen de la infraestructura de la Organización, evitando de esta manera la propagación de un atacante que pudiera haber comprometido la seguridad de una red de cortesía.

#### 14.3.8.2. MEDIDAS TÉCNICAS

615. Los aspectos de seguridad física son los primeros que se debe plantear una Organización a la hora de implantar una red inalámbrica, con el objetivo de que sólo aquel personal autorizado disponga de acceso físico a los elementos principales de la red, como pueden ser los puntos de acceso: mediante un acceso físico un posible atacante podría desconectar el acceso a la red cableada del dispositivo y utilizarla para obtener acceso al segmento interno de la Organización. Además, es importante considerar la cobertura de los puntos de acceso a la hora de ubicarlos físicamente, con el objetivo de minimizar la radiación de éstos fuera del perímetro controlado de la Organización y por tanto las posibilidades de captura de la señal; para ello, también se pueden utilizar las funcionalidades que incluyen algunos puntos de acceso para controlar la potencia de sus antenas. La siguiente figura ilustra algunas recomendaciones en cuanto a la arquitectura del despliegue:



**Figura 26.- Arquitectura de despliegue WiFi**

616. Esto debe considerarse también a la hora de establecer puentes entre puntos de acceso lejanos, por ejemplo para conectar diferentes edificios. En este caso, debe intentarse utilizar antenas direccionales, con el objeto de minimizar la dispersión de la radiación, tal y como muestra la ilustración anterior.
617. La Organización, a partir de lo indicado en la política de seguridad, debe realizar periódicamente análisis de vulnerabilidades, teniendo en cuenta en éstos, además del análisis de las medidas técnicas implantadas, el rango de cobertura de los puntos de acceso de su red. Se debe considerar que estas medidas sólo evitan la detección de una red utilizando antenas de poca ganancia o de forma accidental. Un potencial atacante que utilice una antena de alta ganancia siempre podrá detectar la señal de una red inalámbrica, siendo entonces el único medio de protección la aplicación de medidas específicas entre las que se incluyen la adecuada configuración de los puntos de acceso (evitando especialmente las configuraciones por defecto de éstos), las actualizaciones del software tanto de los puntos de acceso como de los clientes inalámbricos, la implantación de mecanismos de autenticación, de sistemas de detección de intrusión, de mecanismos de cifrado, el uso de tarjetas inteligentes, VPNs, etc.

#### 14.3.8.3. CONFIGURACIÓN GENERAL DE LOS PUNTOS DE ACCESO

618. Los administradores de la red deben configurar los puntos de acceso de acuerdo a lo establecido en la política de seguridad de la Organización. Además de tener en cuenta la importancia de ubicar físicamente de forma segura los puntos de acceso, se deben eliminar los parámetros por defecto de éstos y configurar adecuadamente las contraseñas de administración, listas de control de acceso por MAC, mecanismos de cifrado, uso de protocolos de gestión, etc. En la

configuración de los puntos de acceso deben considerarse, siempre, al menos los siguientes aspectos:

- a. **Contraseñas de administración.** Se deben cambiar las contraseñas y los nombres de usuario que por defecto tienen los puntos de acceso para la administración de los mismos, utilizando contraseñas con los parámetros de robustez adecuados. Además de esto, en la medida de lo posible debe evitarse que se transmita en claro la contraseña en el proceso de autenticación, utilizando para ello protocolos adecuados como SSH o SSL. En aquellos casos en los que los requisitos de seguridad sean muy elevados deben utilizarse elementos de autenticación más complejos como contraseñas de un sólo uso (OTP, *one-time passwords*) o tarjetas inteligentes con certificados digitales.
- b. **Mecanismos de cifrado.** Los servicios de seguridad propios de las redes inalámbricas se configuran en los puntos de acceso. Los mecanismos a implantar deben estar basados en el estándar 802.11i en la medida de lo posible, utilizando AES-CCMP y EAP-TLS como algoritmos y protocolos. En caso de imposibilidad de utilizar éstos, deben estudiarse detenidamente los protocolos a implantar y los riesgos que su uso introduce en la infraestructura. En cualquier caso, **no se debe considerar el uso de WEP estático** debido a la gran cantidad de vulnerabilidades que tiene este protocolo.
- c. **Listas de Control de Acceso (ACL) por MAC.** La mayor parte de los puntos de acceso incluyen la funcionalidad de implementar este tipo de control de acceso a los clientes. Si bien la efectividad de esta medida por sí sola no es muy alta, debido a la facilidad de realizar suplantaciones de direcciones MAC, combinada con el resto de medidas de seguridad sí que debe considerarse efectiva, ya que introduce un grado más de dificultad a los posibles atacantes.
- d. **Cambio del ESSID.** El ESSID debe cambiarse periódicamente y no deben utilizarse ESSIDs en los que se incluya información útil para un potencial atacante (nombre de la Organización, ubicación de los puntos de acceso o de la red, etc.).
- e. **Ocultar el “broadcast” del ESSID.** La mayor parte de los puntos de acceso comerciales incluyen una funcionalidad para deshabilitar la transmisión de esas tramas, de forma que no se anuncie la existencia de los puntos de acceso en la red.
- f. **Uso de protocolos de gestión de red.** En caso de utilizar el protocolo de gestión de red SNMP, debe utilizarse SNMPv3, evitando las dos primeras versiones (SNMPv1 y SNMPv2), ya que no incluyen mecanismos robustos de autenticación. En caso de utilizar alguna de las dos primeras versiones, se deben conocer y aceptar los riesgos que su empleo introduce en la Organización.
- g. **Selección de los canales.** A la hora de desplegar la infraestructura, deben tenerse en cuenta los canales en los que ésta trabajará para evitar interferencias entre los dispositivos de la propia infraestructura y los de otras que puedan estar trabajando en las proximidades.



- h. **DHCP.** Con objeto de poder realizar un filtrado adecuado en otros elementos de seguridad de la red, como los cortafuegos, y mantener un control adecuado de los clientes que se conectan a la infraestructura, se debe evitar en la medida de lo posible el uso de servidores DHCP en la infraestructura propia, manteniendo direccionamiento estático en los clientes.

#### 14.3.8.4. ESCENARIO ESPECIAL DE DESPLIEGUE: RED WIFI DE CORTESIA

619. Una de las necesidades a las que se enfrentan las Organizaciones hoy en día es la de ofrecer servicios de conectividad a Internet de forma inalámbrica para personal ajeno a la entidad. Estas redes son las conocidas como de cortesía o de invitados y sus servicios deben mantenerse al margen de la red corporativa. Para ello, si la Organización requiere el despliegue de una de estas redes, se deben proveer servicios de acceso a Internet paralelos dedicados especialmente para tal uso, adoptando medidas de control como proxies o cortafuegos. A su vez, se deberá aplicar una correcta política de seguridad sobre los dispositivos que soportan la red, tal y como se indica en puntos anteriores. Por lo que respecta a las medidas técnicas se deberán aplicar al menos las siguientes configuraciones de seguridad:
- a. Estándar de seguridad: se debe utilizar WPA2 (802.11i), el cual a día de hoy no presenta vulnerabilidades de seguridad críticas.
  - b. Sistema de cifrado: se debe aplicar el sistema cifrado en bloques AES-CCMP, el cual provee confidencialidad de la información, autenticación y control de acceso.
  - c. Filtrado: se debe aplicar un sistema de filtrado de lista blanca basado en la MAC del usuario.
  - d. Nombre ESSID: se debe establecer un nombre de la red que no induzca a relacionar la Organización con el destino asignado.
  - e. Emisión del ESSID: se debe eliminar la emisión del ESSID ocultando el nombre de la red; pese a que esta salvaguarda no introduce grandes barreras de seguridad para un atacante, sí que cualquier medida de protección que exista debe ser aplicada.
  - f. Clave compartida: en el caso de utilizar un sistema de clave compartida se establecerá utilizar una contraseña con al menos 10 caracteres alfanuméricos (mayúsculas y minúsculas), intercalando algún carácter especial como signos de puntuación, exclamaciones, etc.
620. En el caso de despliegues con arquitecturas distribuidas más complejas se deberá utilizar un sistema 802.1x EAP-TLS, donde los activos encargados de la autenticación y soporte de la red permanecerán al margen de la red privada de la Organización.

#### 14.4. BLUETOOTH

621. Bluetooth es un protocolo inalámbrico que representa un estándar de comunicaciones de redes personales (WPAN) capaz de transmitir de forma inalámbrica información (voz y datos) entre diferentes terminales, haciendo uso

de enlaces de radiofrecuencia móviles o estáticos. Este tipo de tecnología está ampliamente distribuida e incluida en los diferentes activos de las Organizaciones, así como en dispositivos comúnmente utilizados por los usuarios (ordenadores personales, tabletas, teléfonos inteligentes, puntos de información, etc.). Como cualquier tecnología, aporta ventajas y riesgos que la Organización debe considerar para no introducir vulnerabilidades en la seguridad corporativa.

#### 14.4.1. PROPIEDADES DEL ESPECTRO ELECTROMAGNETICO

622. Esta especificación industrial trabaja en la banda de los 2,4-2,48 GHz, dentro del rango ISM comentado con anterioridad. Con el propósito de evitar interferencias e implementar medidas de seguridad desde las primeras capas del modelo OSI (capa física), Bluetooth implementa la técnica de salto en frecuencias FHSS (*Frequency Hopping Spread Spectrum*), dividiendo la banda de comunicación en 79 canales (23 para el territorio nacional), de 1 MHz cada uno, realizando 1.600 saltos por segundo. Este modo de funcionamiento dificulta la implementación de *sniffers* de red y por lo tanto las escuchas de posibles atacantes, ya que la frecuencia de transmisión no se realiza por un único canal, como es el caso de 802.11.

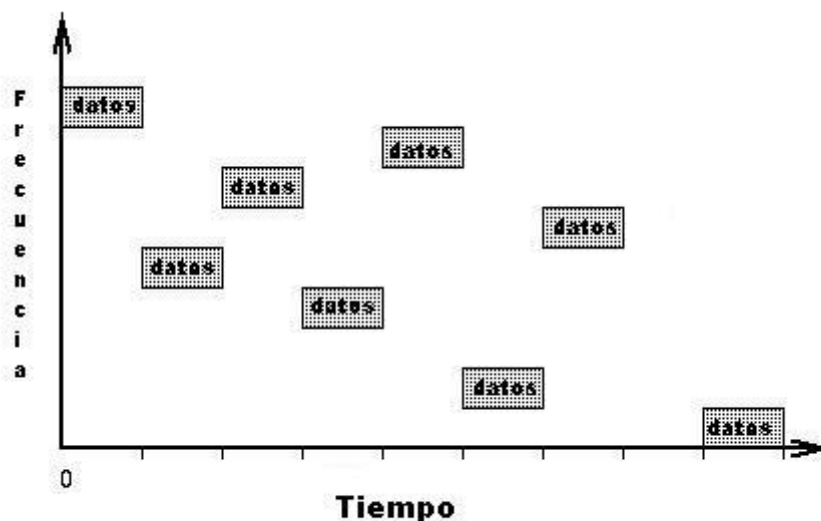


Figura 27.- Modulación FHSS

623. Por lo que respecta a su ancho de banda, éste no es excesivamente alto dado que el objetivo perseguido es el intercambio de voz y datos mediante una conectividad de corto alcance. Desde la primera especificación, este se ha visto aumentado significativamente hasta obtener 24Mbit/s en su versión 4.0. En la tabla siguiente se muestran los anchos de banda de las diferentes versiones del estándar:

Versión	Ancho de banda
1.2	1Mbit/s

2.0 + EDR	3Mbit/s
3.0 + HS	24Mbit/s
4.0	24Mbit/s

#### 14.4.2. ESPECIFICACIONES BLUETOOTH

624. La compañía de telecomunicaciones Ericsson comienza a estudiar en 1994 la posibilidad de habilitar en los terminales móviles capacidades de transmisión de datos y voz en un radio de corto alcance. El estudio formaba parte de un proyecto de mayor envergadura, destinado a dotar de acceso a la red GSM a otros dispositivos a través de los terminales móviles. En breve se identificaron las diferentes aplicaciones que podría llegar a ofrecer esta nueva tecnología, por lo que varias compañías se unieron al proyecto creando la primera especificación (versión 1.0) en julio de 1999. A continuación se presenta una breve descripción de su evolución.

- a. Versión 1.0/1.0b (1999). Primera versión de la especificación con numerosos problemas, lo que fuerza su revisión.
- b. Versión 1.1 (2002). IEEE crea el estándar IEEE 802.15.1-2002 basado en esta versión, corrigiendo los errores de versiones anteriores e incorporando entre otras cosas el indicador de calidad de señal (RSSI). Establece la especificación de capa física y de enlace.
- c. Versión 1.2 (2003). Incluye numerosas mejoras como el descubrimiento de dispositivos, incremento de la resistencia ante interferencias y aumento de la velocidad de transmisión.
- d. Versión 2.0 EDR (2004). Mejora la velocidad de transmisión mediante la incorporación de EDR (*Enhanced Data Rate*), alcanzando los 2.1 Mbit/s reales.
- e. Versión 2.1 EDR (2007). Incluye mejoras de seguridad en el proceso de emparejamiento de dispositivos y permite además reducir el consumo de energía de los dispositivos.
- f. Versión 3.0 HS (2009). Alcanza velocidades de 24 Mbit/s haciendo uso del estándar 802.11 como apoyo en la transmisión de datos, dejando la negociación inicial a la especificación v3.0.
- g. Versión 4.0 (2010). Incluye capacidades de alta velocidad y bajo consumo a un coste reducido, manteniendo las funcionalidades de la implementación clásica de las primeras versiones de Bluetooth, utilizando nuevamente en 802.11.

#### 14.4.3. DISPOSITIVOS

625. La especificación Bluetooth permite comunicar dispositivos de diversos fabricantes y propósitos siempre y cuando cumplan los requerimientos del estándar. A continuación se muestran algunos ejemplos de esta tecnología utilizada ampliamente en dispositivos de audio (manos libres o altavoces), sistemas integrados para la automoción, ordenadores personales, teléfonos

inteligentes, ordenadores personales, puntos de acceso, cámaras de video/fotografía, etc.



Figura 28.- Distintos dispositivos Bluetooth

#### 14.4.4. TOPOLOGIA DE RED

626. Los dispositivos Bluetooth son capaces de descubrirse entre sí mediante funciones de rastreo. Cuando un elemento bajo la norma 802.15 quiere iniciar una comunicación, bien sea para intercambiar archivos, remitir sus coordenadas GPS, transmitir música o la propia voz humana, éste realiza un proceso de emparejamiento de seguridad previo detallado más adelante en esta misma guía. Una vez concluido, permite establecer lo que se denomina una **picored**, la cual puede estar formada por hasta ocho dispositivos diferentes comunicándose de forma conjunta y donde un elemento realiza las funciones de “maestro”, encargado de gestionar la comunicación mediante la programación de los saltos de frecuencia y el reloj de sincronía. Destacar que un “maestro” puede a su vez comportarse como “esclavo” en otra picored, formando lo que se denomina una **red dispersa**. La siguiente ilustración muestra de forma resumida la topología y los elementos que forman una red basada en la especificación Bluetooth.

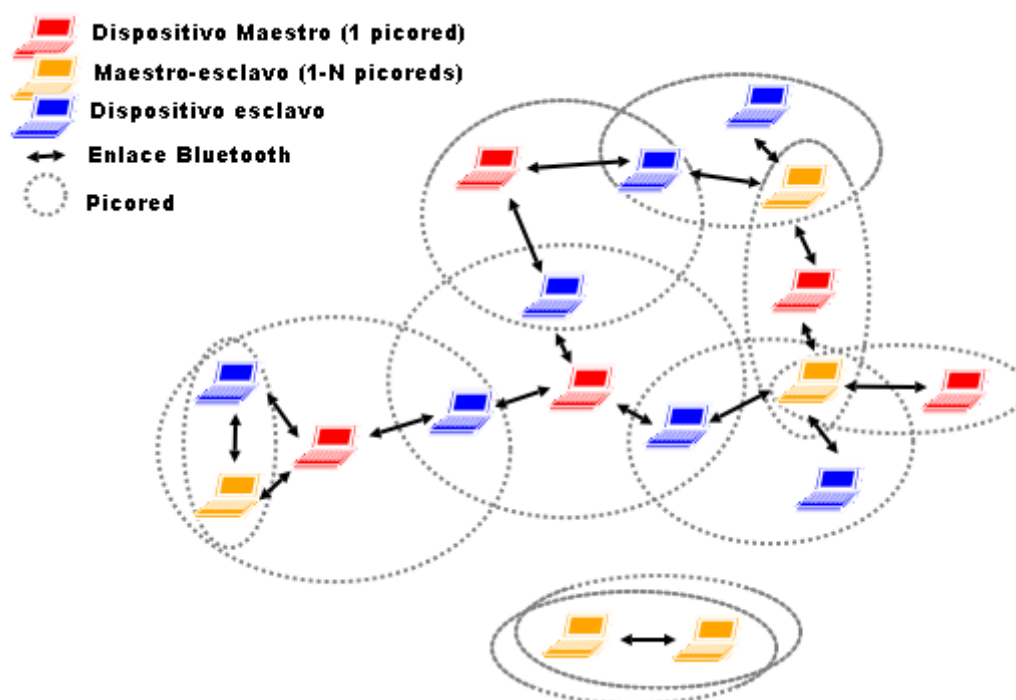


Figura 29.- Topología de red Bluetooth

627. Cada picored gestiona su propio esquema de salto de frecuencias y se sincroniza con un reloj único, pero gracias a la multiplexación por división de tiempo (TDM), un dispositivo puede participar en más de una picored al mismo tiempo.

#### 14.4.5. ELEMENTOS DE SEGURIDAD

628. La especificación Bluetooth establece varias medidas de seguridad desde las primeras capas del modelo OSI, elementos no presentes en el estándar 802.11. Par el nivel 1 o capa física se establece una **modulación de salto en frecuencia**, la cual utiliza un ancho de banda de 1 Mhz dentro de un conjunto de bandas base preestablecidas por el dispositivo maestro; de esta manera cuando un esclavo se conecta a la picored, éste recibe por un canal preestablecido la tabla de frecuencias aleatorias generadas para esa red. A continuación recibe un paquete de sincronización FHS, encargado de corregir las posibles desviaciones de sincronismo entre el maestro y el esclavo; esta información es remitida periódicamente para mantener la comunicación establecida de forma correcta. Por lo tanto cada dispositivo sabrá cuándo y en qué canal escuchar o transmitir en un momento dado; esto supuso un impedimento inicial para la sencilla implementación de *sniffers* de red de bajo coste. Pero dado que el intercambio de la tabla de frecuencias se realiza por un canal determinado, un atacante podría capturarla y sincronizar su dispositivo Bluetooth para capturar el tráfico de la picored, por lo que esta medida de seguridad por sí sola no es suficiente, incorporando mayores capacidades de seguridad en capas superiores.
629. Así, a nivel de la capa de enlace se definen tres mecanismos de seguridad: autenticación, autorización y cifrado de la información.

- a. **Autenticación.** Cada par de dispositivos Bluetooth almacenan una clave de 128 bits compartida previamente entre maestro y esclavo; esta clave permite verificar la identidad de los elementos que forman parte de la comunicación. La primera vez que se inicia un proceso de autenticación entre dos dispositivos, éstos deben realizar un proceso de emparejamiento donde establecen la clave común comentada anteriormente. Al confirmar ambos el código de seguridad, éste ya no es necesario que sea introducido en sucesivas transferencias.
- b. **Autorización.** Para poder determinar a qué servicios e información puede un dispositivo Bluetooth acceder se establecen tres niveles de confianza. Cuando un terminal establece una relación de **confianza total**, éste puede acceder al conjunto de servicios ofrecidos sin restricciones. En segundo lugar se encontraría la **relación parcial**, donde se mantiene el emparejamiento pero sólo se puede acceder a ciertos servicios. Por último un dispositivo **no confiable**, pese a poder mantener el emparejamiento, es posible que presente un grado de confianza nulo, negándole el acceso a cualquier servicio. Para mantener la información de autorización cada dispositivo presenta una pequeña base de datos donde se recopila los siguientes datos.

Campo	Estado	Contenido
BD_ADDR	Obligatorio	Dirección MAC
Nivel de confianza	Obligatorio	Nivel
Clave de enlace	Obligatorio	Clave criptográfica
Nombre	Opcional	Nombre del dispositivo

- c. **Cifrado.** Para garantizar la confidencialidad de la información transmitida entre dispositivos, Bluetooth presenta capacidades de cifrado de forma opcional. Destacar que para que maestro y esclavo puedan negociar el sistema de cifrado es necesario que se produzca una autenticación previa; si ésta se realiza de forma satisfactoria el maestro generará una clave de cifrado utilizando como parámetros de entrada al algoritmo E3, la clave de enlace, un número aleatorio de 128 bits y el parámetro COF (*Ciphering Offset*) derivado del proceso de autenticación. Como salida se obtiene una clave de cifrado de 128 bits apta para cifrar el contenido de la comunicación entre los interlocutores, pero no las cabeceras de los paquetes, tal y como ocurre en el estándar IEEE 802.11.

#### 14.4.6. AMENAZAS Y RIESGOS

630. Desde su creación en 1999 Bluetooth ha ido incorporando progresivamente mejoras de seguridad y mitigando su exposición a ataques. No obstante dependiendo de la versión de la especificación y de las medidas de seguridad aplicadas por el usuario y el fabricante es posible que el riesgo varíe. A continuación se describen algunas de las amenazas identificadas hasta el momento.
  - a. Es posible remitir mensajes no solicitados a dispositivos Bluetooth abusando del protocolo de emparejamiento. Para ello se aprovecha el



campo de datos de 248 caracteres donde se especifica el nombre del terminal que realiza la conexión.

- b. Es posible modificar el contenido del paquete de datos cuando no se han activado las funciones de cifrado. Para ello tan solo es necesario realizar una corrección sobre el valor del CRC.
- c. Es posible trazar o realizar un seguimiento de un objeto o persona si se irradia el nombre del dispositivo de forma continuada, siempre y cuando se habilite el dispositivo para que realice esta función. De esta manera un atacante podría colocar diferentes balizas Bluetooth encargadas de trazar el movimiento de un objetivo en concreto.
- d. Algunas implementaciones de la especificación son susceptibles a ataques de denegación de servicio (DoS), como por ejemplo modelos antiguos de terminales móviles a través de mensajes OBEX. También se han documentado ataques de DoS a dispositivos durante el proceso de emparejamiento, aprovechando los intervalos entre autenticaciones.
- e. Es posible realizar ataques de fuerza bruta sobre la BD\_ADDR (dirección MAC) cuando un terminal está configurado en modo oculto. El objetivo del ataque es identificar el dispositivo para realizar acciones posteriores.
- f. Es posible en algunos dispositivos Bluetooth realizar un robo de las claves de los dispositivos emparejados previamente. Esta amenaza requiere de acceso físico al terminal del objetivo.
- g. Es posible realizar capturas de la información que circula entre dos dispositivos Bluetooth a través de *sniffers* de red, capturando el intercambio de frecuencias inicial. Actualmente existen implementaciones de bajo coste de estos dispositivos intercambiando el firmware del fabricante por uno especialmente modificado.
- h. Algunos dispositivos son susceptibles a revelar información del terminal, detallando por ejemplo el fabricante del producto, modelo, número de serie, etc. Esta información puede ser utilizada para realizar posteriores ataques sobre vulnerabilidades concretas que afecten a esa versión de terminal.
- i. En algunas implementaciones de la especificación realizadas sobre diferentes modelos de teléfonos móviles es posible robar datos del terminal, como por ejemplo la agenda o los mensajes a través de comandos OBEX GET carentes de autenticación y autorización.
- j. Es posible que en modelos antiguos de teléfonos móviles un atacante pueda ejecutar comandos AT, obteniendo la posibilidad de realizar llamadas, gestionar la agenda o manejar los mensajes SMS. Esto es posible a causa de un uso indebido de la capa RFCOMM, la cual tiene acceso a la ejecución del juego de comandos AT.
- k. Es posible realizar ataques de suplantación de dispositivos a través de la modificación de la dirección MAC, accediendo a servicios que requieren autorización y autenticación.



- l. Ciertos fabricantes incorporan claves PIN por defecto en sus terminales, como por ejemplo los sistemas de manos libres o las pasarelas de audio; estas claves son conocidas a través de sus manuales de usuario o en recopilaciones que pueden encontrarse en Internet. Un atacante puede de esta manera emparejarse con el dispositivo, permitiéndole capturar el audio del micrófono o inyectar sonidos a través de los auriculares del objetivo.
- m. Se pueden desplegar equipos falsos, *rogue Bluetooth AP*, para obtener información y realizar ataques de tipo *Man in the Middle*.

#### 14.4.7. INFRAESTRUCTURA RECOMENDADA

631. Antes de adquirir y distribuir equipamiento con capacidades inalámbricas Bluetooth, deben analizarse detenidamente los servicios que se habilitarán, así como los casos de uso y abuso que son posibles en la Organización. Para controlar los riesgos que introducen estos dispositivos inalámbricos, las Organizaciones deben implantar medidas dirigidas a contrarrestar las amenazas y vulnerabilidades específicas de Bluetooth, unidas a las consideraciones generales de seguridad y a las concretas de redes inalámbricas.
632. La combinación de medidas procedimentales y técnicas constituye una solución efectiva para el control de los riesgos asociados con este tipo de tecnologías. Asumiendo que es imposible eliminar todos los riesgos, ni conseguir sistemas seguros al cien por cien, la implantación de estas medidas por una Organización ayudará a conseguir un nivel de seguridad adecuado.

##### 14.4.7.1. MEDIDAS PROCEDIMENTALES

633. Las medidas procedimentales para el aseguramiento de los dispositivos con capacidades Bluetooth deben comenzar por la definición de una política clara de despliegue y uso de los terminales. Esta política debe definirse a partir del análisis de riesgos correspondiente, que determinará las medidas técnicas a implementar. Destacar que estas medidas procedimentales deben formar parte de la política de gestión y control de dispositivos móviles; muchos de los procedimientos aplicables pueden heredarse de la política de seguridad WiFi y deben contemplarse al menos los siguientes:
  - a. Identificación de los casos de uso de la tecnología inalámbrica en la Organización.
  - b. Identificación de los distintos tipos de accesos y servicios requeridos por los usuarios (intercambio de ficheros, acceso a servicios de manos libres, etc.)
  - c. Asignación de las responsabilidades sobre el despliegue e instalación de los dispositivos.
  - d. En el caso de realizarse un despliegue de puntos de acceso Bluetooth se deberán definir las limitaciones sobre las ubicaciones físicas, tanto de puntos de acceso como de usuarios.
  - e. Identificación y restricciones de tratamiento del tipo de información que podrá intercambiarse.

- f. Definición de los estándares mínimos de seguridad y configuraciones a utilizar en los terminales.
- g. Definición de los procedimientos de respuesta frente a pérdidas o robo de equipos con capacidades Bluetooth.
- h. Definición de procedimientos para la gestión de claves en la infraestructura.
- i. Definición de procedimientos para la gestión de incidentes.
- j. Definición de procedimientos y periodicidad de las auditorías que se realizarán sobre los terminales.

#### 14.4.7.2. MEDIDAS TÉCNICAS

634. Al margen de las medidas procedimentales es necesario establecer una serie de medidas técnicas que permitan reducir la probabilidad asociada de sufrir un incidente de seguridad a través de la tecnología Bluetooth. Estas medidas de carácter general deberán ser aplicadas, siempre y cuando el dispositivo lo permita y deberán ser complementadas con las acciones y configuraciones específicas que cada fabricante provea. Se deben contemplar al menos las siguientes salvaguardas:

- a. Mantener activado el servicio Bluetooth del terminal sólo cuando se esté utilizando, manteniéndolo deshabilitado cuando no se requiera.
- b. Establecer una configuración de visibilidad del dispositivo en modo “oculto”, impidiendo que otros terminales puedan observarlo o descubrirlo en su radio de cobertura.
- c. Mantener una configuración de cifrado de la información transmitida habilitada en todo momento. De esta manera es posible mantener un alto grado de confidencialidad de los datos.
- d. No aceptar conexiones entrantes de terminales que no son conocidos por el usuario. Se debe tener precaución con los ataques de ingeniería social que pretendan emparejar el dispositivo, con el pretexto de remitir o recibir un simple archivo.
- e. Nunca se ha de utilizar un nombre del terminal que pueda ayudar a un atacante a identificar la marca, el modelo o el propietario (Organización o persona). Destacar que esta información suele estar configurada por defecto, por lo que se deberá modificar antes de que el dispositivo sea utilizado.
- f. Realizar una comprobación periódica de los dispositivos emparejados y eliminar aquellos que ya no sean necesarios.
- g. Establecer una correcta configuración de la autenticación de los perfiles soportados por el dispositivo, es decir, requerir que cualquier terminal que quiera utilizar un determinado servicio deba autenticarse primero. Este hecho es especialmente relevante ya que puede que ciertos perfiles de un terminal no establezcan autenticación por defecto.

## 15. HERRAMIENTAS DE SEGURIDAD

### 15.1. INTRODUCCIÓN

635. En el establecimiento de una Política de Seguridad de las TIC adecuada, la implementación y el uso de herramientas de seguridad puede proporcionar, de forma significativa, un valor añadido a la actitud general de seguridad de la Organización en lo referente a la protección de los Sistemas cuando éstos originan, modifican, almacenan o transmiten información.
636. Las herramientas de seguridad pueden describirse, en general, como productos hardware o software que proporcionan servicios que refuerzan la seguridad de los Sistemas, bien directamente desde un punto de vista técnico (cortafuegos, sistemas de detección de intrusos...) bien mejorando la gestión de la seguridad corporativa (SIEM, correlación...).
637. Las herramientas de seguridad deben implementarse de forma que proporcionen o apoyen a una o más de las siguientes capacidades funcionales:
- a. Gestión de la Seguridad. Herramientas de seguridad utilizadas para actividades de certificación y acreditación, como pueden ser análisis y gestión de riesgos, análisis de vulnerabilidades, detección de intrusiones, inspecciones periódicas o análisis de incidentes.
  - b. Administración de Seguridad. Herramientas de seguridad utilizadas para administración, como por ejemplo comprobaciones de configuración, comprobaciones de integridad, filtrado o supervisión de los recursos.
638. Las herramientas de seguridad deben permitir la configuración de reglas de autenticación y control de acceso granular, de manera que cada herramienta sólo pueda ser utilizada por los usuarios autorizados para ello, así como roles o grupos de usuarios con diferente nivel de privilegio a la hora de acceder a la herramienta, de manera que la información que ésta proporcione varíe en cada caso según los privilegios del usuario. Adicionalmente, las herramientas de seguridad deben ser capaces de elaborar informes en diversos formatos estándar (HTML, TXT, CSV...) y siguiendo distintos criterios (según el equipo, según la red, según el usuario...), facilitando así el intercambio de datos entre distintas herramientas y una interpretación correcta de la información obtenida.

### 15.2. CLASIFICACIÓN DE HERRAMIENTAS DE SEGURIDAD

639. Las herramientas de seguridad se pueden clasificar en las siguientes categorías:
- a. Antifraude.
  - b. Antimalware.
  - c. Auditoría técnica y forense.
  - d. Autenticación y certificación digital.
  - e. Contingencia y continuidad.
  - f. Control de contenidos.
  - g. Control de tráfico.

- h. Cortafuegos.
  - i. Cumplimiento legal y normativo.
  - j. Gestión de eventos.
  - k. Gestión y control de acceso e identidad.
  - l. Seguridad en movilidad.
  - m. Sistemas y herramientas criptográficas.
640. Analizando la clasificación anterior, y por motivos de claridad y operatividad para el objeto de la presente guía, sobre dicha clasificación se aplican las siguientes consideraciones:
- a. Las familias de Autenticación y certificación digital y Gestión y control de acceso e identidad se unen en una sola categoría denominada Identificación y autenticación.
  - b. La familia denominada Cortafuegos se incluye dentro de la categoría de control de tráfico de red por considerar a los cortafuegos elementos de control en este entorno.
  - c. Se elimina la categoría denominada Seguridad en movilidad por considerar que únicamente se referencia al tipo de plataforma sobre la que la herramienta opera o a la que protege, no al tipo de herramienta en sí.
641. Como resultado, en esta guía CCN-STIC **se propone el uso de la siguiente clasificación** para las herramientas de seguridad de la Organización:
- a. Antifraude.
  - b. Antimalware.
  - c. Auditoría técnica y forense.
  - d. Identificación y autenticación.
  - e. Contingencia y continuidad.
  - f. Control de contenidos.
  - g. Control y monitorización de tráfico.
  - h. Cumplimiento legal y normativo.
  - i. Gestión de eventos de seguridad.
  - j. Herramientas de cifra.
642. La relación anterior no pretende ser exhaustiva, aunque sí reflejar los principales tipos de herramientas de seguridad que se pueden encontrar actualmente. Es necesario indicar que, debido a la rápida evolución de la tecnología, los tipos y capacidades de las herramientas de seguridad aumentan cada día.

**Nota:** Existen multitud de dispositivos técnicos que a pesar de ofrecer un cierto grado de seguridad a los Sistemas, en el ámbito de la presente guía no se consideran herramientas de seguridad pura. Entran en esta categorización routers, proxies, generadores de registros o herramientas de monitorización de sistemas y redes, por poner sólo unos ejemplos.

643. Se resumen a continuación los aspectos más destacables de cada una de las familias definidas anteriormente.

#### 15.2.1. ANTIFRAUDE

644. Las herramientas antifraude protegen a los usuarios del Sistema de las amenazas asociadas al fraude, tanto ejecutado mediante ingeniería social (engaño a los usuarios) como ejecutado mediante ataques puramente técnicos. Se encuentran en esta familia de herramientas los productos antiphishing, antispam o las herramientas de navegación segura, por poner unos ejemplos
645. Las herramientas antifraude deben cumplir al menos las siguientes características:
- a. La herramienta en sí, debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. La herramienta debe permitir la parametrización, automática o manual, de su base de datos o esquema de detección.
  - c. Un responsable de seguridad del Sistema debe ser capaz de gestionar esta herramienta por medio de un sistema centralizado.
  - d. La herramienta debe permitir la detección de posibles fraudes (phishing, SPAM...) en tráficos provenientes de la red, en especial a través de correo electrónico.
  - e. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autoricen la capacidad de administración a los usuarios y/o componentes autorizados.
  - f. La herramienta debe ser capaz de elaborar informes en diversos formatos (html, txt, etc.) y siguiendo diversos criterios (origen, destinatario, sistema...), acordes con los requisitos de Seguridad y operación corporativos.

#### 15.2.2. ANTIMALWARE

646. Estas herramientas están destinadas a proteger un Sistema frente a software malicioso de cualquier tipo (virus, gusanos, troyanos...), comprendiendo de esta forma productos antivirus, *antispyware*, etc. En general las herramientas antimalware permiten analizar objetos del sistema o flujos de información (por ejemplo, tráfico web) para determinar si contienen algún tipo de software o código malicioso, como por ejemplo virus, gusanos o troyanos. Este análisis se realiza, bien bajo demanda, bien de forma automática en tiempo real, mediante diferentes técnicas:
- a. Escáner. La detección se realiza mediante una búsqueda de firmas, o patrones conocidos o mediante el empleo de algoritmos de detección.
  - b. Controles de Integridad. Se determina si el archivo original –considerado legítimo– ha sido modificado, proporcionando así la sospecha de una posible infección.

647. Las herramientas antimalware deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí, debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. El conjunto de patrones (firmas) de código malicioso utilizado por la herramienta debe ser actualizado regularmente (por ejemplo, una vez por semana) por el proveedor. No son admisibles periodos de actualización superiores a un mes.
  - c. Un responsable de seguridad del Sistema debe ser capaz de gestionar esta herramienta por medio de un sistema de gestión centralizado que incluya la distribución de actualizaciones de firmas a cada sistema de la red.
  - d. La herramienta debe permitir a cualquier usuario del Sistema analizar la presencia de código malicioso en cualquier archivo o directorio al que tenga derechos de acceso.
  - e. La herramienta debe permitir a cualquier usuario del Sistema analizar la presencia de código malicioso en los flujos de entrada al sistema, en especial tráfico proveniente de la red.
  - f. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autoricen la capacidad de administración a los usuarios y/o componentes autorizados.
  - g. La herramienta debe ser capaz de elaborar informes en diversos formatos (html, txt, etc.) y siguiendo diversos criterios (equipo, red, firma de código malicioso, etc.), acordes con los requisitos de Seguridad y operación corporativos.

### 15.2.3. AUDITORÍA TÉCNICA Y FORENSE

648. Estas herramientas proporcionan información sobre la desviación del estado de un objeto con respecto a un referencial (norma, estándar o conjunto de buenas prácticas comúnmente aceptado). La desviación puede identificar deficiencias en la configuración técnica del entorno, situaciones que se hayan materializado con un impacto para la Organización o, directamente, vulnerabilidades en el entorno operativo. De esta forma, las herramientas de auditoría permiten a la Organización identificar su estado de seguridad en un ámbito determinado y, a partir de éste, adoptar las medidas apropiadas para contrarrestar cualquier vulnerabilidad o debilidad en el entorno.
649. Dentro de esta familia de herramientas de seguridad se encuentran analizadores de vulnerabilidades, analizadores de puertos, herramientas de auditoría de contraseñas o herramientas de recuperación de datos, por poner sólo unos ejemplos. Estas herramientas deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. Si la herramienta utiliza bases de datos (por ejemplo, herramientas de auditoría de vulnerabilidades, de rotura de contraseñas...), éstas deben

ser actualizadas regularmente (por ejemplo, una vez cada tres meses) por el proveedor.

- c. La herramienta debe permitir a un responsable de seguridad del Sistema seleccionar o deseleccionar uno o más subconjuntos de objetos a auditar del conjunto total, para analizar de esta manera un determinado componente del Sistema.
- d. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso, de tal manera, que sólo permita su utilización a los usuarios y/o componentes autorizados.
- e. La herramienta o el sistema donde se ejecuta deben permitir la protección adecuada de los datos procesados en el análisis y de los informes generados a partir de éstos.
- f. La herramienta debe ser capaz de producir informes en diferentes formatos (txt, html, etc.) y siguiendo distintos criterios (equipos, red, vulnerabilidades, etc.), acordes con los requisitos de Seguridad y operación corporativos.

#### 15.2.4. IDENTIFICACIÓN Y AUTENTICACIÓN

650. Las herramientas de seguridad dentro de esta familia son aquellas que permiten a la Organización identificar a sus actores, autenticarlos en el Sistema y, a partir de ahí, autorizar sus acciones en el mismo. Se encuentran dentro de esta familia herramientas de *single sign on* (SSO), herramientas asociadas a la autenticación biométrica, gestores de identidades y roles o herramientas de control de acceso a la red corporativa.
651. La **identificación** es el proceso por el cual una entidad proporciona su identidad a un Sistema, mientras que la **autenticación** constituye el proceso por el cual se establece la validez de la identidad proporcionada por el Sistema. La identidad puede autenticarse por medio de los siguientes tipos de mecanismos:
- a. Algo que solo el usuario conoce (contraseña).
  - b. Algo que solo el usuario tiene (tarjeta, “token”, etc.).
  - c. Algo que solo el usuario es (huella dactilar, iris del ojo, etc.).
652. La **autenticación fuerte** viene determinada por la implementación simultánea de, al menos, dos (2) de los mecanismos citados previamente.
653. La **autorización** es el proceso mediante el cual se definen y se mantienen los privilegios sobre las acciones autorizadas en el Sistema. Los mecanismos de autorización pueden ser:
- a. Locales. La autorización se establece en cada aplicación o sistema al que se solicita el acceso.
  - b. Centrales. La autorización se establece de forma centralizada en un servidor, proporcionando el acceso a una cuenta de usuario.
  - c. *Single Sign On*. La autorización se establece de forma centralizada en un servidor, permitiendo a un usuario autenticarse una sola vez para acceder a diferentes dominios, equipos, aplicaciones, etc., que emplean diferentes



mecanismos de autenticación. En el servidor se almacenan los datos necesarios para realizar la autenticación en nombre del usuario ante los diferentes recursos para los que tiene derechos de acceso.

- d. *Single Log On*. Similar al anterior, con la salvedad de que todos los recursos emplean el mismo mecanismo de autenticación.

654. Las herramientas de identificación y autenticación deben presentar al menos las siguientes características:

- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
- b. La herramienta debe permitir una autenticación acorde a los requisitos de seguridad de la Organización.
- c. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso, de tal manera, que sólo permita su gestión a los usuarios y/o componentes autorizados.
- d. La herramienta debe ser capaz de producir informes en diferentes formatos (txt, html, etc.) y siguiendo distintos criterios (horarios, identificadores de usuario, objetos...) acordes con los requisitos de Seguridad y operación corporativos.

#### 15.2.5. CONTINGENCIA Y CONTINUIDAD

655. Las herramientas en esta categoría son aquellas cuyo objetivo es facilitar, técnica u organizativamente, la continuidad del servicio en la Organización. Se encuentran en esta familia herramientas de gestión de planes de contingencia y continuidad o herramientas de copias de seguridad.

656. Es necesario utilizar estas herramientas en cualquier Organización, con independencia de su tamaño o servicio, en especial en lo que respecta a copias de seguridad y recuperación de sistemas.

#### 15.2.6. CONTROL DE CONTENIDOS

657. Las herramientas de control de contenidos son aquellas que de forma directa tratan de evitar la fuga o el robo de los datos confidenciales de una Organización. Ejemplos de estas herramientas son las correspondientes a DLP (*Data Loss Prevention*) o los sistemas de control de dispositivos extraíbles. No se consideran en esta categoría las herramientas de filtrado de contenidos, que se ubican en la familia de control y monitorización de tráfico.

658. Las herramientas destinadas al control de contenidos deben tener, como mínimo, las siguientes características:

- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
- b. Si la herramienta utiliza bases de datos, éstas deben ser actualizadas regularmente (por ejemplo, una vez cada tres meses) por el proveedor.

- c. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso, de tal manera, que sólo permita su utilización a los usuarios y/o componentes autorizados.
- d. La herramienta debe ser capaz de producir informes en diferentes formatos (txt, html, etc.) y siguiendo distintos criterios (equipos, red, vulnerabilidades, etc.), acordes con los requisitos de Seguridad y operación corporativos.

#### 15.2.7. CONTROL Y MONITORIZACIÓN DE TRÁFICO

659. Las herramientas dentro de esta categoría son aquellas destinadas a la monitorización y control de las actividades en las infraestructuras de comunicaciones (voz o datos) de una Organización, con distintos objetivos: cumplimiento normativo, seguridad perimetral, uso adecuado de los recursos, etc. Se encuentran en esta familia herramientas de gestión y control de ancho de banda, cortafuegos, sistemas de detección o prevención de intrusiones y filtrado de contenidos.
660. Las herramientas de control y monitorización del tráfico de red deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. Si la herramienta trabaja con firmas (habitualmente, IDS, IPS, filtros de contenidos...), éstas deben ser actualizadas regularmente (por ejemplo, una vez al mes) por el proveedor.
  - c. La herramienta debe ser capaz de controlar y monitorizar el tráfico de red, en sus campos de datos y cabeceras para los protocolos de uso general en la Organización (habitualmente, ARP, RARP, ICMP, IGMP, TCP, UDP, FTP, Telnet, SMTP, DNS, HTTP, SNMP...).
  - d. La herramienta debe permitir a un responsable de seguridad del Sistema crear y aplicar filtros de monitorización o reglas de control para establecer qué tipos de tráfico de red deben tratarse.
  - e. Si la herramienta trabaja con firmas, debe permitir a un responsable de seguridad del Sistema editar cualquiera de las firmas para su personalización o definir nuevas.
  - f. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autoricen su uso a los usuarios y/o componentes autorizados.
  - g. La herramienta debe ser capaz de elaborar informes en diversos formatos (html, txt, etc.) y siguiendo diversos criterios (equipo, red, protocolo, etc.).

#### 15.2.8. CUMPLIMIENTO LEGAL Y NORMATIVO

661. Esta categoría aglutina las herramientas directamente destinadas a facilitar el cumplimiento legal y normativo en la Organización, posibilitando de esta forma la implementación de políticas de seguridad, la realización de análisis de riesgos,

la medida de eficacia y eficiencia de los controles implantados, entre otros. Así, existen herramientas que facilitan el cumplimiento de la LOPD, herramientas para la realización de análisis de riesgos (como PILAR) o herramientas que permiten la explotación de un SGSI.

662. Las herramientas destinadas al cumplimiento legal y normativo deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autoricen su uso a los usuarios y/o componentes autorizados.
  - c. La herramienta debe ser capaz de elaborar informes en diversos formatos (html, txt, etc.) y siguiendo diversos criterios (activo, tratamiento, usuario, etc.).

#### 15.2.9. GESTIÓN DE EVENTOS

663. Las herramientas de gestión de eventos permiten capturar, almacenar y analizar los eventos significativos de seguridad relacionados con el Sistema, proporcionando un flujo para dicha gestión y por tanto facilitando la implementación de los procedimientos operativos de gestión de eventos y alertas de seguridad. Entre ellas se encuentran los gestores de eventos puros, los correladores o los centralizadores de registros (logs) de diferentes dispositivos.
664. Actualmente las herramientas de gestión de eventos buscan centralizar los datos significativos de seguridad, a partir de múltiples fuentes, para procesarlos y extraer de ellos información valiosa para la toma de decisiones, permitiendo así a la Organización responder adecuadamente ante situaciones que puedan degradar la seguridad corporativa. Estas herramientas deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. La herramienta debe permitir recibir eventos significativos de diferentes componentes del Sistema.
  - c. La herramienta debe permitir a un responsable de seguridad del Sistema tratar los eventos más significativos para la seguridad y que necesitan ser recopilados.
  - d. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autorice su utilización a los usuarios y/o componentes autorizados.
  - e. La herramienta debe ser capaz de elaborar informes en diversos formatos (html, txt, etc.) siguiendo diversos criterios (equipo, red, registro de eventos, etc.).

#### 15.2.10. HERRAMIENTAS DE CIFRA

665. Estas herramientas proporcionan cifrado lógico o físico de la información manejada en el sistema, por ejemplo cifrado de correo o volúmenes cifrados para almacenamiento de información. Deben ser empleadas para proteger datos personales, información contenida en soportes extraíbles o información intercambiada entre usuarios y/o componentes autorizados.
666. Estas herramientas deben tener, como mínimo, las siguientes características:
- a. La herramienta en sí debe ser actualizada regularmente (por ejemplo, una vez al año) por el proveedor.
  - b. La herramienta debe permitir a un responsable de seguridad del Sistema configurar reglas de autenticación y acceso que sólo autoricen su empleo a los usuarios y/o componentes autorizados.
  - c. La herramienta debe disponer de controles de integridad que detecten su manipulación.
  - d. La herramienta debe disponer de certificación criptológica en función del grado de clasificación de la información que va a proteger. En esta certificación se especificarán las condiciones y limitaciones de utilización.

### 15.3. SELECCIÓN, CONTROL DE LA CONFIGURACIÓN Y USO

#### 15.3.1. SELECCIÓN

667. Como norma general, las herramientas de seguridad que se utilicen en los Sistemas deben ser **aprobadas** por la Autoridad responsable de la aplicación de la Política de Seguridad de las TIC de la Organización. Siempre que sea posible las herramientas de seguridad deberán haber superado, o estar en proceso de superar, una **evaluación funcional de seguridad** siguiendo un estándar reconocido como *Common Criteria* (CC), *Information Technology Security Evaluation Criteria* (ITSEC), *Trusted Computer System Evaluation Criteria* (TCSEC) o equivalente, o en su defecto ser aprobados por una Autoridad competente de acuerdo a la documentación del producto.
668. El nivel de certificación requerido debe determinarse en función del análisis de riesgos que se lleve a cabo en cada caso, aunque se recomienda, como mínimo, un nivel de garantía de evaluación EAL3 en la certificación CC. La aprobación de una herramienta de seguridad por parte de la Autoridad correspondiente, cuando no esté certificada o en proceso de certificación, debe basarse en un Plan de Evaluación y Pruebas de Seguridad aprobado por ésta y que identifique al menos los siguientes aspectos:
- a. Las ventajas que se obtienen al utilizar la herramienta, en términos de mitigación del riesgo.
  - b. Las vulnerabilidades derivadas de su uso, cuando sea el caso.
  - c. Las limitaciones de uso.
  - d. Los recursos, experiencia, apoyo y formación necesarios para su correcta explotación en la Organización.

669. Esta autorización dependerá de las condiciones de empleo, de la criticidad del Sistema y de la ausencia de este tipo de herramientas en el mercado con los requisitos de certificación establecidos.
670. Los criterios de selección indicados son aplicables a todas las herramientas de seguridad tratadas en el presente documento, excepto para las herramientas de cifrado software que pueden necesitar la certificación criptológica correspondiente, especialmente en el caso de emplearse para la protección de información clasificada. En cualquier caso, la Autoridad correspondiente debe ser responsable de aprobar la implementación de estas herramientas y, por tanto, de su comprobación periódica.

### 15.3.2. CONTROL DE LA CONFIGURACIÓN

671. El control respecto a la configuración de las herramientas de seguridad instaladas en un Sistema se debe llevar a cabo mediante los procedimientos aplicables, que deben especificar con claridad la configuración autorizada en cada Sistema.
672. En el caso de utilización temporal de este tipo de herramientas, la configuración de las mismas se debe realizar de acuerdo con la correspondiente documentación de seguridad aprobada.
673. La frecuencia de actualizaciones dependerá de la funcionalidad de la herramienta y debe reflejar los cambios de la tecnología asociada con la misma. Los requisitos de actualización se incluyen en la documentación de seguridad aprobada y deben ser acordados previamente con la Autoridad correspondiente.

### 15.3.3. USO OPERATIVO

674. Las herramientas de seguridad deben ser controladas y utilizadas según la documentación de seguridad aprobada para el Sistema. La Autoridad Operativa del Sistema, como responsable del mismo, debe garantizar que se implementan las actividades descritas a continuación, dependiendo de la categoría de la herramienta:
  - a. Control de la configuración y la gestión de la herramienta, incluido garantizar que sólo los usuarios autorizados tienen acceso a la misma.
  - b. Análisis y protección de los datos derivados del uso de la herramienta.
  - c. Clasificación de los datos y protección de los mismos contra la revelación, modificación o destrucción no autorizadas.
  - d. Identificación y resolución de las incidencias derivadas del uso de la herramienta.
  - e. Informe de incidentes a las Autoridades correspondientes, de acuerdo con lo establecido en los Procedimientos Operativos de Seguridad (POS) del Sistema.
675. Sólo el personal autorizado y especialmente designado para ello (por ejemplo, el equipo de respuesta a incidentes o el equipo de análisis de vulnerabilidades) debería poder utilizar herramientas de seguridad capaces de explotar

vulnerabilidades de seguridad. El uso de las herramientas de seguridad debe cumplir estrictamente con las leyes o normas aplicables en cada caso.

676. La información recopilada por las herramientas de seguridad debe protegerse y distribuirse siguiendo lo establecido en la documentación de seguridad aprobada.

#### **15.4. RESPONSABILIDADES**

677. En este apartado se recogen de forma genérica las distintas responsabilidades y funciones que se deben considerar durante el ciclo de vida de las herramientas de seguridad.

##### **15.4.1. PLANEAMIENTO Y ADQUISICIÓN**

678. Los organismos responsables del planeamiento y adquisición deben tener en cuenta:
- a. Los requisitos obligatorios a incluir en cualquier Pliego de Prescripciones Técnicas (PPT) como parte de los requisitos técnicos generales.
  - b. La especificación detallada, en la documentación de adquisición para cada PPT, de los requisitos de software y hardware de las herramientas de seguridad correspondientes.
  - c. Los recursos adicionales que se consideren necesarios para explotar adecuadamente las herramientas de seguridad (por ejemplo, horas-hombre para mantener las actividades de forma ininterrumpida, costes de implantación, etc.).

##### **15.4.2. AUTORIDAD RESPONSABLE DEL SISTEMA**

679. La Autoridad responsable del Sistema, como responsable de la implementación y uso de las herramientas de seguridad, debe garantizar en todo momento que:
- a. Los recursos asignados como herramientas de seguridad están implementados y se utilizan adecuadamente.
  - b. Se asignan fondos de operación y mantenimiento que aseguren la continuidad de las actividades basadas en herramientas de seguridad.
  - c. Las actividades basadas en herramientas de seguridad se realizan, y se da cuenta de ellas, según lo establecido en la documentación de seguridad aprobada.
  - d. El uso de las herramientas de seguridad aporta beneficios a la Organización en términos de mitigación del riesgo.
680. Con objeto de garantizar que se implementan las actividades relativas a las herramientas de seguridad, la Autoridad responsable del Sistema podrá designar a cuantos responsables de seguridad del Sistema estime oportuno.

##### **15.4.3. RESPONSABLES DE SEGURIDAD DEL SISTEMA**

681. Cuando la Autoridad responsable del Sistema delegue las funciones de seguridad del Sistema, el personal designado debe ser responsable del empleo y protección de la información generada por estas herramientas. Todas las actividades a realizar con estas herramientas deben estar detalladas en la documentación de seguridad del Sistema.



## V. ANEXOS

## ANEXO A. REFERENCIAS

- Caballero, Pino. *Introducción a la Criptografía*. RA-MA, 1996.
- CESID. *Glosario de términos de Criptología*. Centro Superior de Información de la Defensa, 1991.
- CCN. *Guía de seguridad de las TIC (CCN-STIC-400)*. Manual de Seguridad de las Tecnologías de la Información y Comunicaciones. Centro Nacional de Inteligencia, 2005.
- Diffie, W. y Hellman, M.E. *New directions in cryptography*. IEEE Transactions on Information Theory. IT-22, 644-654. 1976
- Schneier, B. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley & Sons. 1994
- Shannon, C.E. *Communication theory of secrecy systems*. Bell Systems Technology Journal, 28, 657—715. 1949.
- Villalón, A. *Analista de Sistemas de Información*. Cap. 55. Criptografía. COIICV, 2003.
- W. Richard Stevens. *TCP/IP Illustrated, Vol. 1: The Protocols*. Addison-Wesley Professional. 1994.
- Matthew G. Naugle. *Illustrated TCP/IP*. Wiley Computer Publishing, John Wiley & Sons, Inc. 1998.
- Mark A. Dye. *Aspectos básicos de networking*. Cisco Press. 2008.
- Arbaugh, W., Shankar, N., Wan, J. *Your 802.11 Wireless Network has No Clothes*. 2001.
- NIST. SP 800-94. *Guide to Intrusion Detection and Prevention Systems*. Febrero, 2007.
- Villalón, A. *Seguridad en Unix y Redes*. GNU Free Documentation License. 2002.
- Muller Nathan, J. *Tecnología Bluetooth*. McGraw-Hill, 2002
- Moreno, A. *Seguridad en Bluetooth*. Universidad Pontifica de Comillas, 2006
- Pellejero, I., Andreu, F., Lesta, A. *Redes WLAN, fundamentos y aplicaciones de seguridad*. Marcombo, 2006.
- Fluhrer, S., Mantin, I., Shamir, A. *Weakness in the Key Scheduling Algorithm of RC4*. 2004.
- Planas, A. *Criptoanálisis WEP*. Linux Magazine, 2005.
- Korek. *Choop Choop attack*. 2004
- IEEE Computer Society. *IEEE802.11 Medium Access Control (MAC) and Physical Layer Specifications*. 2003.
- IEEE Computer Society. *IEEE802.11i Medium Access Control (MAC) Security Enhancements*. 2004.
- IEEE Computer Society. *IEEE802.11a Medium Access Control (MAC) High-speed Physical Layer in the 5 GHz Band*. 1999.
- IEEE Computer Society. *IEEE802.11b Medium Access Control (MAC) Higher-Speed Physical Layer Extension in the 2.4 GHz Band*. 1999.

IEEE Computer Society. *IEEE802.11g Medium Access Control (MAC) mendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band*. 2003.

Sankar, K, Sundaralingam, S., Balinsky, A., Miller, D. *Cisco Wireless LAN Security*, Cisco Press, 2005.

Cache, J., Liu V. *Hacking Exposed Wireless*. McGraw-Hill, 2007.

Tanenbaum, A. *Redes de Computadoras*. Pearson, 2002.

NIST. SP 800-41. *Guidelines on Firewalls and Firewall Policy*. Noviembre, 2009.

Vladimirov, A., Gavrilenko, K., Mikhailovsky, A. *Hacking Wireless. Seguridad en redes inalámbricas*. Anaya Multimedia, 2004.

Brenne, P. *A Technical Tutorial on the IEEE 802.11 Protocol*. Breezecom, 2006.

Stephen Northcutt. *Network Intrusion Detection: An Analyst's Handbook*. New Riders, 1999.

Amado, Roberto. *Análisis de la seguridad en redes 802.11*. Universidad de Valencia, 2008.

IETF website: <http://www.ietf.org/>

TCP Guide website: <http://www.tcpipguide.com/>

Cisco Documentation website: <http://www.cisco.com/>

Wikipedia website: <http://www.wikipedia.org/>

MAP. MAGERIT v.2.0. *Metodología de Análisis y Gestión de Riesgos de las Administraciones Públicas*. 2006.

Terry Escamilla. *Intrusion Detection: Network Security beyond the Firewall*. John Wiley and Sons, 1998.

UNE-ISO/IEC 27001. *Sistemas de Gestión de la Seguridad de la Información. Requisitos*. AENOR. Noviembre, 2007.

UNE-ISO/IEC 27002. *Código de buenas prácticas para la gestión de la seguridad de la información*. AENOR. Diciembre, 2009.

ISO/IEC 27035. *Information technology -- Security techniques -- Information security Incident Management*. ISO. Agosto, 2011.

NIST. SP 800-100. *Information Security Handbook: A Guide for Managers*. Octubre, 2006.

## ANEXO B. ACRÓNIMOS

- 3DES.** Triple DES (*Data Encryption Standard*).
- ACL.** Lista de control de acceso (*Access Control List*).
- AR.** Análisis de riesgos.
- AP.** Autorización para Pruebas.
- AP.** Punto de Acceso (*Access Point*).
- APO.** Autorización Provisional para Operar.
- ATPO.** Autorización Temporal con Propósitos Operacionales.
- CC.** *Common Criteria*.
- CCN.** Centro Criptológico Nacional.
- CERT.** *Computer Emergency Response Team*.
- CNI.** Centro Nacional de Inteligencia.
- CO.** Concepto de Operación.
- DDoS.** *Distributed Denial of Service*.
- DES.** Data Encryption Standard.
- DLP.** *Data Loss Prevention*.
- DMZ.** Zona desmilitarizada (*De-Militarized Zone*).
- DRS.** Declaración de Requisitos de Seguridad.
- DoS.** *Denial of Service*.
- FTP.** *File Transfer Protocol*.
- HIDS.** Sistema de detección de intrusos basado en host (*Host-based Intrusion Detection System*).
- HTTP.** *Hyper Text Transfer Protocol*.
- HTTPS.** HTTP seguro.
- ICMP.** *Internet Control Messaging Protocol*.
- IDS.** Sistema de detección de intrusos (*Intrusion Detection System*).
- IPS.** Sistema de prevención de intrusiones (*Intrusion Prevention System*).
- ISO.** *International Organization for Standardization*.
- ITSEC.** *Information Technology Security Evaluation Criteria*.
- LFM.** *Log File Monitor*.
- MAGERIT.** Metodología de Análisis y GEstión de Riesgos de los sistemas de Información de las adminisTraciones públicas.
- NIDS.** Sistema de detección de intrusos basado en red (*Network-based Intrusion Detection System*).
- OSI.** Modelo de interconexión de sistemas abiertos (*Open System Interconnection*).

**OTP.** Clave de uso único (*One Time Password*).

**PILAR.** Procedimiento Informático Lógico de Análisis de Riesgos.

**POS.** Procedimientos Operativos de Seguridad.

**PPT.** Pliego de Prescripciones Técnicas.

**QoS.** Calidad de Servicio (*Quality of Service*).

**RPF.** Filtrado de camino inverso (*Reverse Path Filtering*).

**SEM.** *Security Information Management*.

**SIEM.** *Security Information and Event Management*.

**SIV.** *System Integrity Verifier*.

**SSH.** *Secure Shell*.

**SSO.** *Single Sign On*.

**STIC.** Seguridad de las Tecnologías de la Información y las Comunicaciones.

**TCP.** *Transport Control Protocol*.

**TCSEC.** *Trusted Computer System Evaluation Criteria*.

**TEMPEST.** *Transient Electro Magnetic Pulse Emanation Standard*.

**UDP.** *User Datagram Protocol*.

**UTM.** Gestión unificada de amenazas (*Unified Threat Management*).

**VPN.** Red Privada Virtual (*Virtual Private Network*).

**WAF.** Web Application Firewall.

**WEP.** *Wired Equivalent Privacy*.

**WPA.** *WiFi Protected Access*.