



## MF0487\_3: Auditoría de seguridad informática

**Certificado de Profesionalidad**  
**IFCT0109 - Seguridad informática**



IFCT0109 > MF0487\_3

# ***MF0487\_3: Auditoría de seguridad informática***

## ÍNDICE

Capítulo 1 Criterios generales comúnmente aceptados sobre auditoría informática .....	4
1. Introducción.....	7
2. Código deontológico de la función de auditoría .....	7
3. Relación de los distintos tipos de auditoría en el marco de los sistemas de la información .....	14
4. Criterios a seguir para la composición del equipo auditor.....	17
5. Tipos de pruebas a realizar en el marco de la auditoría. Pruebas sustantivas y pruebas de cumplimiento .....	19
6. Tipos de muestreo a aplicar durante el proceso de auditoría .....	21
7. Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools) .....	24
8. Explicación de los requerimientos que deben cumplir los hallazgos de auditoría .....	26
9. Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades .....	28
10. Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas.....	29
11. Resumen.....	31
Capítulo 2 Aplicación de la normativa de protección de datos de carácter personal.....	32
1. Introducción.....	32
2. Principios de protección de datos de carácter personal .....	32
3. Normativa europea recogida en la directiva 95/46/CE .....	38
4. Normativa nacional recogida en el Código penal, Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD), Ley orgánica de Protección de Datos (LOPD) y Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (R. D. 1720/2007).....	41
5. Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización .....	45
6. Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007 .....	46
7. Guía para la realización de la auditoría bienal obligatoria de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal .....	50
8. Resumen .....	52

Capítulo 3 Análisis de riesgos de los sistemas de información.....	53
1. Introducción.....	53
2. Introducción al análisis de riesgos.....	53
3. Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura.....	60
4. Particularidades de los distintos tipos de código malicioso .....	64
5. Principales elementos del análisis de riesgos y sus modelos de relaciones .....	68
6. Metodologías cualitativas y cuantitativas de análisis de riesgos .....	71
7. Identificación de los activos involucrados en el análisis de riesgos y su valoración .....	74
8. Identificación de las amenazas que pueden afectar a los activos identificados previamente ..	77
9. Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo análisis local, análisis remoto de caja blanca y de caja negra.....	81
10. Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría .....	84
11. Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas .....	85
12. Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse .....	87
13. Determinación de la probabilidad e impacto de materialización de los escenarios.....	90
14. Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza .....	92
15. Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no.....	94
16. Relación de las distintas alternativas de gestión de riesgos.....	96
17. Guía para la elaboración del plan de gestión de riesgos .....	98
18. Exposición de la metodología NIST SP 800-30.....	101
19. Exposición de la metodología Magerit versión 2.....	103
20. Resumen.....	106
Capítulo 4 Uso de herramientas para la auditoría de sistemas.....	108
1. Introducción.....	108
2. Herramientas del sistema operativo tipo Ping, Traceroute, etc. ....	108
3. Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc. ....	112

4. Herramientas de análisis de vulnerabilidades tipo Nessus .....	120
5. Analizadores de protocolos tipo WireShark, DSniff, Cain & Abel, etc. ....	122
6. Analizadores de páginas web tipo Acunetix, Dirb, Parosproxy, etc. ....	127
7. Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc. ....	131
8. Resumen .....	134

## Capítulo 5 Descripción de los aspectos sobre cortafuegos en auditorías de sistemas informáticos .....

1. Introducción.....	136
2. Principios generales de cortafuegos.....	136
3. Componentes de un cortafuegos de red .....	141
4. Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad .....	144
5. Arquitecturas de cortafuegos de red.....	149
6. Otras arquitecturas de cortafuegos de red .....	154
7. Resumen .....	155

## Capítulo 6 Guías para la ejecución de las distintas fases de la auditoría de sistema de información .....

1. Introducción.....	156
2. Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada.....	156
3. Guía para la elaboración del plan de auditoría .....	163
4. Guía para las pruebas de auditoría.....	168

## **CAPÍTULO 1 CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA**

### **1. INTRODUCCIÓN**

La complejidad y evolución de los sistemas de informáticos necesaria la aparición de profesionales informáticos que se encarguen de evaluar su correcto funcionamiento y detectar aquellos puntos débiles que requieran la adopción de medidas correctivas y preventivas para evitar pérdidas de información relevante que podrían conllevar costes importantes a las organizaciones.

Por este motivo, la figura del auditor informático se hace cada vez más presente en las organizaciones: un profesional independiente que evalúe la eficiencia de sus sistemas informáticos y que sea capaz de formular recomendaciones y propuestas de mejora con la finalidad de mantener la integridad y exactitud de los datos y así garantizar un servicio correcto dentro de unos estándares de calidad.

En este capítulo, se enumeran las características principales tanto de la actividad de la auditoría informática como de la figura del profesional auditor, además de introducir las principales tareas que se deben ejecutar para que la auditoría cumpla con los objetivos previstos.

### **2. CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA**

La auditoría es el análisis exhaustivo de los sistemas informáticos con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse.

En el momento de desempeñar las funciones de auditoría en un sistema de información, los auditores deben cumplir una serie de normas éticas y un código deontológico para cumplir con profesionalidad y rigidez sus objetivos.

El código deontológico consiste en una serie de preceptos en los que se determinan los derechos exigibles a ciertos profesionales cuando desempeñan su actividad con el fin de ajustar los comportamientos profesionales a unos principios éticos y morales adecuados.

En el caso de la auditoría informática, existe una organización internacional que diseña los estándares de auditoría y control de sistemas de información aceptados por la comunidad general de auditoría.

Esta organización, llamada ISA CA (Information Systems Audit and Control Association), expide además el certificado CISA (Certified Information Systems Auditor) a quien cumpla los requisitos estipulados en cuanto a normas, código ético, procedimientos de control, etc.

#### **2.1.- Normas profesionales de la ISACA**

Los miembros que pertenecen a ISACA y los que están en posesión del certificado CISA deben comprometerse a comprender y cumplir las diez Normas de Auditoría de Sistemas de Información:

1. El auditor de los sistemas de información debe ser independiente del ente auditado, tanto en actitud como en apariencia.

2. Para que la auditoría se desarrolle de un modo objetivo, la función de auditoría debe ser independiente del área que se pretende auditar.
3. El auditor debe cumplir con los preceptos del Código de Ética Profesional de la ISACA.

Nota: El Código de Ética Profesional de la ISACA está formado por una serie de directivas de actuación profesional y personal que deben seguir todos los miembros que forman parte de la asociación.

4. El auditor debe tener los suficientes conocimientos técnicos y destrezas para desempeñar correctamente las funciones de auditoría encomendadas.
5. El auditor de sistemas de información debe reciclar continuamente sus conocimientos para mantener en un nivel adecuado su competencia técnica.
6. Las auditorías de sistemas de información deben ser planificadas y supervisadas con suficiente rigor para mantener la seguridad de que se cumplen los objetivos de auditoría establecidos y las normas estipuladas.
7. En el proceso de auditoría, el auditor debe respaldarse necesariamente con evidencias que confirmen sus hallazgos, resultados y conclusiones.
8. Las tareas de auditoría deben llevarse a cabo con sumo cuidado profesional, cumpliendo las normativas de auditoría aplicables.

Nota: En la actualidad, ISACA cuenta con más de 95.000 miembros de más de 160 países, lo que apoya su seriedad y profesionalidad.

9. Durante la realización del informe, el auditor debe expresar con claridad los objetivos de la auditoría, su duración (de fecha a fecha) y las tareas realizadas en todo el proceso.
10. En el mismo informe, el auditor también deberá mencionar las observaciones necesarias para una mejor comprensión y las conclusiones obtenidas con las distintas tareas realizadas.

En la imagen siguiente, se observa una descripción básica de cada una de las normas que forman parte de la normativa profesional de la ISACA.



## Normas profesionales de la ISACA

- Actitud y apariencia
- Relación en la organización
- Código de ética profesional
- Destrezas y conocimientos
- Educación profesional
- Planificación y supervisión

El incumplimiento del Código de Ética de ISACA puede desembocar en una investigación de las actuaciones de la empresa por parte de ISACA e, incluso, en la adopción de medidas disciplinarias.

### 2.2.- Código deontológico de la auditoría

Además de las Normas Profesionales y el Código de Ética propuestos por ISACA, hay también un código deontológico que deben tener en cuenta todos los profesionales que quieran dedicarse a la actividad de auditoría informática.

Como ya se ha mencionado, el código deontológico está formado por una serie de principios morales elaborados que sirvan de guía a los auditores informáticos en el momento de ejercer su profesión, teniendo en cuenta una ética de la informática.

#### Principios del código deontológico de la auditoría

El código deontológico de la auditoría está formado por una serie de principios fundamentales, descritos a continuación.

##### Principio de beneficio del auditado

Las tareas del auditor deben estar enfocadas a maximizar el beneficio de sus clientes sin anteponer sus intereses personales. En caso de hacer prevalecer sus intereses antes de los clientes, se considerará una conducta no ética.

Además, el auditor también deberá evitar recomendar actuaciones que no sean necesarias o que impliquen algún tipo de riesgo sin justificación para el auditado.



**Principio de calidad**

El auditor debe ejercer sus tareas dentro de unos estándares de calidad de modo que, en caso de no disponer de medios adecuados para realizar sus actividades convenientemente, deberá negarse a realizarlas hasta que no se garantice un mínimo de condiciones técnicas.

Si el auditor, en el momento de elaborar el informe, considera que no tiene conocimientos técnicos suficientes, deberá remitirlo a otro técnico más cualificado para mejor calidad de la auditoría.

**Principio de capacidad**

El auditor informático debe estar plenamente capacitado para el ejercicio de su profesión y, para ello, debe actualizar sus conocimientos de forma periódica mediante actividades de formación continua.

El auditor debe planificar su formación para que sus conocimientos se actualicen de un modo acorde con la evolución de las tecnologías de la información.

Para conocer sus necesidades de formación, el auditor deberá ser consciente en todo momento de sus aptitudes y capacidades, conociendo también sus puntos débiles con el fin de cometer menos errores en el ejercicio de sus tareas.

**Principio de cautela**

Las recomendaciones del auditor siempre deben estar basadas en sus conocimientos y experiencias, manteniendo al auditado siempre informado de la evolución de las tecnologías de la información y de las actuaciones que se deben llevar a cabo.

**Principio de comportamiento profesional**

En el momento de realizar las tareas de su profesión, el auditor siempre deberá tener en cuenta las normas tanto explícitas como implícitas, teniendo sumo cuidado en la exposición de sus opiniones.

Además, debe tener seguridad en sus actuaciones y en la exposición de sus conocimientos técnicos, transmitiendo una imagen de precisión y exactitud a sus auditados.

**Principio de concentración en el trabajo**

En momentos de alto volumen de trabajo, el auditor deberá evitar que el exceso de trabajo dificulte su capacidad de concentración y precisión en sus tareas.

Por ello, deberá realizar previsiones de posibles acumulaciones de trabajo y evaluar las consecuencias de no llevar a cabo sus tareas con la precisión y profesionalidad requerida para mantener unos estándares de calidad en la auditoría.

**Nota**

En momentos de alta carga de trabajo, el auditor nunca deberá realizar informes y emitir conclusiones partiendo de trabajos anteriores para ahorrar esfuerzos; no solo habrá una merma de la calidad, sino que también pueden obtenerse conclusiones erróneas y, por tanto, auditorías poco válidas.

**Principio de confianza**

El auditor deberá dar siempre sensación de confianza al auditado mediante la transparencia en sus actuaciones. Esta confianza entre auditor y auditado se confirmará resolviendo las posibles dudas que puedan surgir en ambas partes y utilizando un lenguaje llano que mejore la comprensión y comunicación de las tareas realizadas.

**Principio de criterio propio**

El auditor deberá actuar siempre con criterio propio e independencia, sin permitir que su criterio dependa de otros profesionales.

En caso de haber diferencia de criterios, el auditor deberá reflejarlo en el informe, justificando y motivando con claridad su criterio.

**Principio de economía**

El auditor deberá delimitar específicamente el alcance y los límites de la auditoría, evitando retrasos innecesarios que puedan llevar a costes extra y protegiendo siempre los derechos económicos de los auditados.

**Principio de fortalecimiento y respeto de la profesión**

Los auditores deberán cuidar y proteger el valor de su profesión, manteniendo unos precios acordes con su preparación.

Deberán evitar establecer precios demasiado reducidos para no caer en términos de competencia desleal y evitar confrontaciones con otros auditores, promoviendo en todo momento el respeto entre ellos.

**Principio de integridad moral**

Los auditores deberán desempeñar sus tareas con una actitud honesta, leal y diligente, evitando siempre participar en actividades que puedan perjudicar a terceras personas o al auditado.

Además, en ningún caso deberán aprovecharse de sus conocimientos para utilizarlos en contra del auditado.

**Recuerde**

La ética debe estar presente siempre en la actuación profesional de los auditores informáticos, protegiendo los derechos del auditado y evitando su perjuicio derivado de la aplicación de sus conocimientos técnicos.

**Principio de legalidad**

El auditor deberá promover la preservación de la legalidad a sus auditados, no consintiendo la eliminación de dispositivos de seguridad y ni de datos relevantes para la elaboración de la auditoría.

**Principio de precisión**

La actuación del auditor debe realizarse siempre con precisión, no emitiendo conclusiones ni informes hasta no estar completamente convencido de su correcta elaboración.

En el momento de la exposición de las conclusiones, el auditor actuará con carácter crítico e indicando con claridad cómo se ha llevado a cabo el análisis de los datos y los motivos que han llevado a sus conclusiones.

**Principio de responsabilidad**

El auditor debe asumir la responsabilidad de sus actuaciones, juicios y consejos y estará obligado a hacerse cargo de los posibles daños y perjuicios que haya podido causar alguna de sus actuaciones.

**Nota**

El hecho de obligar a asumir responsabilidades por parte del auditor le obliga a actuar con suma cautela y seguridad para evitar juicios y conclusiones erróneas que puedan llevar a consecuencias dañinas.

**Principio de secreto profesional**

El auditor deberá mantener siempre la confidencialidad de los datos de los auditados, manteniendo siempre una relación de confianza entre ellos. En ningún momento podrá difundir datos obtenidos en la realización de sus tareas a terceras personas.

Para mantener este secreto profesional, será necesaria la implantación de medidas de seguridad que garanticen la protección de la información obtenida en la auditoría.

### **Principio de veracidad**

El auditor, en el ejercicio de su profesión, deberá asegurar en todo momento la veracidad de sus manifestaciones y opiniones, sin incumplir el secreto profesional y el respeto al auditado.

PRINCIPIOS DEL CÓDIGO DEONTOLÓGICO DE LA AUDITORÍA
Principio del beneficio del auditado
Principio de calidad
Principio de capacidad
Principio de cautela
Principio de comportamiento profesional
Principio de concentración en el trabajo
Principio de confianza
Principio de criterio propio
Principio de economía
Principio de fortalecimiento y respeto de la profesión
Principio de integridad moral
Principio de legalidad
Principio de precisión
Principio de responsabilidad
Principio de secreto profesional
Principio de veracidad

### 3. RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE LA INFORMACIÓN

La auditoría en sí es una actividad que consiste en emitir un juicio y opinión profesional sobre el objeto o la materia analizada, indicando si se están cumpliendo los requisitos que procedan en cada temática. Esta opinión deberá fundamentarse en una serie de procedimientos que justifiquen y sirvan de soporte al análisis realizado.

En la siguiente tabla, se muestran varios tipos de auditoría, atendiendo al tipo de información que se maneja:

<b>Clase Objeto analizado Finalidad</b>	<b>Clase Objeto analizado Finalidad</b>	<b>Clase Objeto analizado Finalidad</b>
<b>Financiera Cuentas anuales</b> <b>Verificar la representación de la realidad financiera de la empresa.</b>	Financiera Cuentas anuales Verificar la representación de la realidad financiera de la empresa.	Financiera Cuentas anuales Verificar la representación de la realidad financiera de la empresa.
<b>De gestión Acciones de los departamentos de la empresa</b> <b>Comprobar la eficacia y eficiencia de los procesos de la organización.</b>	De gestión Acciones de los departamentos de la empresa Comprobar la eficacia y eficiencia de los procesos de la organización.	De gestión Acciones de los departamentos de la empresa Comprobar la eficacia y eficiencia de los procesos de la organización.
<b>De cumplimiento Normas establecidas</b> <b>Comprobar si las operaciones y actuaciones respetan las normas establecidas.</b>	De cumplimiento Normas establecidas Comprobar si las operaciones y actuaciones respetan las normas establecidas.	De cumplimiento Normas establecidas Comprobar si las operaciones y actuaciones respetan las normas establecidas.
<b>Informática</b>	Sistemas informáticos	Comprobar la operatividad y eficiencia de los procesos informáticos según normas establecidas.

La variedad de tipologías de auditoría no solo está presente en temáticas generales, sino que dentro de cada una de ellas se pueden distinguir subtipos de auditorías según las áreas específicas.

#### 3.1.- Tipos de auditorías dentro de los sistemas de información

Dentro del área de los sistemas de información, se pueden encontrar varias divisiones, descritas en el siguiente gráfico:

## Tipos de auditorías de sistemas de información

- Explotación
- Sistemas
- Comunicaciones
- Desarrollos de proyectos
- Seguridad

### Auditoría informática de explotación

La auditoría informática de explotación se encarga de analizar resultados informáticos de todo tipo: listados impresos, órdenes automatizadas de procesos, etc.

El análisis consistirá sobre todo en someter los resultados obtenidos a controles de calidad y en analizar si su distribución posterior (al cliente, a otros empleados, a superiores, etc.) se realiza mediante un proceso adecuado.

También se auditan las distintas secciones que componen la informática de explotación y las relaciones existentes entre ellos.

#### Recuerde

La explotación informática es el proceso encargado de realizar los resultados informáticos de cualquier tipo.

### Auditoría informática de sistemas

La auditoría informática de sistemas se encarga de analizar las actividades relacionadas con en el entorno de sistemas informáticos. Más concretamente, en esta tipología se analizan los siguientes componentes:

- **Sistemas operativos:** se comprueba si están actualizados y, en caso de no estarlo, se averiguan las causas de la desactualización. También se analizan posibles incompatibilidades de software ocasionadas por el sistema operativo.
- **Software básico:** se analizan las distintas aplicaciones instaladas para verificar que no agreden ni condicionan al sistema operativo.

- **Tunning:** se evalúan las distintas técnicas y medidas de evaluación de los comportamientos del sistema y de los subsistemas.
- **Optimización de los sistemas y subsistemas:** la auditoría comprobará que las acciones de optimización de sistemas y subsistemas son efectivas y que no se compromete su operatividad.
- **Administración de las bases de datos:** el auditor se asegurará del conocimiento de los distintos procedimientos de la base de datos y comprobará la seguridad, la integridad y la consistencia de los datos.
- **Investigación y desarrollo:** la auditoría se encargará de mantener la actividad de investigación y desarrollo, impidiendo que por estas se dificulten procesos y tareas fundamentales.

### **Auditoría informática de comunicaciones y redes**

La auditoría informática de comunicaciones y redes se encargará de analizar los distintos dispositivos de comunicación que forman parte de las redes de la organización para detectar sus debilidades y proponer medidas que las corrijan.

Para ello, los auditores deberán conocer la topología de la red de comunicaciones, en la que se describan con detalle las líneas que forman parte de ella, cómo son y su ubicación para comprobar su nivel de operatividad.

### **Auditoría de desarrollo de proyectos**

En la auditoría de desarrollo de proyectos, los auditores informáticos analizan la metodología utilizada para desarrollar los distintos proyectos de la organización, distinguiendo entre cada área de negocio de la empresa.

También se analiza el desarrollo de proyectos globales que se extienden al conjunto de la organización, comprobando su correcta ejecución y el mantenimiento de la seguridad a lo largo de todo el proceso.

### **Auditoría de seguridad informática**

La auditoría de seguridad informática analiza todos los procesos referentes a la seguridad informática, tanto física como lógica.

La seguridad física es la protección de los componentes hardware, dispositivos, instalaciones y entornos de los distintos sistemas informáticos.

Los auditores deberán analizar la correcta protección de los elementos físicos ante posibles catástrofes, incendios, robos, etc.



La seguridad lógica, por el contrario, es la protección del software, los procesos y programas del sistema., y su auditoría consistirá en analizar la correcta protección y actualización de estos componentes, además de la protección de los datos que forman parte del sistema.

#### 4. CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR

Antes de empezar la auditoría, el auditor deberá elaborar una planificación en la que se detallen los objetivos y procedimientos que se llevarán a cabo para realizar la auditoría informática.

En esta planificación se deberá incluir sobre todo:

- Lugar o lugares en los que se realizarán las tareas de auditoría.
- Duración de la auditoría.
- Fecha límite para la finalización de la auditoría.
- Composición del equipo de auditoría.
- Áreas que serán auditadas.

En resumen, el auditor planificará los objetivos a cumplir y los métodos y procedimientos que se van a proseguir para lograr dichos objetivos de un modo eficaz y eficiente.

Como ya se puede observar, la composición del equipo de auditoría es un aspecto fundamental para lograr el éxito de la auditoría informática.

Las tareas del auditor son de lo más variadas y es necesario formar un equipo con profesionales multidisciplinares y capacitados para que, de forma global, se puedan llevar a cabo una serie de actividades básicas, descritas en la tabla siguiente.

ACTIVIDADES BÁSICAS DEL AUDITOR INFORMÁTICO
Establecimiento y análisis de la política de seguridad.
Verificación y cumplimiento de los estándares, normas y cualificaciones relacionadas con la auditoría y la seguridad informáticas.
Organización de la seguridad y clasificación de los recursos.
Análisis de las inversiones realizadas y futuras de seguridad.
Análisis de los riesgos de la organización.
Análisis y control de la seguridad física de la organización.
Establecimiento de medidas de protección y control de accesos al sistema.
Evaluación de la seguridad en las comunicaciones y operaciones.
Evaluación de la seguridad y vulnerabilidades de los sistemas operativos y demás software del sistema.
Definición del plan de continuidad de la organización.
Gestión de la seguridad de la organización. con el establecimiento de medidas y definición del cuadro integral de mandos.

#### **4.1.- Características y capacidades del equipo auditor**

Para llevar a cabo todas las actividades mencionadas en la tabla anterior, no es necesario que sean desempeñadas por un solo auditor informático, sino que se recomienda seleccionar una serie de técnicos especializados que abarquen los conocimientos y capacidades suficientes para desarrollar todas las tareas de un modo global.

El número de personas que formen el equipo auditor puede variar según las dimensiones de la organización, de los sistemas y de los equipos, pero, independientemente de la magnitud del equipo, sus miembros deberán estar suficientemente capacitados y deberán tener un alto sentido de la ética y la moralidad.

Para seleccionar el equipo adecuado, en un primer lugar hay que pensar en profesionales con suficiente nivel para realizar una correcta coordinación del desarrollo de las tareas de la auditoría, siendo capaz de facilitar la información requerida en todo momento.

Además, el equipo debe estar formado por profesionales con conocimientos básicos en cuanto a:

- Desarrollo de proyectos informáticos.
- Gestión del departamento de sistemas.
- Análisis de riesgos en sistemas informáticos.
- Sistemas operativos.
- Redes locales y telecomunicaciones.
- Gestión de bases de datos.
- Seguridad física y del entorno.
- Planificación informática.
- Gestión de la seguridad de los sistemas.
- Gestión de problemas, incidencias y cambios en entornos informáticos.
- Administración de datos.
- Ofimática.
- Permisos de acceso y encriptación de datos.
- Comercio electrónico.

Además, a todos estos conocimientos básicos habría que añadir otros conocimientos más especializados, atendiendo a las características de los sistemas y organizaciones a auditar. Por ejemplo, para auditar empresas cuya actividad principal es el desarrollo del negocio *on-line* no se requerirá el mismo conocimiento que para empresas cuya actividad se desarrolla enteramente *off-line*; para las primeras será necesario que los auditores tengan conocimientos más específicos de comercio electrónico, plataformas de pago seguras para Internet, etc.

**Nota**

El equipo auditor, para que la auditoría termine con éxito, deberá contar con el apoyo de la alta dirección de la organización. Si se cuenta con el apoyo suficiente, la obtención de los datos necesarios para la auditoría y la colaboración de los empleados y departamentos será más fácil y rápida, mejorando la eficiencia y eficacia de los procesos de auditoría.

Debido a la gran variedad de conocimientos específicos necesarios para abarcar todo tipo de empresas, el equipo auditor deberá contar con una serie de colaboradores directos en la realización de la auditoría para complementar las posibles deficiencias técnicas que puedan surgir. En concreto, es recomendable contar con colaboradores con características como:

- Técnicos en informática.
- Conocimientos en administración y finanzas.
- Experiencia en informática y análisis de sistemas.
- Experiencia y conocimiento en psicología industrial.
- Conocimientos específicos de sistemas operativos, bases de datos, redes, etc., según el área que se vaya a auditar.
- Conocimientos en análisis de riesgos.

Una vez decidido el equipo auditor y el personal que va a colaborar en la auditoría informática, ya se podrá proceder a la elaboración de contrato o carta convenio en la que se definan específicamente los objetivos, miembros, limitaciones, colaboración necesaria por parte de la organización, informes a elaborar y entregar y responsabilidad asumida por los auditores.

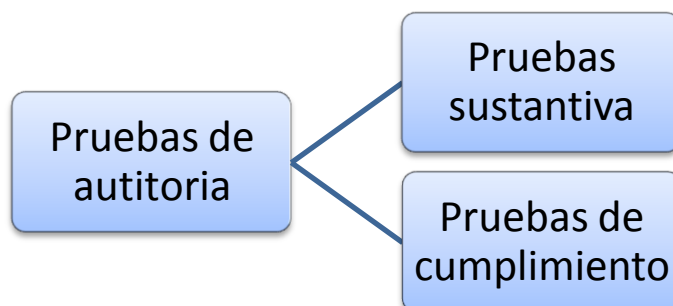
Este contrato o carta convenio deberá ser aceptada por la organización y el equipo auditor para poder comenzar con las tareas específicas de la auditoría.

## **5. TIPOS DE PRUEBAS A REALIZAR EN EL MARCO DE LA AUDITORÍA. PRUEBAS SUSTANTIVAS Y PRUEBAS DE CUMPLIMIENTO**

Una de las tareas fundamentales de la auditoría informática son las pruebas de auditoría. Las pruebas clásicas consisten en el desarrollo de un conjunto de técnicas para probar las aplicaciones y sistemas operativos con datos de prueba. Mediante la observación de los datos de entrada, los datos de salida obtenidos y los datos de salida esperados, se pueden realizar comparaciones para verificar la calidad, eficiencia y eficacia de los sistemas evaluados.

En auditoría informática, se distinguen dos tipos de pruebas:

- **Pruebas sustantivas:** pruebas que pretenden identificar los errores derivados de la falta de seguridad o confidencialidad de los datos. Evalúan la calidad de los datos y verifican si los controles establecidos por las políticas o procedimientos son eficaces.
- **Pruebas de cumplimiento:** las que permiten determinar si un sistema de control interno y/o procedimiento funciona correctamente y si es acorde con las políticas, normativas y procedimientos definidos por la organización.



Mientras que las pruebas de cumplimiento tienen como objeto la obtención de evidencias que prueben el cumplimiento de los procedimientos de control, las pruebas sustantivas pretenden obtener evidencias para evaluar la integridad de los datos y procedimientos individuales.

Las pruebas de cumplimiento verifican la correcta utilización de los controles de un modo acorde con las políticas y procedimientos de la gestión establecidos por la organización. Un ejemplo de estas es la prueba de la auditoría para determinar si los controles de una librería de programas es adecuada: el auditor puede hacer una selección de programas y determinar la adecuación de su utilización con las políticas de la organización.

Sin embargo, las pruebas sustantivas pretenden obtener evidencias de la validez e integridad de los datos almacenados en los equipos y dispositivos. Por ejemplo, una prueba sustantiva sería la revisión del inventario para comprobar si todos los dispositivos magnéticos están correctamente inventariados.

En concreto, las diferencias fundamentales entre ambas pruebas se determinan en la tabla siguiente.

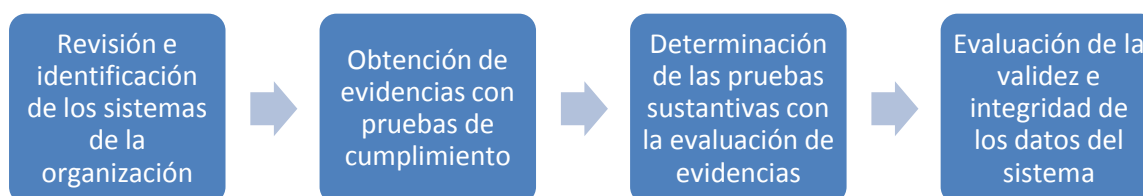
Tipo de prueba	De cumplimiento	Sustantiva
<b>Objetivo</b>	Funcionamiento de los procedimientos y controles internos de la organización.	Validar la integridad y exactitud de los datos del sistema.
<b>Objeto auditado</b>	Gestión de la organización.	Sistema de información de la organización

### 5.1.- Relación entre las pruebas de cumplimiento y las pruebas sustantivas

Existe una correlación directa entre las pruebas de cumplimiento y las pruebas sustantivas necesarias para una correcta auditoría.

Si los resultados obtenidos de las pruebas de cumplimiento indican que los controles de sistemas aplicados son correctos y adecuados, son motivo de justificación para utilizar menos pruebas sustantivas (se entiende que, si los controles son correctos, se cumple con las políticas de la organización y hay menos probabilidades de detectar errores y fallos de seguridad).

Sin embargo, si los resultados de las pruebas de cumplimiento determinan fallos y debilidades en los controles, las pruebas sustantivas deben ser más detalladas y extensas para comprobar la validez, integridad y exactitud de los datos del sistema (si hay fallos en los controles es muy probable que las políticas de seguridad establecidas en la organización no se cumplan adecuadamente y, por lo tanto, que existan problemas de integridad y validez de los datos).



De este modo, la relación entre los dos tipos de pruebas de auditoría se puede visualizar en la siguiente tabla.

El procedimiento para la obtención y análisis de evidencias que relaciona ambas pruebas se define en varias fases:

1. Revisión de los sistemas de la organización para identificar cuáles son los controles que dispone.
2. Realización de pruebas de cumplimiento que evalúen el correcto funcionamiento de los controles identificados.
3. Evaluación de las evidencias obtenidas en las pruebas de cumplimiento para determinar la extensión y precisión de las pruebas sustantivas.
4. Evaluación de la validez de los datos con las evidencias obtenidas en las pruebas sustantivas.

## 6. TIPOS DE MUESTREO A APLICAR DURANTE EL PROCESO DE AUDITORÍA

Los auditores informáticos, para que la auditoría se ejecute dentro de unos estándares de calidad adecuados, deben obtener una serie de evidencias para realizar análisis, comprobaciones y obtener resultados concluyentes que permitan la elaboración del informe correctamente. Para que los resultados no sean erróneos, es necesario que las evidencias sean comprobatorias, suficientes y competentes, siempre teniendo en cuenta las limitaciones que pueden encontrarse en el desarrollo de las tareas de auditoría.

No obstante, es fundamental que la auditoría detecte y señale las deficiencias del sistema analizado de un modo eficaz y eficiente.

El muestreo es una herramienta de investigación científica muy utilizado para obtener las evidencias necesarias para detectar estas deficiencias.

Su finalidad principal es determinar y facilitar información sobre cuáles son las partes analizadas que requieren un examen más exhaustivo para obtener los resultados y conclusiones más relevantes.

### Importante

El concepto de evidencia en las auditorías informáticas no solo abarca las técnicas de muestreo, es un concepto mucho más amplio que facilita información suficiente como para que el auditor sea capaz de tomar decisiones firmes y correctas.

El muestreo de auditoría deberá permitir a los auditores informáticos la obtención y evaluación de las evidencias de auditoría sobre una cierta característica de los elementos seleccionados; su finalidad principal será la de ayudar a determinar una conclusión respecto a la población de la que se ha obtenido la muestra (decidiendo si se cumplen o no las hipótesis formuladas previamente).

La obtención de muestras se puede llevar a cabo mediante varios tipos de muestreos: estadístico y no estadístico.

### 6.1.- Muestreo estadístico

Los muestreos estadísticos son aquellos en los que el auditor utiliza técnicas matemáticas para decidir varios aspectos importantes de la muestra como:

Puntos relevantes a auditar.

- Tamaño de la muestra.
- Grados de confianza.
- Márgenes de error admitidos.

Esta técnica para obtener la muestra sirve de complemento para reforzar los criterios del auditor, facilitando información que permita confirmar sus hipótesis. También en caso de que el auditor esté incurriendo en análisis erróneos, las técnicas de muestreo estadístico le confirmarán su error y le facilitarán pistas para formular nuevas hipótesis.

**Nota**

El método de muestreo estadístico no debe ser el único a utilizar para obtener la muestra, sino que debe servir como complemento al muestreo no estadístico.

**Ejemplo de muestreo estadístico**

Se obtienen los siguientes datos referentes al tiempo de ejecución de un proceso de varios empleados de la organización:

Empleado	1	2	3	4	5
Tiempo	10 min	12 min	9 min	11 min	15 min

De estos datos, se deduce que:

- El promedio de tiempo de ejecución del proceso es de 11,4 minutos, suma de todos los tiempos dividida entre el número de empleados:

$$(10 + 12 + 9 + 11 + 15) / 5.$$

- Las desviaciones de los distintos empleados se calculan restando el tiempo de cada empleado del tiempo medio obtenido, siendo:

Empleado	1	2	3	4	5
Tiempo	10 min	12 min	9 min	11 min	15 min
Desviaciones	-1,4	+0,6	-2,4	-0,4	+3,6

Viendo las desviaciones el empleado número 4, es el que más se ha acercado al promedio obtenido.

Las diferencias extremas (empleado 3 y empleado 5), tanto positivas como negativas, deberán estudiarse con más profundidad para detectar alguna deficiencia que pueda provocarlas.



## 6.2.- Muestreo no estadístico

El método de muestreo no estadístico se basa sobre todo en el criterio del auditor informático, siendo un criterio subjetivo.

En este caso, el auditor decide la muestra utilizando las técnicas aprendidas en el desarrollo de su profesión y los conocimientos adquiridos por su experiencia como auditor informático.

De este modo, decidirá el tamaño de la muestra teniendo en cuenta aquellos aspectos que considere menos confiables según sus criterios personales. También decidirá el grado de profundización del análisis de la muestra según la confiabilidad obtenida en el análisis del control interno del sistema o sistemas analizados.

## 7. UTILIZACIÓN DE HERRAMIENTAS TIPO CAAT (COMPUTER ASSISTED AUDIT TOOLS)

Las herramientas tipo CAAT (Computer Assisted Audit Tools) están formadas por un conjunto de herramientas y técnicas cuya función es facilitar al auditor informático el desarrollo de sus tareas y actividades. Las más utilizadas son las aplicaciones de auditoría generalizadas, los datos de prueba y los sistemas expertos de auditorías.

Estas herramientas se utilizan en tareas de auditoría tales como:

- Pruebas de controles en aplicaciones.
- Selección y monitorización de transacciones.
- Verificación de datos.
- Análisis de los programas de las aplicaciones.
- Auditoría de los centros de procesamiento de la información.
- Auditoría del desarrollo de aplicaciones.
- Técnicas de muestreo.

El auditor de sistemas de información debe tener un conocimiento profundo de estas herramientas y de sus posibles aplicaciones para saber utilizarlas correctamente e interpretar los resultados obtenidos de un modo pertinente y adecuado.

### Importante

Las herramientas CAAT son muy útiles para desarrollar la auditoría. No obstante, es imprescindible que el auditor documente los resultados de las pruebas obtenidas para dotarlas de confiabilidad y exactitud.

Estas herramientas constan de una serie de aspectos fundamentales y, entre sus funcionalidades principales, destacan las siguientes:

- Capacidad de muestreo.
- Utilización de algoritmos de búsqueda de patrones de fraude.
- Acceso a datos de varios formatos.
- Filtrado de datos.
- Recurrencia de pruebas.
- Relación de información procedente de varios archivos distintos.
- Generación de informes y reportes, tanto de texto como con gráficos.

La capacidad de las herramientas CAAT para tratar y analizar los datos es de lo más variada, facilitando información en varios formatos. La información que puede obtener de los datos entrantes se resume en la siguiente tabla.

<b>ANÁLISIS Y TAREAS EJECUTADAS POR LAS CAAT CON LOS DATOS ENTRANTES</b>
Verificación de campos
Obtención de totales de control
Utilización de comandos
Contar datos
Totalización de datos
Elaboración de perfiles
Elaboración de estadísticas
Ejecución de controles de secuencias

Estas herramientas para auditoría son muy útiles para facilitar al auditor el desarrollo de sus tareas. Como ya se ha mencionado, sus funcionalidades son de lo más variadas y extensas, dependiendo de la complejidad de la herramienta el desarrollo de análisis más o menos técnicos y profundos.

No obstante, todas las herramientas CAAT facilitan una serie de ventajas comunes, destacando entre ellas las siguientes:

- Se reduce el nivel de riesgo de la auditoría, al ser aplicaciones especializadas que minimizan la probabilidad de error.
- Al ser técnicas mecanizadas, añaden independencia a las actividades desarrolladas por el auditor.
- Proporcionan mayor coherencia a los resultados de la auditoría.
- Facilitan una mayor disponibilidad de la información.
- Facilitan y mejoran la identificación de las posibles excepciones.
- Añaden posibilidades de detectar, analizar y cuantificar los puntos débiles de los controles internos de los sistemas auditados.

### **7.1.- Documentación de las técnicas de las herramientas CAAT utilizadas**

Como se ha comentado anteriormente, las herramientas CAAT son de especial interés para añadir confiabilidad y facilidad de obtención de los datos y resultados de la actividad de auditoría.

A pesar de ser herramientas precisas y confiables, los resultados obtenidos no servirán si el auditor no documenta las técnicas utilizadas convenientemente.

Algunos de los modos de documentación de las técnicas CAAT utilizadas para ayudar y complementar al auditor son:

- Listado de los programas analizados y utilizados.
- Flujogramas.
- Informes que justifiquen las muestras obtenidas.
- Diseño de los archivos y los registros.
- Definición de los campos analizados.
- Relación de las instrucciones de operación realizadas.

#### **Definición**

##### **Flujogramas o diagramas de flujo**

Representaciones gráficas que reflejan las fases y/o etapas de un proceso mediante símbolos y figuras distintas.

Todos estos documentos servirán al auditor como medio para fundamentar las tareas realizadas, los datos obtenidos, los análisis realizados y los resultados alcanzados.

## **8. EXPLICACIÓN DE LOS REQUERIMIENTOS QUE DEBEN CUMPLIR LOS HALLAZGOS DE AUDITORÍA**

El término "hallazgo" tiene varios y numerosos significados y connotaciones. Dentro del ámbito de la auditoría, un hallazgo se refiere a un conjunto de información que recopila información específica sobre la actividad, tarea, proceso, condición, etc., analizados y evaluados, que sea considerada de interés para la organización.

En general, los hallazgos obtenidos se emplean a modo de crítica y muestran información sobre deficiencias o debilidades detectadas en el sistema auditado y presentadas en el informe de auditoría. No obstante, hay que tener en cuenta que, aunque son menos abundantes, también hay hallazgos positivos.

**Nota**

Los hallazgos no abarcan las conclusiones obtenidas por el auditor, sino simplemente hechos e informaciones obtenidas que ayudan al análisis de los resultados obtenidos en la elaboración del informe.

Los hallazgos de auditoría en concreto son hechos que el auditor ha detectado durante su examen y servirán como base para que el auditor pueda emitir sus conclusiones y recomendaciones para mejorar el funcionamiento del sistema auditado.

**8.1.- Requisitos básicos de los hallazgos de auditoría**

El hallazgo de auditoría es el resultado de comparar un criterio establecido y la situación real encontrada durante el examen del sistema auditado. Esta información permitirá al auditor identificar los hechos y debilidades importantes en la gestión de los recursos del sistema de información y en su correcto funcionamiento.

No obstante, los hallazgos de auditoría suelen informar sobre defectos y puntos negativos del sistema y, por ello, deben cumplir una serie de requisitos básicos que les den garantía y confiabilidad:

- Los hallazgos de auditoría deben tener cierta importancia que les dé la suficiente relevancia para que merezcan ser comunicados a la organización en el informe de auditoría.
- Los hallazgos deben estar basados en hechos y evidencias concretos que figuren en los papeles de trabajo y que les permitan ser identificados con facilidad.
- Los hallazgos deben haber sido detectados con criterios de objetividad, equidad y realidad para otorgarles independencia del criterio del auditor.
- Los hallazgos deben ser lo suficientemente convincentes para que sean comprensibles y coherentes para otras personas que no hayan participado en el proceso de auditoría.
- Además, los hallazgos deben estar basados en una labor y trabajo profundos y extensos que respalden las conclusiones y recomendaciones formuladas a partir de estos.

En resumen, los requisitos de los hallazgos de auditoría se mencionan en la tabla siguiente.

Importancia relativa
Basados en hechos y evidencias precisas
Objetivos
Convincentes
Basados en un trabajo suficiente

Como se puede comprobar, estos requisitos son subjetivos y están sujetos a interpretaciones. Los términos de "importancia", "precisión", "convincientes", etc., de estos requisitos son de difícil definición concreta y requerirán de justificaciones lo suficientemente firmes para que los hallazgos obtenidos sean firmes y confiables y no lleven a conclusiones erróneas.

## **8.2.- Pasos a seguir en el desarrollo de hallazgos**

Una vez detectado el hallazgo, el auditor deberá desarrollarlo de modo que se obtengan todos los aspectos importantes del problema. Esta fase de desarrollo estará formada por las siguientes tareas o pasos:

1. Identificación de la condición o asuntos deficientes o debilidades del sistema de información según los criterios aceptables definidos.
2. Identificación de los responsables respecto a las operaciones implicadas en el hallazgo.
3. Verificación de la causa o causas de la deficiencia detectada.
4. Determinación de si la deficiencia es un caso aislado o una condición generalizada y difundida.
5. Determinación de la relevancia y consecuencias de la deficiencia.
6. Entrevista con los interesados que puedan estar afectados con el hallazgo para obtener datos adicionales.
7. Determinación de las conclusiones de auditoría obtenidas por el análisis de la evidencia a raíz del hallazgo.
8. Definición de las acciones correctivas y/o recomendaciones que subsanen la deficiencia detectada.

## **9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES**

Los hallazgos son una serie de hechos que han sido detectados con el análisis y la evaluación de los documentos, procesos, actividades, entrevistas, etc., de todas las partes que integran el sistema de información auditado.

En términos de auditoría, se consideran desviaciones los incumplimientos de los requisitos de acreditación detectados por la observación de los hallazgos detectados en la auditoría.

Los hallazgos de auditoría que manifiestan debilidades del sistema auditado se pueden clasificar en:

- **Oportunidades de mejora:** no son fallos detectados en sí, son recomendaciones del auditor para mejorar la eficiencia y eficacia del sistema de información auditado.
- **Observaciones:** aspectos de requisitos que podrían mejorarse, pero que no requieren una actuación inmediata.
- **No conformidades:** se detectan no conformidades cuando se encuentra algún incumplimiento de un requisito definido en la auditoría. Requieren una actuación inmediata en cuanto son detectadas.

La clasificación de los hallazgos en no conformidades, observaciones u oportunidades de mejora deberá realizarse teniendo en cuenta una serie de criterios comunes:

- Un hallazgo se clasificará como no conformidad cuando:
  - Se trate de fallos generales del sistema.
  - Se detecte la ausencia de algún elemento importante para el sistema de información.
  - Se detecte un conjunto de varias observaciones que, vistas de un modo aislado, no son importantes, pero que en su detección global pueden desembocar en fallos más relevantes.
- Se considerarán observaciones aquellos hallazgos en que:
  - Se detecten fallos ocasionales, aislados, que no se produzcan con periodicidad.
  - Se detecten fallos cuya resolución sea fácil o rápida.
  - Se detecten incumplimientos parciales de los requisitos definidos en la auditoría.
- Serán oportunidades de mejora:
  - Las recomendaciones del auditor que, en caso de no aplicarlas, no provoquen debilidades o fallos en el sistema.
  - Las recomendaciones que estén basadas en el juicio y la experiencia del auditor.

La clasificación de los hallazgos no es un proceso exacto; siempre está la posibilidad de no tener clara su categorización debido a la falta de información suficiente para conocer la gravedad exacta de la debilidad detectada.

**Nota**

Cuando debe tomarse la decisión sobre la clasificación de un hallazgo como no conformidad u observación, siempre es recomendable ser prudente y clasificarla como no conformidad para darle prioridad a su análisis y corrección.

La dificultad de aplicar un criterio exacto para clasificar los hallazgos hace necesario que el auditor emita juicios lo más objetivos posibles basados en sus experiencias anteriores que le permitan respaldar sus decisiones de categorización y de otorgamiento de prioridades.

## **10. RELACIÓN DE LAS NORMATIVAS Y METODOLOGÍAS RELACIONADAS CON LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMÚNMENTE ACEPTADAS**

El desarrollo de una auditoría informática se basa en la aplicación de una serie de normas y metodologías comúnmente aceptadas que permiten al auditor realizar sus tareas dentro de unos criterios de calidad.

En cuanto a las metodologías de la auditoría de sistemas, cabe destacar dos fundamentales:

- **Metodología tradicional:** en la que el auditor se encarga sobre todo de revisar los controles del sistema, ayudándose de una lista de control que incluirá varias preguntas pendientes de verificar. La evaluación del sistema consistirá en identificar y verificar una serie de controles establecidos o estandarizados previamente.
- **Metodología basada en la evaluación de riesgos:** en este caso, el auditor no hace un chequeo simple, sino que hace evaluaciones de los riesgos potenciales existentes, bien por la ausencia de controles bien por la deficiencia del sistema. Aquí, el auditor deberá verificar y cuantificar los riesgos para conocer el grado de confiabilidad del sistema, atendiendo a la exactitud y a la integridad de su información.

### 10.1.-Normativas relacionadas con la auditoría de sistemas comúnmente aceptadas

Las normas o normativas de auditoría son los requisitos mínimos de calidad que deben cumplir tanto el auditor en el trabajo que realiza como la información obtenida a raíz de dicho trabajo.

De este modo, la mayoría de organismos encargados de elaborar normativas sobre auditoría las clasifican en tres apartados:

- **Normas personales:** estas normas hacen referencia a las características, conocimientos, experiencia y ética que los auditores deben poseer para poder desarrollar correctamente las tareas de auditoría. El auditor debe ser una persona independiente del área a auditar y debe estar debidamente formado para desarrollar sus tareas con rigor y seriedad.  
Nota: Dentro de las normas personales, se encuentran el código deontológico y el código ético de los auditores mencionados al inicio del capítulo.
- **Normas técnicas de ejecución el trabajo:** todas aquellas normas referentes a la planificación, métodos y procedimientos necesarios para que la auditoría termine con éxito. También se incluye la designación de papeles y responsabilidades dentro del equipo auditor.
- **Normas de información o de elaboración de informes:** normas que debe cumplir el auditor para que el análisis de resultado, y su reflejo en el informe de auditoría final, se elabore de un modo correcto. Los informes de auditoría deberán ajustarse a los Principios y Normas de Auditoría Informática Generalmente Aceptados (NAIGA), principios elaborados por la Electronic Data Processing Auditors Foundation (EDPAF).

#### Nota

El informe de auditoría es el instrumento que utilizan los auditores para comunicar a los responsables las debilidades detectadas, el alcance de estas, las conclusiones y las recomendaciones obtenidas por la realización de la auditoría.



## **11. RESUMEN**

La auditoría informática consiste en el análisis exhaustivo de los sistemas de información de una organización con la finalidad de detectar, identificar y describir las distintas vulnerabilidades que puedan presentarse.

Para que la auditoría se lleve a cabo satisfactoriamente, es de vital importancia la figura del auditor, que debe actuar conforme a un código deontológico y un código ético para que las actividades se desarrollen con objetividad e independencia. No es necesario que el auditor sea una sola persona, todo lo contrario, se recomienda que exista un equipo auditor en el que cada uno de los miembros esté especializado en áreas distintas de la auditoría para que ejecuten sus tareas de un modo complementario y así aumentar la calidad del informe elaborado.

Una vez elegido el equipo auditor, se podrá empezar a planificar la auditoría teniendo en cuenta la necesidad de obtener pruebas sustantivas y pruebas de cumplimiento a través del análisis de los hallazgos (debilidades del sistema auditado detectadas) obtenidas gracias a los conocimientos y la experiencia del auditor y a las herramientas de auditoría utilizadas, que añadirán precisión y exactitud a los resultados obtenidos.

Los hallazgos, para ser considerados como tales, deberán cumplir con una serie de requisitos básicos y se categorizarán como observaciones, no conformidades u oportunidades de mejora según su gravedad y alcance, dando prioridad a aquellos hallazgos que afecten al sistema en general y cuyos daños puedan ser graves.

Todos estos procedimientos y tareas deberán cumplir una serie de criterios comunes y deberán realizarse mediante unas normativas y metodologías comúnmente aceptadas relacionadas con la auditoría de sistemas de información, que den fiabilidad y respaldo profesional a las técnicas y herramientas utilizadas y garanticen el éxito de la auditoría.

## CAPÍTULO 2 APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

### 1. INTRODUCCIÓN

La evolución de las tecnologías de la información ha provocado un aumento de la circulación de información a nivel nacional e incluso internacional.

Teniendo en cuenta que parte de esta información puede contener datos de carácter personal referentes a la intimidad de las personas, fue necesario el establecimiento de normativas que ofrecieran protección a las personas físicas en cuanto a la difusión de sus datos personales.

A pesar de haber varias normativas que protegían estos datos, han tenido que hacerse actualizaciones y modificaciones para adaptarlas a la situación actual en la que la tecnología es el soporte fundamental de la información.

Por ello, se han ido desarrollando una serie de leyes, reglamentos y directrices europeas que garantizan que todo ente y organización que trate datos de carácter personal realice estos tratamientos adecuadamente y que los titulares de estos datos puedan conocer en todo momento el uso que se está haciendo de ellos.

Debido a la relevancia de esta materia, en este capítulo se irán analizando las distintas normativas nacionales e internacionales vigentes referentes a la protección de datos de carácter personal y a los derechos de los interesados.

### 2. PRINCIPIOS DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

La protección de datos de carácter personal forma parte de uno de los derechos fundamentales de las personas y consiste fundamentalmente en la capacidad de estas de decidir sobre la utilización de sus datos personales.

Las personas deben tener conocimiento y control de lo que hacen otras personas o entidades con sus datos personales a fin de respetar los derechos reflejados en la Constitución española sobre la intimidad y las libertades públicas. En España, la protección de estos datos se garantiza con la Ley 15/1999 de Protección de Datos de Carácter Personal (LOPD) y su reglamento de desarrollo.

#### Nota

Aunque la información legal sobre la protección de datos personales se encuentra en la LOPD, se reflejaron medidas adicionales en su reglamento de desarrollo (Real Decreto 1720/2007), que derogó otros reglamentos que se habían quedado obsoletos por el avance de las tecnologías de la información.

Aparte de las medidas legales de carácter nacional, también existen directivas comunitarias (que se comentarán más adelante) que añaden seguridad al tratamiento de los datos de carácter personal.

### 2.1.- Conceptos principales de la protección de datos

Antes de comentar más detalladamente la normativa y los principios generales de la protección de datos personales, es vital conocer una serie de conceptos fundamentales definidos en la LOPD:

- **Datos de carácter personal:** cualquier tipo de dato que concierna a las personas físicas identificadas o identificables.
- **Fichero:** conjunto organizado de datos personales, independiente de cómo se haya realizado su creación, almacenamiento, organización y acceso.
- **Tratamiento de datos:** conjunto de operaciones (automatizadas o no) con las que se pueda recoger, grabar, conservar, elaborar, modificar, bloquear y cancelar datos, además de aquellas cesiones de datos que deriven de comunicaciones, consultas, interconexiones y transferencias.
- **Responsable del fichero o tratamiento:** persona (tanto física como jurídica) que tiene capacidad de decisión sobre la finalidad, el contenido y el uso de los datos.
- **Interesado o afectado:** persona física cuyos datos han sido o pueden ser tratados.
- **Procedimiento de disociación:** tratamiento de datos de carácter personal con el fin de aislar la información del interesado que se obtenga de ellos.  
Nota: El procedimiento de disociación permite tratar datos personales del interesado (edad, localidad de residencia, etc.) sin que este sea identificado para garantizar su confidencialidad.
- **Encargado del tratamiento:** persona física o jurídica, autoridad pública, servicio u otros organismos (solos o conjuntamente con otros) que traten datos personales por cuenta del responsable del tratamiento.
- **Consentimiento del interesado:** cualquier manifestación de voluntad libre, inequívoca, específica e informada con la que el interesado consiente el tratamiento de sus datos personales.

#### Importante

El interesado debe dar su consentimiento conociendo claramente el uso específico de sus datos personales. En caso contrario, el consentimiento no será válido.

- **Cesión o comunicación de datos:** cualquier revelación de datos que se realice a otras personas distintas del interesado.

- **Fuentes accesibles al público:** ficheros que pueden ser consultados por cualquier persona (exceptuando que estén limitados por alguna norma limitativa) sin más exigencia que el abono de una contraprestación. Se considerarán fuentes accesibles al público exclusivamente las siguientes:
  - Censo promocional.
  - Repertorios telefónicos (según lo establecido en su normativa específica).
  - Diarios y boletines oficiales.
  - Medios de comunicación.
  - Listas de personas de ciertos grupos profesionales que solo contengan información sobre:
    - Nombre.
    - Título.
    - Profesión.
    - Actividad.
    - Grado académico.
    - Dirección.
    - Indicación de su pertenencia al grupo.

**Nota**

En el caso de que las listas de profesionales contengan algún otro dato que no sea de los indicados anteriormente, ya no será fuente de acceso público y no podrá ser consultadas libremente; deberá someterse a la normativa específica de datos personales de la LOPD.

**2.2.- Principios de protección de datos de carácter personal**

Debido a la especial protección a la que se deben someter los datos de carácter personal, sus medidas y métodos de protección deben establecerse atendiendo a una serie de principios mencionados a continuación.

**Principio de calidad**

Solo podrán recogerse para su tratamiento aquellos datos personales que sean adecuados, pertinentes y no excesivos según el ámbito y finalidades para las que se obtengan.

En ningún momento los datos personales se podrán utilizar para otros fines distintos a los que definieron en el momento de su obtención. La única utilización compatible distinta a la finalidad original es la utilización de los datos personales con fines históricos, estadísticos o científicos.

Los datos deberán cancelarse cuando dejen de ser necesarios o pertinentes para la finalidad por la que se recabaron.

### **Principio de información**

Los interesados a los que se les solicite cualquier tipo de dato personal deberán ser informados expresa, precisa e inequívocamente sobre los aspectos siguientes:

- La existencia de un fichero o tratamiento de datos personales, junto con su finalidad y destinatarios.
- El carácter obligatorio o facultativo de responder a cada pregunta que le sea planteada.
- Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- Posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).
- La identidad y dirección del responsable del tratamiento o de su representante legalmente establecido.

#### **Importante**

Los derechos del interesado de acceso, rectificación, cancelación y oposición, también llamados derechos ARCO, deben tenerse siempre en mente cuando se tratan datos de carácter personal, ya que la LOPD y su reglamento de desarrollo los toman en consideración a lo largo de toda la disposición legal.

### **Principio de consentimiento del afectado**

El consentimiento inequívoco del interesado es requisito indispensable para poder efectuar el tratamiento de sus datos personales. No obstante, se establecen las excepciones siguientes:

- Cuando se disponga otra cosa por ley.
- Cuando los datos personales sean recogidos para las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- Cuando los datos sean referidos a las partes de un contrato o precontrato y sean necesarias para su cumplimiento o mantenimiento.
- Cuando el tratamiento de los datos se realice con el fin de proteger un interés vital del interesado.
- Cuando los datos aparezcan en fuentes accesibles al público.

En el caso de no ser necesario el consentimiento del afectado por las excepciones mencionadas arriba, el interesado siempre podrá oponerse a su tratamiento cuando haya motivos fundados y legítimos relacionados con alguna situación personal concreta.

**Datos especialmente protegidos**

Son datos especialmente protegidos aquellos que se refieran a la ideología, religión o creencias del afectado, teniendo en cuenta que:

- Bajo ningún concepto nadie puede ser obligado a declarar sobre este tipo de datos.
- El interesado debe ser advertido de su derecho a no declarar sobre datos de este carácter.
- Solo se pueden tratar con el consentimiento expreso y escrito del afectado.
- No pueden crearse ficheros con la finalidad exclusiva de almacenar este tipo de datos.

**Datos relativos a la salud**

Las instituciones, los centros sanitarios públicos y privados y los profesionales correspondientes solo podrán tratar datos personales relativos a la salud del afectado de aquellas personas que acudan a ellos o que deban ser tratadas en los mismos.

**Seguridad de los datos**

El responsable del fichero y/o el encargado del tratamiento deberán adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y se eviten problemas de alteración, pérdida, tratamiento o acceso no autorizado a los mismos.

**Nota**

Las medidas de seguridad para evitar alteraciones y accesos no autorizados a datos personales se tomarán siempre atendiendo a la naturaleza de los datos almacenados, los riesgos a los que están expuestos y la tecnología disponible.

**Deber de secreto**

Tanto el responsable del fichero como todos los que formen parte del tratamiento de datos personales están obligados a someterse al secreto profesional de dichos datos, aun cuando ya se hayan agotado sus relaciones con el titular del fichero o con su responsable.

**Principio de comunicación de datos**

Los datos de carácter personal tratados solo se podrán comunicar a terceros en las siguientes condiciones:

- Que los datos se comuniquen solo para cumplir las finalidades específicas (indicadas en el momento de su recogida del interesado o del cedente de los datos).
- Que haya consentimiento previo del interesado.
- Que el interesado conozca la identidad del cesionario y de los fines de la cesión de sus datos personales.

### **Principio de acceso a los datos por cuenta de terceros**

El acceso a los datos por cuenta de terceros se produce cuando acceden a los datos usuarios distintos al responsable del tratamiento del fichero.

Este acceso debe definirse específicamente bajo una relación contractual en la que el tercero que trate los datos se convertirá en el encargado del fichero y prestará servicios al responsable original del mismo.

A modo de resumen, en la siguiente tabla se muestran los principios fundamentales de la protección de datos junto con conceptos básicos de su definición.

<b>PRINCIPIOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL</b>	
<b>Principio de calidad</b>	Datos adecuados, pertinentes y no excesivos según su finalidad.
<b>Principio de consentimiento del afectado</b>	Deber información y de consentimiento previo e inequívoco del interesado para poder tratar los datos.
<b>Datos especialmente protegidos</b>	Datos que requieren medidas más estrictas por hacer referencia a la ideología, religión o creencias del interesado.
<b>Datos relativos a la salud</b>	Los datos relativos a salud solo podrán ser utilizados por instituciones sanitarias o profesionales cuando el interesado acuda a ellos o deba ser tratado en estos.
<b>Principio de seguridad de los datos</b>	El responsable del fichero deberá establecer medidas de seguridad suficientes para mantener la integridad de los datos y no sufrir modificaciones no autorizadas.
<b>Principio de deber de secreto</b>	El responsable del fichero y todos los partícipes de su tratamiento deberán someterse obligatoriamente al secreto profesional aunque <i>ya</i> se haya terminado la relación contractual.



PRINCIPIOS DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL	
<b>Principio de comunicación de datos</b>	Condiciones específicas para la cesión de datos personales a terceros.
<b>Principio de acceso a los datos por cuenta de terceros</b>	Relación contractual entre el responsable del tratamiento del fichero y el tercero, convirtiéndose este desde ese momento en encargado del fichero.

### 3. NORMATIVA EUROPEA RECOGIDA EN LA DIRECTIVA 95/46/CE

La directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, se aplica a los tratamientos realizados con medios automatizados (bases de datos informatizada de los pacientes de un médico privado, por ejemplo) y a los datos incluidos en ficheros no automatizados (ficheros en papel).

Esta directiva no se aplicará a aquellos tratamientos de datos que:

- Se realicen por personas físicas con fines particulares exclusivamente.
- No comprendan actividades incluidas en el ámbito de aplicación comunitario (por ejemplo datos referentes a la seguridad nacional de un país).

La finalidad principal de esta directiva es la protección de los derechos y libertades de las personas en relación al tratamiento de datos personales y está concretada en una serie de principios fundamentales (como en la LOPD).

#### 3.1.- Principios de protección de datos personales de la Directiva 95/46/CE

Del mismo modo que la LOPD, la Directiva europea 95/46/CE también define y regula varios principios con el fin de garantizar una protección adicional de los datos personales, definidos a continuación.

##### **Principio de calidad de los datos**

Los datos personales deben ser tratados lícita y lealmente y deben recogerse exclusivamente con fines determinados, explícitos y legítimos.

Estos datos deben ser exactos y actualizarse cada vez que sufran cualquier modificación.

##### **Principio de legitimación del tratamiento**

El consentimiento inequívoco del interesado será obligatorio para poder tratar datos de carácter personal, salvo las siguientes excepciones:

- La ejecución de un contrato en el que el interesado sea una de las partes implicadas.
- El cumplimiento de requerimientos y obligaciones jurídicas en las que esté sujeto el responsable o el encargado del tratamiento.
- La protección del interés vital del interesado.
- Para fines de interés público.
- El cumplimiento del interés legítimo (manifestado en el momento de la obtención de los datos) por parte del responsable del tratamiento.

### **Categorías especiales de tratamiento**

Se prohíbe el tratamiento de datos especialmente protegidos que revelen información sobre:

- Origen racial o étnico.
- Opinión política.
- Religión.
- Pertenencia a sindicatos.
- Datos relativos a salud.
- Datos relativos a la sexualidad.

La prohibición del tratamiento de este tipo de datos tiene varias excepciones siempre a favor del titular de los datos.

#### **Nota**

La prohibición del tratamiento de datos referentes a la salud se exceptúa en casos de necesidad para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.

### **Principio de información**

El interesado, en el momento de la obtención de los datos personales, debe ser informado de la identidad del responsable del tratamiento, los fines específicos a los que serán destinados y los destinatarios de estos.

### **Principio de derecho de acceso**

El interesado tiene derecho a solicitar (y recibir) información al responsable del tratamiento sobre:

- La existencia o inexistencia del tratamiento de sus datos.
- Las comunicaciones efectuadas de sus datos objeto de tratamiento.

Además, tendrá derecho a solicitar la modificación, cancelación y bloqueo de los datos en los que su tratamiento no esté ajustado adecuadamente a la directiva 95/46/CE por inexactitud o por estar incompletos los datos sujetos al tratamiento.

### **Principio de oposición**

El interesado podrá oponerse al tratamiento de sus datos por razones legítimas. También tendrá derecho a oponerse al tratamiento de sus datos cuando se destinen a fines prospectivos.

Este también tendrá derecho a ser informado previamente de la comunicación de sus datos con fines prospectivos y podrá oponerse a dicha cesión.

### **Principio de seguridad**

El encargado o responsable del tratamiento de los datos deberá implantar las medidas de seguridad necesarias que garanticen su confidencialidad e impidan su alteración o acceso no autorizado.

### **Principio de notificación**

El responsable del tratamiento debe notificar previamente el inicio del tratamiento de datos a la autoridad de control nacional.

En ese momento, la autoridad de control nacional deberá estudiar los posibles riesgos del tratamiento respecto a los derechos de los interesados.

Esta autoridad también deberá publicar los tratamientos efectuados, además de llevar un registro de todos los tratamientos que les han sido notificados.

#### **Nota**

La autoridad de control nacional en materia de protección de datos de carácter personal en España es la Agencia Española de Protección de Datos o AEPD.

Varios de los principios mencionados, concretamente los referentes a la calidad de los datos, la información del interesado, el derecho de acceso y la publicidad de los tratamientos, podrán limitarse cuando se deban salvaguardar la seguridad del Estado, la defensa y la seguridad pública, la represión de infracciones penales, los intereses económicos importantes de algún Estado miembro de la Unión Europea o de la UE en su conjunto o la misma protección del interesado .

Según el principio de legitimidad del tratamiento, será necesario el consentimiento explícito del titular de los datos para poderlos tratar.

Sin embargo, en el mismo principio se establece una excepción en la que se indica que no será necesario el consentimiento en la ejecución de un contrato en la que una de las partes sea el titular de los datos.

En este caso, hay un contrato de alquiler y se necesitan tratar los datos para unas gestiones descritas en dicho contrato, por lo que entra dentro de las excepciones y no será necesario el consentimiento del titular.

#### **4. NORMATIVA NACIONAL RECOGIDA EN EL CÓDIGO PENAL, LEY ORGÁNICA PARA EL TRATAMIENTO AUTOMATIZADO DE DATOS (LORTAD), LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD) Y REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (R. D. 1720/2007)**

Además de las normativas europeas, la legislación española también ofrece una especial protección a los datos de carácter personal. Esta protección se encuentra reflejada en varias normativas:

- Código penal.
- Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD).
- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).
- Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (LOPD 1720/2007).

En los siguientes apartados, se irán describiendo los principales detalles relacionados con la protección de datos personales en cada normativa.

##### **4.1.- La protección de datos personales en el Código Penal**

La protección de datos personales en el Código penal se encuentra reflejada específicamente en su artículo 197, que trata sobre el delito de apoderamiento.

En este artículo, se definen penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses a quien se apodere, utilice o modifique sin consentimiento y en perjuicio de un tercero datos de carácter personal registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado.

Las mismas penas recaen sobre los que accedan sin autorización a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Además, se condena con distintas penas a quienes:

- Accedan a sistemas informáticos con datos personales en contra de la voluntad del que tenga el legítimo derecho de excluirlo.
- Revelen, difundan o cedan a terceros datos, hechos descubiertos o imágenes captadas por el acceso a los sistemas informáticos mencionados anteriormente.

Las penas serán mayores en ciertas circunstancias especiales:

- Si los que realizan el delito son las personas encargadas o responsables de los ficheros.

- Si los datos personales revelan información sobre la ideología, religión, creencias, salud, origen racial o vida sexual.
- Si los datos personales afectan a un menor de edad o a un incapaz.
- Si el delito se comete con fines lucrativos.
- Si el delito se comete dentro de una organización o grupo criminales.

**Importante**

Si los que infringen los preceptos del Código penal del artículo 197 son funcionarios públicos o autoridades, pueden incurrir en penas superiores, además de llegar a ser inhabilitados por tiempo de 6 a 12 años.

**4.2.- Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD)**

La Ley Orgánica para el Tratamiento Automatizado de Datos o LORTAD (5/1992) fue la primera norma en materia de protección de datos aprobada en España.

En 1999, esta norma fue derogada por la actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) a raíz de los preceptos definidos en la Directiva 95/46 del Parlamento europeo, en los que se pretende proteger a las personas físicas en cuanto a tratamiento de datos personales y a su libre circulación.

En la LORTAD ya se fijan y definen los principios relativos a los siguientes aspectos:

- Tratamiento de datos personales.
- Calidad.
- Información.
- Consentimiento.
- Datos especialmente protegidos.
- Datos relativos a la salud.
- Deber de secreto.
- Seguridad de los datos personales.
- Cesión de datos personales.

También se formulan artículos sobre parte de los derechos ARCO (derechos de acceso, rectificación y cancelación de los datos).

**Nota**

El derecho de oposición y la figura del encargado del tratamiento no están reflejados en la LORTAD, sino que se definirán en la LOPD por seguimiento de las directrices europeas.

#### 4.3.- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), Ley Orgánica 15/1999, fue redactada a raíz de lo establecido en la Directiva europea 9 5/46/CEE, mencionada anteriormente, y derogó a la antigua Ley Orgánica de Tratamiento Automatizado de Datos (LORTAD).

La LOPD tiene su ámbito de aplicación en los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a su utilización posterior por los sectores público y privado.

Esta ley está estructurada en siete títulos y 49 artículos, resumidos en la tabla siguiente.

CONTENIDO DE LA LOPD	
Título	Descripción
Título I: Disposiciones generales	Ámbito de aplicación y definiciones principales.
Título II: Principios de la protección de datos	Principios referentes a la protección de datos personales definidos en el apartado 2.2.
Título III: Derechos de las personas	Definición de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición de los datos).
Título IV: Disposiciones sectoriales	Protección de los ficheros de titularidad pública y de los de titularidad privada.
Título V: Movimiento internacional de datos	Normativa relacionada con el movimiento de datos personales fuera del territorio nacional (tanto Unión Europea como otros territorios).
Título VI: Agencia de Protección de Datos	Definición y funciones principales del organismo dedicado a la protección de datos personales: la Agencia de Protección de Datos.
Título VII: Infracciones y sanciones	Calificación, tipificación y descripción de sanciones por infracciones relacionadas con los datos de carácter personal.

#### 4.4.- Reglamento de desarrollo de la LOPD (R. D. 1720/2007)

En 2008 entró en vigor el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) con la finalidad de establecer medidas de protección de datos personales referentes al derecho de la intimidad.

Se elaboró y aprobó, no para repetir los preceptos de la LOPD, sino que su redacción debe considerarse como un desarrollo de la misma para su mayor comprensión y para resolver las posibles dudas de interpretación. También se pretende añadir una visión más práctica a los conceptos definidos en la LOPD.

Como novedad principal, se establece la obligación de las empresas de implantar medidas para una adecuada protección de datos personales sobre todo en los sistemas informáticos, soportes de almacenamiento, procedimientos operativos, etc. A raíz del reglamento de desarrollo, todas las empresas deben adecuar el tratamiento de datos personales y las medidas de seguridad establecidas en este para poder cumplir los requerimientos legales establecidos.

La estructura del R. D. 1720/2007 se distribuye en 9 títulos y 158 artículos, resumidos en la siguiente tabla.

<b>CONTENIDO DE LA LOPD</b>	
<b>Título</b>	<b>Descripción</b>
Título I: Disposiciones generales	Ámbito de aplicación y definiciones principales.
Título II: Principios de la protección de datos	Ampliación de la definición de los principios referentes a la protección de datos personales definidos en el apartado 2.2.
Título III: Derechos de las personas	Definición y desarrollo de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición de los datos).
Título IV: Disposiciones aplicables a determinados ficheros de titularidad privada	Tratamiento de los ficheros de titularidad privada para actividades de publicidad y prospección comercial.
Título V: Obligaciones previas al tratamiento de datos	Definición del procedimiento de notificación e inscripción de ficheros de titularidad pública y privada.
Título VI: Transferencias internacionales de datos	Movimiento de datos fuera del territorio nacional, diferenciando entre los países con un nivel adecuado de protección de datos y los que no.
Título VII: Códigos tipo	Regulación de los códigos deontológicos y la ética profesional a seguir por las empresas y organizaciones.
Título VIII: De las medidas de seguridad en el tratamiento de datos	Medidas de seguridad aplicables a los ficheros tanto automatizados como no automatizados.
Título IX: Procedimientos tramitados por la Agencia Española de Protección de Datos	Desarrollo de las funciones y procedimientos (tramitación, plazos, etc.) que tramita la AEPD.

## **5. IDENTIFICACIÓN Y REGISTRO DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL UTILIZADOS POR LA ORGANIZACIÓN**

Todas las empresas y organizaciones están obligadas a cumplir los requerimientos legales de la Ley de Protección de Datos de Carácter Personal, siempre que en su actividad recaben datos personales.

Para cumplir con esta normativa, es fundamental conocer exactamente qué son los datos de carácter personal: cualquier tipo de dato que haga referencia a una persona física.

De este modo, la empresa deberá tener especial cuidado con los datos de todos los agentes físicos de los cuales necesite datos personales (principalmente, sus clientes, proveedores y empleados).

### **Ejemplo**

En el momento en el que la empresa contrate a un trabajador y necesite sus datos personales (edad, nombre completo, dirección, teléfono, número de cuenta bancaria, número de la seguridad social, etc.), deberá informar de dicha obtención de datos y de su finalidad exclusiva como trabajador de la organización.

### **5.1.- Proceso de implantación de la LOPD**

Para que la identificación y el registro de los ficheros con datos personales se lleven a cabo adecuadamente, será necesario seguir un procedimiento de implantación de la LOPD claramente definido.

Las fases de este procedimiento son las siguientes:

1. Identificación de los ficheros de la organización que contengan datos de carácter personal: habrá que identificar todos los ficheros que contengan datos de trabajadores, clientes, proveedores y cualquier otra persona física. Por ejemplo: las fichas con los datos de contacto de los clientes o proveedores, las nóminas de los empleados (contienen su nombre completo, dirección, etc.), el fichero con los correos electrónicos de los empleados, etc.
2. Identificación del nivel de seguridad a aplicar a cada fichero: dependiendo del tipo de datos que contenga el fichero, este requerirá unas medidas de seguridad u otras (que se describirán más adelante).
3. Identificación del responsable o encargado del fichero: debe estar identificado en todo momento para cumplir con el deber de información a los interesados.
4. Confección del documento de seguridad: es un documento interno de la organización que debe contener todos los aspectos referentes a las medidas, normas, procedimientos, reglas y estándares de esta para garantizar la seguridad de sus datos.

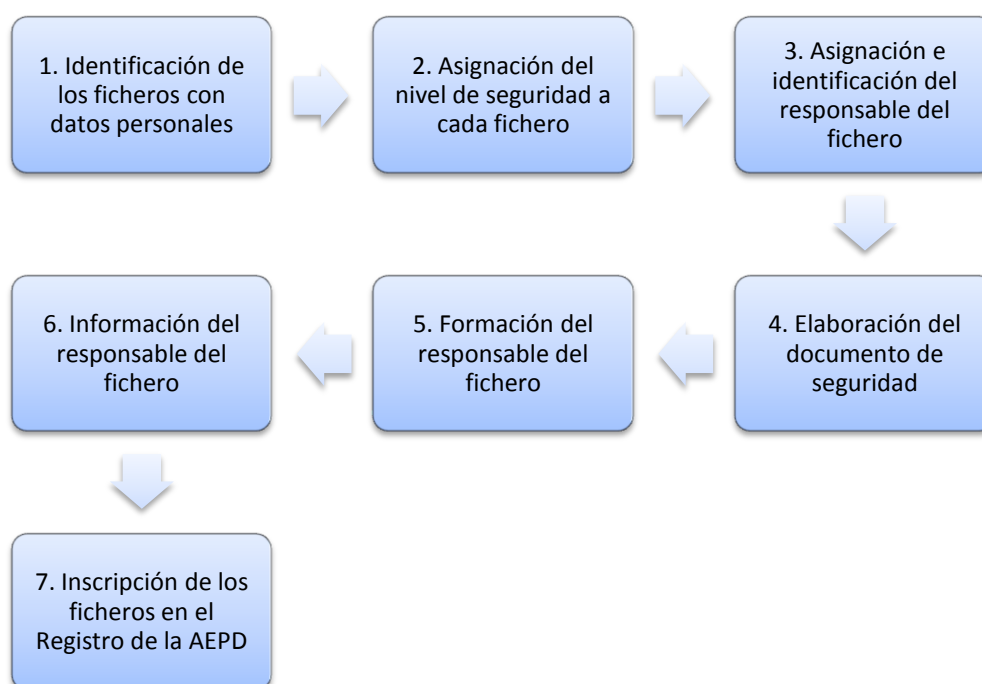
**Nota:** La información sobre el documento de seguridad y los requisitos para elaborarlo está contenida en el reglamento de desarrollo de la LOPD (R. D. 1720/2007). Este deberá ser elaborado por el responsable del fichero o por el encargado del tratamiento.



5. Impartir formación específica al responsable del fichero para cumplir adecuadamente con todos los preceptos de la LOPD y su reglamento de desarrollo.
6. Información a los interesados de la existencia de un fichero con sus datos, la finalidad específica de estos y la posibilidad de ejercer los derechos ARCO.
7. Inscripción de los ficheros en el Registro de la AGPD: las organizaciones deben informar a la Agencia Española de Protección de Datos de la existencia de ficheros con datos de carácter personal mediante notificación formal para que lo inscriban en su registro.

Si, además, la empresa dispone de datos cuyo nivel de protección es medio o alto, deberá elaborar auditorías mm1mo cada dos años obligatoriamente y, en caso de que en la auditoría se detecten deficiencias en la protección de datos personales, la organización deberá realizar todas las modificaciones necesarias para recuperar el nivel de protección adecuado y no infringir los preceptos de la LOPD.

En resumen, las fases de implantación de la LOPD que permiten una adecuada identificación y registro de los datos de carácter personal en las organizaciones se muestran en la tabla siguiente.



## **6. EXPLICACIÓN DE LAS MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL RECOGIDAS EN EL REAL DECRETO 1720/2007**

La Ley de Protección de Datos, en su artículo 9, establece el principio de seguridad de los datos, en el que se indica que el responsable del fichero o el encargado del tratamiento deberán implantar las medidas de seguridad, tanto técnicas como organizativas, que garanticen una adecuada protección de los datos en cuanto a su confidencialidad, integridad y disponibilidad.

Las medidas que deberán adoptarse serán distintas en función de la naturaleza de los datos, los riesgos a los que se exponen y el estado de la tecnología en sí.

En caso de incumplimiento de estas medidas de seguridad, se estará incurriendo en una infracción grave, con multas de 40.001 a 300.000 €.

**Nota**

El artículo 44.3.h de la LOPD indica que es infracción grave "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

El reglamento de desarrollo de la LOPD establece los distintos niveles de seguridad de los datos, las obligaciones de los responsables y los requisitos que deben cumplir los ficheros que los contengan.

Los niveles de seguridad de los datos se corresponden con una serie de medidas a aplicar en cada uno de los niveles mostrados en la siguiente tabla.

NIVELES DE SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL	
<b>Medidas de nivel básico</b>	
	Se aplican a cualquier fichero o tratamiento de datos de carácter personal.
<b>Medidas de nivel medio</b>	
	Se aplicarán, además de las medidas de nivel básico, a ficheros que contengan infracción sobre comisión infracciones administrativas o penales, información financiera de solvencia patrimonial y crédito, datos de seguridad social y mutualidades de previsión social, datos de la Administración tributaria, etc.
<b>Medidas de nivel alto</b>	
	Se aplicarán, además de las medidas de nivel básico y medio, a ficheros que contengan datos sobre ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual, además de aquellos que contengan datos recabados sin consentimiento por fines policiales.

El documento de seguridad mencionado anteriormente deberá contener las medidas necesarias y exigibles para garantizar una correcta protección de los datos de carácter personal. Las medidas se

clasifican en las generales, las aplicables al tratamiento de datos automatizado y las aplicables al tratamiento de datos no automatizado.

### **6.1.- Medidas de seguridad generales para todo tipo de ficheros**

En todos los casos, el documento de seguridad contendrá las delegaciones de las funciones del responsable del fichero y todas las autorizaciones emitidas a otras personas, determinando obligatoriamente el período de validez de esta autorización.

Los ficheros de carácter temporal deberán ser eliminados una vez ya no se utilicen para cumplir la finalidad definida inicialmente.

Las medidas de seguridad generales también se clasifican en medidas de nivel básico, medio y alto.

Las medidas de seguridad de nivel básico son:

- Definir las funciones y obligaciones del personal para el tratamiento de los datos, incluyendo todas las autorizaciones y delegaciones establecidas por el responsable del fichero o tratamiento.
- Informar a todo el personal de las normas de seguridad que afecten a sus funciones de un modo comprensible.
- Establecer, documentar e incluir en el documento de seguridad el procedimiento de notificación y gestión de incidencias.
- Limitar el acceso a los usuarios solo a los datos necesarios para llevar a cabo sus funciones.
- Mantener actualizado un registro de los usuarios y perfiles de usuario con los accesos autorizados para cada uno de ellos.
- Establecer los mecanismos que eviten el acceso no autorizado a los documentos.

Estas medidas de seguridad se aplicarán tanto a los ficheros automatizados como a los no automatizados que contengan cualquier tipo de dato de carácter personal.

Las medidas de seguridad de nivel medio son:

- Designar los responsables de seguridad y registrarlos en el documento de seguridad.
- Realizar una auditoría como mínimo bianual de los sistemas de información e instalaciones encargadas del tratamiento y almacenamiento de datos.
- Realizar una auditoría extraordinaria cuando deban realizarse modificaciones extraordinarias en el sistema de tratamiento de los datos.
- Establecer un sistema de registro de las entradas y salidas de soportes o documentos que contengan datos personales.

### **6.2.- Medidas de seguridad para el tratamiento de datos automatizado**

Las medidas de seguridad para el tratamiento de datos automatizado se establecen con la finalidad de garantizar un nivel de protección de dichos datos adecuado en las redes de comunicaciones públicas o privadas.

Las medidas de seguridad de nivel básico son:

- En los soportes con datos personales, se debe poder identificar el tipo de información que contienen, además de estar incluidos en un inventario.
- Solo se puede permitir el acceso a dichos soportes exclusivamente a personal autorizado.
- La salida de soportes, documentos y correos electrónicos con datos personales deberá autorizarse por el responsable del fichero o su autorizado.
- El traslado de los documentos deberá seguir unas medidas de seguridad que eviten el acceso, la pérdida o el robo.
- Los soportes que ya no se utilicen deberán destruirse de modo que nadie pueda acceder a ellos ni recuperar la información que contienen.
- Implantar un sistema de identificación y autenticación inequívoco y personalizado para cada usuario.
- Establecer procedimientos de realización de copias de seguridad y mínimo cada 7 días (o incluso menos en casos de modificaciones importantes de los datos).
- Establecer procedimientos que garanticen la recuperación de los datos.
- El responsable del fichero deberá definir el funcionamiento y la aplicación de los procesos de copia y recuperación de datos.

Las medidas de seguridad básica para ficheros automatizados se dividen en tres grandes bloques: gestión de soportes, identificación y autenticación y procesos de copias de respaldo y recuperación de datos.

Las medidas de nivel medio son:

- Establecer medidas que impidan el acceso reiterado y no autorizado al sistema de información.
- Implantar medidas que restrinjan el acceso a los lugares donde se encuentren los servidores solo al personal autorizado.
- Registrar las recuperaciones de datos. Deberán ser autorizadas por el responsable del fichero.
- Las medidas de nivel alto son:
- La identificación de los soportes no podrá ser comprensible para el personal no autorizado.
- La distribución de los soportes se deberá realizar con mecanismos que impidan el acceso o la manipulación no autorizada. Los datos de los dispositivos que se transporten fuera del área de seguridad deberán estar cifrados.
- Almacenar una copia de seguridad de los datos y de los procedimientos de recuperación fuera de los locales de la organización.
- Elaborar un registro en el que se almacenen los intentos de acceso a los datos y las acciones realizadas por los usuarios en estos. Este registro deberá mantenerse como mínimo durante dos años y deberá ser revisado mensualmente por el responsable de seguridad.
- Las comunicaciones de datos a través de redes públicas o redes inalámbricas deberán realizarse con mecanismos que impidan el acceso o la manipulación de terceros, como el cifrado de datos.

**Definición****Tratamiento de datos automatizado**

Aquel que se realiza con datos almacenados en ficheros y soportes informatizados.

**6.3.- Medidas de seguridad para el tratamiento de datos no automatizado**

El tratamiento de datos no automatizado es aquel en el que no se utiliza ningún medio informático. En este caso, los datos suelen estar almacenados en formato papel. Las medidas especiales para este tipo de tratamiento también se distinguen entre medidas de nivel básico, medio y alto.

Las medidas de seguridad de nivel básico son:

- Garantizar la correcta conservación del archivo de soportes, además de una rápida localización y consulta de los mismos.
- Implantar mecanismos que impidan el acceso y la apertura de los soportes con datos de carácter personal.
- Establecer normas internas para que los que traten soportes con datos personales antes de su almacenamiento custodien correctamente e impidan el acceso de usuarios no autorizados.

Las medidas de seguridad de nivel alto son:

- Los documentos no automatizados y sus soportes deberán estar ubicados en áreas de acceso restringido con puertas de acceso que deben permanecer cerradas cuando no se esté accediendo a la información.
- Las copias de los soportes o documentos se realizarán siempre bajo control del personal autorizado. Las copias que no se vayan a utilizar deberán ser destruidas.
- Elaborar un registro que almacene todos los intentos de acceso a los datos y las acciones realizadas por los usuarios. El registro deberá revisarse mensualmente por el responsable de seguridad, que emitirá un informe del registro.
- Implantar medidas que permitan identificar los accesos a documentos cuando los documentos puedan ser utilizados por varios usuarios.
- Implantar medidas que impidan el acceso o manipulación de los datos cuando se produzcan traslados de sus soportes o documentos.

**7. GUÍA PARA LA REALIZACIÓN DE LA AUDITORÍA BIENAL OBLIGATORIA DE LA LEY ORGÁNICA 15/1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

La LOPD 15/1999 obliga a las organizaciones y entidades que traten ficheros de nivel medio o alto a realizar una auditoría mínimo cada dos años. En los otros casos, no hay ninguna obligación

respecto a auditorías, pero se recomienda realizar alguna periódicamente para conocer el estado y el grado de cumplimiento de las obligaciones definidas en esta normativa.

Esta auditoría puede ser interna o externa (realizada por la misma organización o encargarla a una empresa externa) y deberá realizarse antes de transcurrir los dos años de plazo en caso de modificaciones sustanciales del sistema de información para comprobar si las medidas de seguridad siguen siendo adecuadas y eficaces.

Para llevarla a cabo, deberán seguirse una serie de pasos determinados:

1. Determinación del alcance de la auditoría: en esta fase se identificarán los ficheros que incluyan datos de carácter personal que serán objeto de la auditoría. También se deberán identificar los tratamientos realizados, los sistemas de tratamiento, los procedimientos en materia de tratamiento y protección de datos personales, etc.
2. Planificación de recursos: deberán determinarse los recursos que sean necesarios para poder realizar la auditoría. Por ejemplo: las fuentes de información utilizada, la ubicación o ubicaciones de los ficheros, las instalaciones de la organización, los equipos y dispositivos que almacenan los datos automatizados, etc.
3. Obtención de los datos a auditar: se deberá proceder a la recogida de los datos que serán evaluados en el proceso de auditoría mediante una serie de técnicas y herramientas, destacadas en la tabla siguiente.

MÉTODOS DE OBTENCIÓN DE DATOS PARA LA AUDITORÍA BIENAL
Elaboración de una relación de los ficheros con datos personales, incluyendo su estructura y contenido específico.
Obtención de la información referente a las políticas de seguridad y a los procedimientos establecidos en la organización. Por ejemplo: procedimiento de copias de respaldo, restauración de datos, autorizaciones, eliminación de soportes, sistemas de autenticación, etc.
Examen del documento de seguridad y de las auditorías realizadas anteriormente.
Revisión del diseño físico y lógico de los sistemas de información (ubicación, dispositivos utilizados, sistema de redes y comunicaciones, etc.).
Elaboración de una relación de los usuarios con sus accesos autorizados y sus funciones específicas.
Elaboración y mantenimiento de un inventario de los soportes con datos personales y de los registros de entrada y salida de los mismos.
Entrevistas a los usuarios, responsables de seguridad, encargados de tratamiento y a todos los demás implicados en el tratamiento de los datos personales.

**Importante**

Los datos a recabar por las organizaciones para cumplir con los requisitos de la auditoría bienal no son solo los especificados en la tabla. Cada organización deberá adaptar su estructura y procedimientos y recabar toda la información que considere importante para la seguridad de los datos de carácter personal.

4. Evaluación de las pruebas: una vez obtenidos los datos, deberán evaluarse y realizar comprobaciones para comprobar si se cumplen los requisitos de la LOPD y su reglamento de desarrollo y detectar posibles deficiencias en la seguridad de los datos personales.

En caso de detectar deficiencias, deberán establecerse medidas correctivas que permitan recuperar un nivel de seguridad adecuado y modificar el documento de seguridad, incluyendo los cambios y medidas implantados.

**8. RESUMEN**

La protección de datos de carácter personal forma parte de los derechos fundamentales de las personas y les ofrece la posibilidad de poder decidir en todo momento la utilización de sus datos personales.

Esta protección se ha formalizado mediante una serie de normativas y directrices, tanto nacionales como europeas, de obligatorio cumplimiento para cualquier organización.

En cuanto a normativa nacional, la LORTAD (Ley Orgánica para el Tratamiento Automatizado de Datos) fue la primera norma en materia de protección de datos aprobada en el país. Su intención era proteger a las personas físicas en cuanto a tratamientos de datos y a su libre circulación.

Debido a la evolución de las tecnologías de la información y a la utilización de soportes informáticos para almacenar datos personales, se derogó la LORTAD y se aprobó la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD 15/1999) y su Reglamento de desarrollo (R.D. 1720/2007) para cubrir los vacíos de la ley anterior e incluir las medidas de seguridad obligatorias para las organizaciones.

En materia internacional, destaca la Directiva 95/46/CE, aprobada por el Parlamento europeo con el fin de proteger a las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación.

Siguiendo los requerimientos legales, las organizaciones establecerán una serie de medidas de seguridad de nivel básico, medio o alto según el tipo de datos que traten, sus riesgos y las tecnologías actuales, y elaborarán un documento de seguridad (en el que se incluirán las medidas y procedimientos de la organización) en el caso de tratar datos con niveles medio y básico.

## **CAPÍTULO 3 ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN**

### **1. INTRODUCCIÓN**

Los sistemas de información de las organizaciones tienen multitud de recursos vulnerables ante ataques de seguridad. Por ello, es necesario que desarrollen estrategias y herramientas que sean capaces de identificar y valorar estos recursos y que, a su vez, puedan dar información sobre los ataques y daños que pueden afectarles.

Las herramientas de gestión de riesgos sirven precisamente para estas funcionalidades: ayudan a identificar los recursos importantes en la organización, los riesgos a los que están sometidos y el daño que pueden sufrir en caso de producirse una amenaza de cualquier tipo.

En este capítulo, se describen las herramientas fundamentales de gestión de riesgo, se facilitan guías de apoyo para poder identificar todos los factores que forman parte de esta y se comentan varias técnicas que permitan a las organizaciones combatir los riesgos y aumentar la seguridad de sus sistemas de información.

### **2. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS**

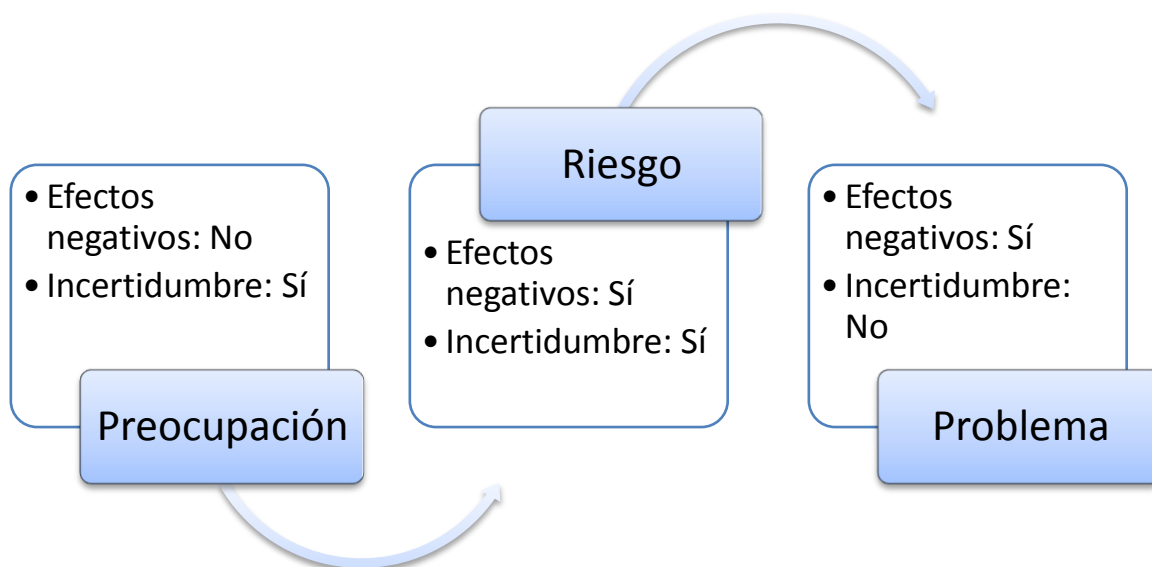
Un riesgo es un evento o conjunto de eventos que puede poner en peligro un proyecto de la organización o que puede impedir su éxito.

La definición de riesgo en sí siempre ha ocasionado grandes debates. Aun así, existe un acuerdo sobre las características comunes que debe tener todo riesgo informático:

- **Incertidumbre:** el evento que caracteriza al riesgo puede ocurrir o no ocurrir, no hay certeza sobre su ocurrencia.
- **Pérdida:** en caso de materializarse el riesgo, habría varias consecuencias negativas para la organización. Si no hay efectos negativos, no hay riesgo en sí. Es bastante común la confusión entre las definiciones de problema, preocupación y riesgo, siendo necesario conocer sus diferencias:
- Una preocupación es una situación sobre la que hay dudas y que deberá ser evaluada como un posible riesgo. No obstante, analizada la preocupación es posible que se determine que no existen efectos negativos y que, por tanto, no se puede considerar riesgo.
- Un problema, sin embargo, es un riesgo que ya se ha materializado. En este caso, no hay incertidumbre, ya que hay certeza sobre su ocurrencia y, por tanto, tampoco se puede considerar riesgo.

En la siguiente tabla, se puede observar con mayor claridad la diferencia entre estos conceptos.





### 2.1.- Conceptos básicos de la gestión de riesgos

La gestión de riesgos se define como el conjunto de procesos desarrollados por una organización con el fin de disminuir la probabilidad y ocurrencia de amenazas y de aumentar la probabilidad y ocurrencia de oportunidades con efectos negativos.

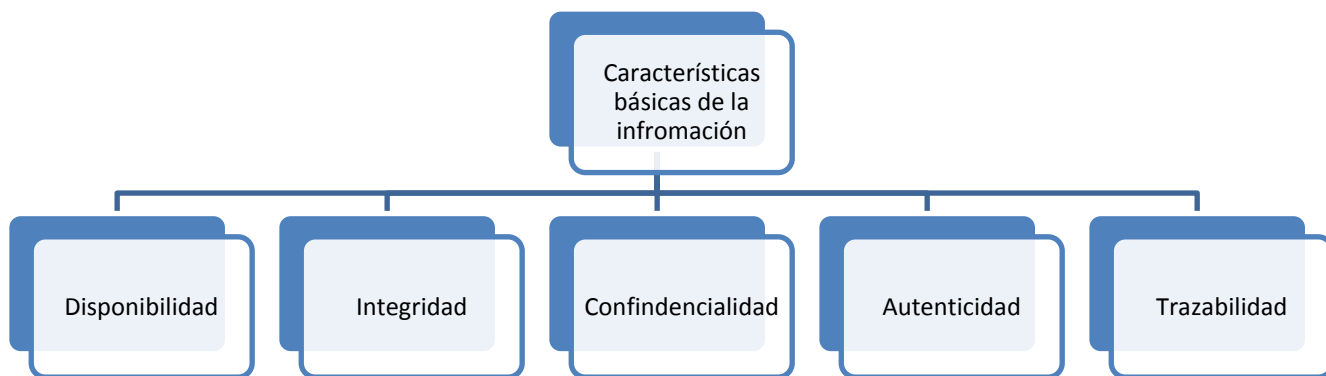
Se trata de una metodología o conjunto de metodologías encaminadas a gestionar correctamente las incertidumbres de una amenaza.

En el ámbito de la gestión de riesgos, entra en juego el concepto de seguridad de la información: la seguridad se define como el conjunto de medidas y capacidades de los sistemas de información para resistir a las amenazas manteniendo la disponibilidad, autenticidad, integridad y confidencialidad de los datos.

De este modo, una correcta gestión de riesgos utilizará unas medidas de seguridad que protejan sus datos e información en cuanto a:

- **Disponibilidad:** la información debe estar disponible a los usuarios siempre que sea necesario. Una carencia de disponibilidad provoca interrupciones de servicio y mermas de calidad.
- **Integridad:** la información debe ser correcta y completa. La seguridad debe impedir que se manipule, corrompa o elimine información sin autorización.
- **Confidencialidad:** la información debe estar disponible solo para los usuarios que estén correctamente autorizados. La seguridad debe encargarse en todo momento de proteger la información ante accesos no autorizados.

- **Autenticidad:** garantía de la fuente de la que proceden los datos. La seguridad de la organización debe asegurar que los datos proceden de sitios seguros sin haber sufrido manipulación alguna.
- **Trazabilidad:** se debe conocer en todo momento quién y cuándo ha realizado cada acción con la información de la información. Esta característica es muy útil para analizar los incidentes y para detectar a los atacantes.



Aparte de los conceptos referentes a las características de la información, para una correcta comprensión de la gestión de riesgos hay que tener claros los siguientes conceptos:

- **Riesgo:** estimación de las probabilidades de que una amenaza se materialice sobre los activos de la organización, causando efectos negativos o pérdidas.
- **Análisis de riesgos:** proceso y metodología utilizados para estimar la magnitud de los riesgos a los que se expone una organización.
- **Tratamiento del riesgo:** procesos realizados para modificar los riesgos de una organización.

## 2.2.- Estándar ISO 31000 de gestión y tratamiento de riesgos

En cuanto a gestión, análisis y tratamiento de riesgos existe un estándar ISO (ISO 31000:2009) que incluye una serie de recomendaciones y actividades para que las organizaciones gestionen sus riesgos de un modo más adecuado y eficaz.

No obstante, aunque sea un estándar, no ofrece certificación, por lo que solo debe ser tomada como una guía en la que encontrar los principios, el marco y el proceso para lograr una gestión de riesgos transparente, sistemática y creíble. A raíz de la ISO31000:2009, las organizaciones deben ser capaces de desarrollar sus propias estrategias de gestión de riesgos.

**Nota**

La norma ISO 31000:2009 no es específica a ningún sector en concreto y puede ser utilizada por cualquier tipo de entidad, pública o privada, y por cualquier tipo de usuario.

**Principios de la ISO 31000**

Para una correcta y efectiva gestión de riesgos, la norma ISO 31000 propone once principios fundamentales a las organizaciones:

- Crear valor: la gestión de los riesgos debe crear valor y mantenerlo.
- Estar integradas en los procesos de la organización: la gestión de riesgos debe ser una actividad integrada dentro de los procesos de la organización y no ser tratada como un proceso aislado.
- La gestión de riesgos debe estar presente en la toma de decisiones de la organización.
- La gestión de riesgos debe tratar explícitamente la incertidumbre: las amenazas y aspectos inciertos deben ser analizados para conocer el origen de su incertidumbre y su posible tratamiento.
- La gestión de riesgos debe ser sistemática, estructurada y utilizarse a su debido tiempo.
- Debe basarse en la mejor información de la que dispone: la gestión de riesgos se debe llevar a cabo tomando en consideración la opinión de profesionales especializados y la experiencia.
- Debe adaptarse a las circunstancias locales y específicas: para una correcta gestión de riesgo, las organizaciones deben tener en cuenta el sector de su actividad y el entorno en el que trabajan.
- Se deben valorar los factores humanos y culturales para conocer la visión de las distintas partes implicadas y que así colaboren con la actividad de la organización.
- La gestión de riesgos debe ser transparente e inclusiva, basándose en la comunicación de las partes implicadas y teniendo en cuenta sus opiniones.
- También debe ser dinámica, iterativa y sensible al cambio: en la gestión de riesgos debe tenerse en cuenta que la organización está en continuo cambio y debe ser capaz de adaptarse a las alteraciones que puedan ocurrir.
- Además, debe facilitar la mejora continua de la organización basada en el aprendizaje, la experiencia y la formación.

**PRINCIPIOS DE LA NORMA ISO 31000: LA GESTIÓN DE RIESGOS:****1. Crea valor.****2. Está integrada en los procesos de la organización.****3. Forma parte de la toma de decisiones.**

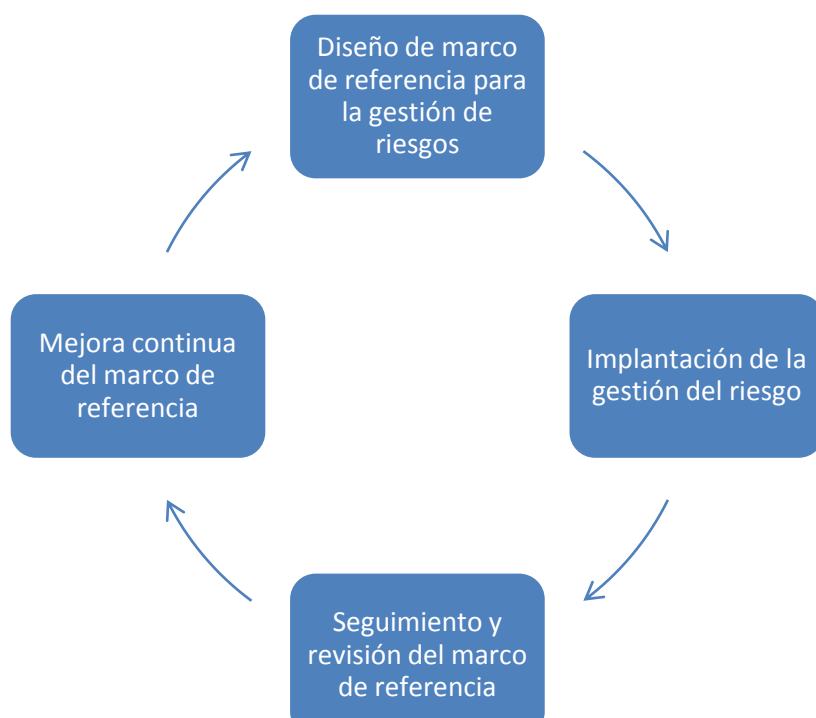
PRINCIPIOS DE LA NORMA ISO 31000: LA GESTIÓN DE RIESGOS:
4. Trata explícitamente la incertidumbre.
5. Es sistemática.
6. Está basada en la mejor información disponible.
7. Está hecha a medida.
8. Tiene en cuenta factores humanos y culturales.
9. Es transparente e inclusiva.
10. Es dinámica, iterativa y sensible al cambio.
11. Facilita la mejora continua de la organización.

### 2.3.- Marco de trabajo para la gestión del riesgo

La norma ISO 31000 también establece un marco de referencia o *framework* para la gestión de riesgos formado por las siguientes actividades:

- Las organizaciones deben diseñar un marco de referencia para la gestión de riesgos que tenga en cuenta sus propias peculiaridades y su entorno.
- Una vez diseñado el marco de referencia, deberán implantar la gestión del riesgo para poder disminuir la probabilidad de amenazas y pérdidas.
- La gestión de riesgos debe ser evaluada y revisada periódicamente para valorar si sigue siendo eficiente y es necesario realizar algún cambio.
- Con estas revisiones periódicas, las organizaciones deben ser capaces de aprender de los fallos detectados y entrar en un proceso de mejora continua que garantice una mejor gestión de riesgos.
- Todas estas actividades y fases deben contar con el apoyo y compromiso de la dirección de la organización para que puedan ser implantadas de modo global en todas sus tareas y procedimientos.

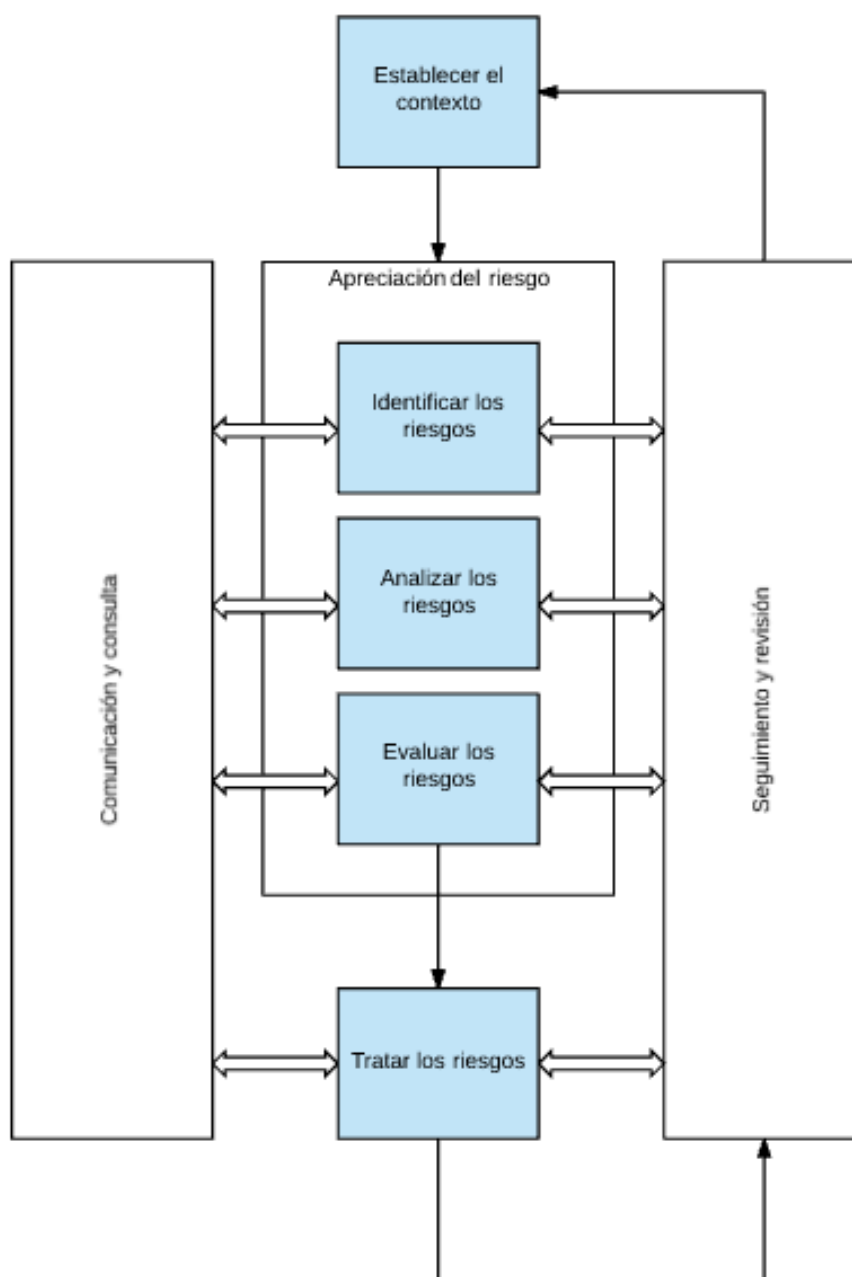
En la tabla imagen, se observa *el framework* de la gestión de riesgos propuesto por la norma ISO 31000.



#### **2.4.- Proceso de gestión del riesgo**

La norma ISO 31000 establece, después de introducir los principios de gestión del riesgo y el marco de trabajo, un proceso de gestión del riesgo con un conjunto de fases y pasos recomendados para que las organizaciones lo adapten e implanten correctamente, consiguiendo mejoras en la efectividad y precisión ante posibles amenazas.

El proceso de gestión de riesgo se puede observar en la tabla siguiente.



El proceso de gestión de riesgos definido por la norma ISO 31000 propone una serie de fases o procesos:

- **Establecimiento del entorno y del contexto:** en un primer momento, deberán analizarse todas las peculiaridades de la organización, del entorno y de sus sistemas de información para desarrollar una estrategia de gestión de riesgos que se adapte a sus necesidades.

- **Fase de apreciación del riesgo:** consiste en una serie de tareas relacionadas con la detección e identificación de los riesgos de una organización para su evaluación y categorización. Dentro de esta fase, se encuentran las subfases siguientes:
  - Identificación del riesgo: una vez detectado el riesgo, habrá que proceder a identificarlo para conocer sus características básicas.
  - Análisis del riesgo: cuando ya se ha identificado el riesgo, será necesario realizar un análisis más profundo y detallado para conocer sus características y comportamientos particulares.
  - Evaluación del riesgo: después de conocer en profundidad el riesgo identificado, se tendrán que evaluar los potenciales daños y efectos negativos que puede ocasionar para determinar su importancia y magnitud.
- **Fase de tratamiento del riesgo:** según lo determinado en el análisis y evaluación del riesgo, se tomarán una serie de decisiones y medidas que minimicen la probabilidad de su ocurrencia y su daño potencial.
- **Monitorización y revisión:** cuando ya se ha decidido e implantado la metodología de detección, análisis, evaluación y tratamiento de riesgos, habrá que monitorizarla lo máximo posible para que se integre en la organización como un proceso automático. Además, requerirá revisiones periódicas para detectar posibles fallos y solucionarlos en el menor tiempo posible. Durante la implantación, también se recomienda ir realizando revisiones que garanticen su desarrollo correcto.
- **Comunicación y consulta:** durante todas las fases de gestión del riesgo, la organización deberá estar en permanente contacto con los distintos agentes y participantes de su sistema de información con una serie de objetivos:
  - Ayudar a establecer el contexto adecuadamente.
  - Garantizar los intereses de las partes interesadas y asegurarse que están bien informadas.
  - Ayudar a asegurar que los riesgos están identificados correctamente.
  - Dar apoyo al sistema de gestión de riesgos.
  - Desarrollar una correcta política de comunicación interna y externa de la organización, para que todos los agentes tengan la posibilidad de consultar los riesgos del sistema de información y sus consecuencias.

### **3. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA**

Para una correcta y completa gestión del riesgo de un sistema de información, hay que prestar atención a los distintos tipos de agentes e incidencias que pueden afectar al flujo de datos. Los más importantes a considerar son las vulnerabilidades o fallos de programa y los programas maliciosos (*software* malicioso).

A continuación, se van describiendo cada uno de ellos, detallando sus particularidades principales.

### **3.1.- Principales tipos de vulnerabilidades/fallos de programa**

Una vulnerabilidad es un fallo de seguridad en un programa o en un sistema de información. No todos los fallos de programas son fallos de seguridad, hay errores que simplemente provocan que funcione incorrectamente o que tenga comportamientos inesperados, sin que ello suponga un riesgo para la información que manejan.

No obstante, las vulnerabilidades son, en numerosas ocasiones, el origen de muchos fallos de seguridad y, por ello, deben tomarse en consideración cuando se planifica la gestión de riesgos del sistema de información.

La variedad de vulnerabilidades y fallos de programa es de lo más extensa y se distingue su tipología atendiendo a sus características especiales.

Entre las vulnerabilidades más importantes, cabe destacar las que se describen a continuación.

#### **Vulnerabilidades de configuración**

Son vulnerabilidades generadas por una mala gestión del *software* por parte del usuario final. No se originan por un fallo del diseño en sí, sino que se originan en el momento en el que el usuario configura el sistema erróneamente.

#### **Nota**

También pueden surgir vulnerabilidades cuando la configuración por defecto del programa contiene fallos y es insegura.

#### **Validación de entrada**

Se trata de una vulnerabilidad que se genera cuando la aplicación no comprueba adecuadamente la entrada de datos que provienen desde el exterior.

#### **Salto de directorio**

Es una vulnerabilidad que se aprovecha de la falta de seguridad de los servicios de red para moverse por los directorios de la aplicación hasta llegar a su directorio raíz.

En caso de sistemas operativos, esta vulnerabilidad puede ocasionar que usuarios no autorizados accedan a su directorio raíz y puedan conectarse a ellos para ejecutar acciones de modo remoto.



### Inyección de comandos en el sistema operativo

La inyección de comandos en el sistema operativo consiste en la capacidad que tiene el usuario para ejecutar comandos en el sistema operativo que puedan poner en peligro su integridad.

#### Nota

La vulnerabilidad referente a la inyección de comandos en el sistema operativo puede encontrarse en varios sistemas operativos como Unix/ Linux o Microsoft Windows.

### Inyección SQL

Se trata de una vulnerabilidad que se localiza en el nivel de base de datos del programa o aplicación. Se produce cuando el filtrado de las variables utilizadas con código SQL no se realiza correctamente.

Al realizarse un filtrado incorrecto, los atacantes pueden inyectar nuevo código SQL para modificar el comportamiento de la aplicación e, incluso, introducir código malicioso en el sistema.

### Error de búfer

Un búfer es un espacio de la memoria de un disco o de un instrumento digital reservada para el almacenamiento de información digital de forma temporal hasta que esta se procese.

Se producen errores de búfer cuando se intentan almacenar datos de forma incontrolada en su espacio (provocando daños en zonas de la aplicación) o cuando la velocidad de entrada de datos en el búfer es inferior a la velocidad de lectura de los mismos (provocando fallos y la detención momentánea de la ejecución de la aplicación).

### Fallo de autenticación

Vulnerabilidad que se origina cuando el programa no puede autenticar correctamente al usuario que intenta acceder en él.

### Error en la gestión de recursos

Este tipo de vulnerabilidad ocurre cuando el fallo de programa permite al usuario no autorizado provocar una gestión deficiente de los recursos del sistema, provocando un consumo excesivo en estos.

Cuando esto sucede, la aplicación suele dejar de responder e interrumpe el servicio.

### Error de diseño

Son vulnerabilidades ocasionadas cuando el programador realiza el diseño de la aplicación con fallos y errores, tanto en el diseño inicial como en su desarrollo posterior.

Estos errores pueden llevar a un mayor riesgo de entrada de atacantes que intenten aprovecharse de los fallos de diseño para introducir código malicioso en la aplicación.

#### Nota

Las vulnerabilidades mencionadas en este apartado son las más relevantes. No obstante, hay que tener en cuenta que no son las únicas y que constantemente se generan nuevos fallos de programa que pueden provocar vulnerabilidades.

### 3.2.- Programas maliciosos y su actualización permanente

Un programa malicioso o *malware* es un tipo de programa diseñado para que usuarios no autorizados accedan a un sistema de información sin autorización de su propietario y producir efectos indeseados en este.

Dentro de estos programas se engloban una gran variedad de *software*: virus, troyanos, gusanos, *spyware*, etc., que se describirán más adelante.

Los programas maliciosos suelen diseñarse para modificar o eliminar datos e información almacenada en el disco duro, incurriendo en ilegalidades que pueden ser penalizadas.

Otra de sus funcionalidades principales es conseguir el control del sistema de información en el que consiguen acceder para envíos masivos de *spam* por correo electrónico o para alojar información ilegal (como pornografía infantil), entre otras utilidades no autorizadas.

#### Definición

##### **Spam o correo basura**

Envío masivo de correos electrónicos (normalmente con fines publicitarios) causando un perjuicio al receptor. Suele ser una fuente común de entrada de virus de la red al sistema.

El *software* malicioso está en continua actualización para conseguir mayor daño, mayor impacto o simplemente para acceder a más sistemas de información. Por ello, es necesaria la actualización periódica de antivirus, de otras herramientas que combaten este tipo de *software* y de todas las aplicaciones y sistemas operativos del sistema de información para minimizar el riesgo de acceso de usuarios no autorizados y de daños en la información del sistema.

### 3.3.- Criterios de programación segura

La programación segura se define como una rama de la programación encargada de la seguridad del código fuente de una aplicación con el fin de solucionar fallos y errores de programa descritos en apartados anteriores.

Son criterios de programación segura las acciones destinadas a:

- Protección de los desbordamientos de pila (problemas provocados por el exceso de flujo de datos en la pila de una función) utilizando funciones seguras.
- Utilizar el flujo de datos para un control continuo del trabajo realizado.
- Realización de pruebas y testeos de programas en ejecución para analizar sus fallos y errores.
- Creación de parches, actualizaciones de programas que arreglan los fallos detectados en las aplicaciones.
- Utilización de técnicas criptográficas y de cifrado para evitar que el *software* sea modificado por usuarios no autorizados.

#### **Definición**

##### ***Pila (o stack)***

*Estructura de datos en la que los datos se van almacenando ordenadamente a medida que van accediendo al sistema.*

## 4. PARTICULARIDADES DE LOS DISTINTOS TIPOS DE CÓDIGO MALICIOSO

Como se ha mencionado en epígrafes anteriores, los códigos maliciosos son un conjunto de programas informáticos diseñados para acceder a un sistema de información de forma no autorizada y provocar daños en este. Sus principales objetivos son:

- Destrucción o modificación de información.
- Robo de información y de claves de acceso.
- Propagación a otros equipos de una misma red o a través de Internet.

- Introducir publicidad de forma masiva.
- Comprometer la integridad de aplicaciones y sistemas operativos.

La evolución de las tecnologías de la información provoca que los códigos maliciosos sean cada vez más complejos y variados.

#### **4.1.- Tipos de códigos maliciosos**

La variada tipología de códigos maliciosos viene dada por su forma, origen, los daños que provocan o la finalidad para la que son diseñados, siendo los más importantes:

- Virus.
- *Cookies*.
- Troyanos.
- *Keyloggers*.
- *Spyware*.
- Gusanos o *worms*.

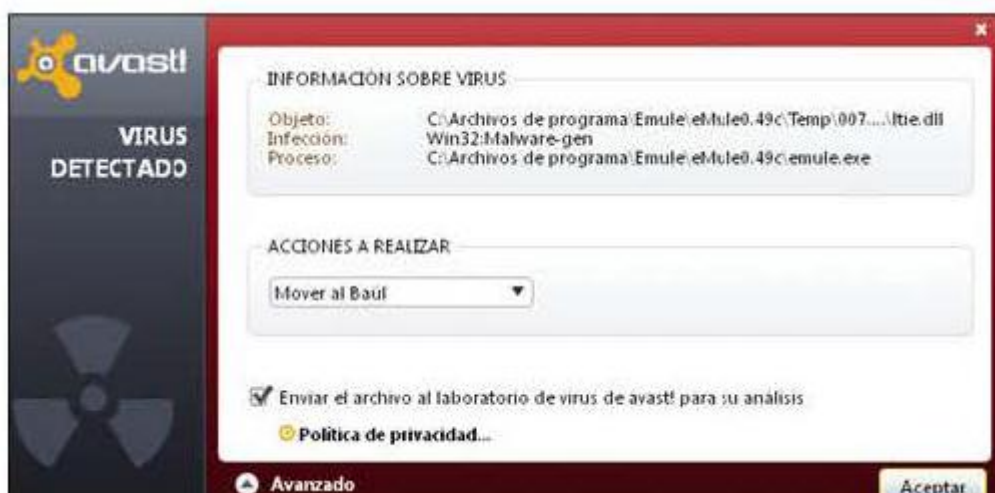
#### **Virus**

Los virus son un tipo de *software* malicioso que se diseñan para dañar el equipo al que acceden, pasando desapercibidos por el usuario.

Su funcionamiento también varía según el tipo de virus: suelen alojarse en un anfitrión o huésped y provocar daños desde su ubicación.

Lo malicioso de los virus también es variable; algunos virus son poco nocivos (provocando, por ejemplo, la aparición de mensajes o ventanas molestas), mientras que otros pueden ser más dañinos, provocando el borrado de archivos o incluso del sistema operativo al completo.

El modo de acceso y contagio suele ser por Internet, aunque también puede producirse mediante otros dispositivos de almacenamiento (como discos duros externos, *pendrives*, etc.) o, incluso, mediante redes locales (pudiendo estar infectados todos los ordenadores y dispositivos de la red).



*Virus detectado por el antivirus Avast!*

## Cookies

Las *cookies* no son una amenaza de seguridad en sí, pero pueden afectar a la privacidad y confidencialidad de los usuarios. Se trata de un tipo de *software* informático que detecta y almacena los datos de navegación de un usuario para conocer sus preferencias. Esta información se utiliza posteriormente para mostrar a los usuarios publicidad acorde con sus datos de navegación. Por ello, las *cookies* se consideran una herramienta de *marketing* muy potente para ofrecer a los usuarios información personalizada con sus preferencias de navegación y consumo.

Su funcionamiento es bastante simple:

1. En un momento inicial, las *cookies* (que provienen del servidor del atacante) se almacenan en el navegador del usuario.
2. En cuanto el usuario accede al navegador y empieza a navegar por páginas web, las *cookies* almacenan la información y la reenvían al servidor inicial.
3. Con la información recibida de la *cookie*, el atacante introducirá publicidad, relacionada con los gustos del usuario, en el navegador de este.

## Troyanos

Los troyanos son aplicaciones que contienen funcionalidades ocultas con finalidades maliciosas para el usuario.

Mientras que los virus se almacenan en un sistema y se propagan continuamente, los troyanos no ofrecen esta posibilidad.

Su modo de acceso es a través de aplicaciones inofensivas que incitan al usuario a ejecutarlo y provocan daños inmediatos o aplazados, como el borrado de datos, la instalación de más programas maliciosos, etc.

**Nota**

Los troyanos son muy utilizados para la distribución de otro *software* malicioso denominado *spyware*. Para ello, los troyanos se asocian a programas conocidos y deseables que son descargados por el usuario intencionadamente.

**Keyloggers**

Los *keyloggers* son otro tipo de *software* malicioso que se diseña con la finalidad de recopilar y almacenar remotamente el comportamiento de los usuarios.

Actúan almacenando toda la información tecleada por el usuario del sistema y enviándola al atacante (que también la almacenará para acceder a ella cuando lo requiera).

En la actualidad, otros tipos de *software* malicioso (como virus, troyanos, gusanos, etc.) también incorporan *keyloggers* como complemento a su funcionalidad, para conseguir información adicional del usuario.

**Spyware**

El *spyware* es una aplicación que se diseña con la finalidad de obtener información del usuario con fines lucrativos. Se recopilan comportamientos del usuario para conseguir información útil y venderla a terceros con fines publicitarios o de *marketing*.

Su procedimiento de actuación es el siguiente:

1. Acceso al sistema del usuario.
2. Obtención y recopilación de la información del usuario almacenada en el sistema.
3. Monitorización del sistema del usuario.
4. Registro y venta de la información del comportamiento del usuario.
5. Actuación de los terceros ante la información comprada al atacante.

**Nota**

Aunque todos los *spyware* tienen un procedimiento de actuación similar, existen varias tipologías calificadas según sus finalidades específicas (incluir ventanas de publicidad, personalizar la publicidad del navegador del usuario, etc.).

## Gusanos o worms

Los gusanos o *worms* son programas maliciosos autocontenidos cuya finalidad principal es su propagación a otros sistemas para mermar su rendimiento.

No ocasionan un daño como tal, aunque sí pueden contener otros códigos maliciosos complementarios que sí produzcan efectos perjudiciales al sistema de información.

Suelen infectarse a través de correos electrónicos, con la explotación de vulnerabilidades de programas y de los servicios de red o a través de redes de compartición de datos P2P.



Gusano detectado por el antivirus AVAST

## 5. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES

Cuando se pretende implantar un proceso de gestión de riesgos en la organización para aumentar el nivel de seguridad de la información, deben conocerse previamente una serie de conceptos y las relaciones existentes entre ellos.

### 5.1.- Elementos del análisis de riesgos

El proceso de gestión de riesgos conlleva el análisis de una serie de elementos importantes del sistema de información: los elementos más vulnerables ante posibles amenazas y aquellos cuyo deterioro pueda suponer un daño mayor en el sistema.

A continuación, se describen los principales elementos del análisis a tener en cuenta en el proceso de gestión de riesgos.

## Activo

Un activo es un recurso del sistema de información, necesario para garantizar el correcto funcionamiento de los procesos de la organización.

Los activos también son fundamentales para lograr los objetivos definidos por la organización y requieren de una especial protección: cualquier amenaza que pueda afectar a un activo puede poner en peligro la actividad de la organización y su servicio al cliente.

## Amenaza

Una amenaza es cualquier evento que puede afectar al activo de un sistema de información, provocando un incidente de seguridad y produciendo efectos adversos (materiales o inmateriales) o pérdidas de información.

Las amenazas afectan directamente a las propiedades de la información: integridad, disponibilidad, confidencialidad y autenticidad.

Las amenazas pueden ser de origen externo o interno: mientras que las de origen interno provienen de procesos internos, del propio personal o de las condiciones técnicas del sistema de información, las de origen externo provienen de agresiones humanas, técnicas o de agentes de carácter natural.

Además, las amenazas se clasifican en tres grupos, descritos en la tabla siguiente:

Tipos de amenazas	
Grupo	Definición
<b>Criminalidad</b>	Acciones causadas por humanos que incumplen requerimientos legales. Son ejemplos el sabotaje, el robo, el espionaje, el fraude, etc.
<b>Sucesos de origen físico</b>	Eventos de origen natural y/o técnico, además de eventos causados por humanos de forma indirecta. Por ejemplo: inundaciones, sobrecargas eléctricas, fallos de corriente, incendios, etc.
<b>Negligencia y decisiones institucionales</b>	Acciones realizadas por personas con poder e influencia sobre el sistema de información. Por ejemplo: gestión deficiente de contraseñas y permisos de usuario, falta de protocolo y normas de actuación, falta de formación, falta de capacitación, etc



**Vulnerabilidad**

Una vulnerabilidad consiste en alguna característica o capacidad de un activo del sistema de información que lo hace susceptible a amenazas.

También se define como la capacidad de actuación o reacción de un sistema de información ante la aparición de amenazas, además de la capacidad de recuperación de los daños ocasionados.

**Riesgo**

Como se ha mencionado anteriormente, un riesgo es la posibilidad de que una amenaza se materialice causando efectos negativos o positivos.

**Control atenuante**

Se consideran atenuantes aquellos activos y medidas que consiguen reducir las posibilidades de amenazas y, por tanto, el nivel de riesgo del sistema de información de la organización.

**Impacto**

El impacto es la magnitud del daño que provoca un ataque exitoso en el que se han perjudicado la confidencialidad, la disponibilidad, la integridad y la autenticidad de la información del sistema.

Dependiendo de los daños causados y los activos afectados, el impacto será mayor o menor: es posible que una amenaza comprometa a un activo prescindible del sistema (causando un impacto bajo) o que, sin embargo, comprometa a un activo importante, ocasionando efectos graves en el correcto funcionamiento de una organización (causando un impacto muy elevado).

**Probabilidad**

La probabilidad se define como la estimación de posibilidades de que se materialice el riesgo o, lo que es lo mismo, que se produzca una amenaza real.

**5.2.- Modelos de relaciones de conceptos de gestión de riesgos**

Las relaciones entre los conceptos definidos en el epígrafe anterior sobre gestión de riesgos se ven reflejadas en el siguiente cuadro.



Una correcta gestión del riesgo se consigue con la determinación del impacto y de la probabilidad de un riesgo potencial.

El impacto de una posible amenaza deberá calcularse con un análisis profundo de los distintos activos de la organización y de las amenazas que pueden afectar a estos. A mayores amenazas y activos más relevantes, mayor impacto para la organización. Y, por el contrario, a menor nivel de amenazas y afectación a activos menos relevantes, menor impacto.

Por otro lado, deberá calcularse también la probabilidad de ocurrencia de una amenaza. Esta probabilidad vendrá determinada por un análisis de las vulnerabilidades de la organización y de los atenuantes de los que se dispone. Del mismo modo que con el impacto, a menor nivel de vulnerabilidades y mayores atenuantes, menor probabilidad de amenazas. Por el otro lado, a mayor nivel de vulnerabilidades y menores atenuantes, mayor probabilidad de amenazas y, por tanto, mayor riesgo .

## 6. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS

Un control de seguridad es un conjunto de medidas encargadas de paliar las vulnerabilidades y reducir el riesgo de un sistema de información.

En la actualidad, se distinguen cuatro tipos de controles, mostrados en la tabla siguiente.

Tipos de controles de seguridad	
Control	Descripción
Disuasorio	Su finalidad principal es reducir la probabilidad de recibir un ataque.
Preventivo	Su finalidad es proteger al sistema de

	información de sus vulnerabilidades, intentando impedir el acceso de los atacantes o reduciendo el impacto de los daños causados.
<b>Correctivo</b>	Tienen como finalidad principal reducir el impacto de una amenaza.
<b>Detectivo</b>	Se encargan de detectar e impedir posibles ataques.

La gestión de riesgos debe ser capaz de determinar cuáles de estos controles son los más adecuados, eficientes y rentables y, para ello, existen dos metodologías distintas para realizar el análisis de riesgos:

- Metodología cuantitativa.
- Metodología cualitativa.

Una metodología se define como el procedimiento y el conjunto de técnicas utilizadas para el análisis del riesgo.

### 6.1.- Metodología cuantitativa de análisis de riesgos

El enfoque cuantitativo del análisis de riesgos tiene en cuenta dos elementos: la probabilidad de ocurrencia de un evento y el impacto que puede provocar en caso de que suceda.

Para determinar y analizar los riesgos, la metodología cuantitativa se basa en un modelo matemático que sirva de apoyo a la toma de decisiones.

Como ventajas de esta metodología, cabe destacar:

- Facilita comparaciones entre vulnerabilidades con características muy diferenciadas.
- Apoya numéricamente la toma de decisiones y las opiniones creadas.
- Sirve como justificante para la aplicación de medidas de gestión de riesgos.

En cuanto a sus desventajas, se distinguen las siguientes:

- Se utilizan metodologías de análisis de riesgos estándares, no ofrece la posibilidad de personalizarlas según las particularidades del sistema de información.
- Deben ser desarrolladas obligatoriamente por profesionales especializados para que proporcionen resultados fiables.
- Resultan difíciles de mantener y de modificar.
- Solo permiten la estimación de pérdidas cuando estas dependen de valores cuantificables. En el momento que entra un valor indefinido o que no permite cuantificación, la estimación de las pérdidas no será válida.

**Nota**

La metodología cuantitativa se considera una metodología objetiva, ya que se basa en términos estadísticos, no influye ningún tipo de opinión.

**6.2.- Metodología cualitativa de análisis de riesgos**

Al revés que la metodología cuantitativa, la metodología cualitativa se basa en el raciocinio humano para calcular las pérdidas potenciales estimadas sin necesidad de utilizar métodos probabilísticos. Es la metodología utilizada con más frecuencia para el análisis de riesgos.

También requieren la participación de un profesional, pero el coste en recursos humanos implicados es sumamente inferior.

Esta metodología suele utilizarse cuando el nivel de riesgo no es elevado o cuando los datos numéricos no son adecuados para una correcta estimación del riesgo. También se utiliza como base inicial para definir la metodología cuantitativa a utilizar en el análisis.

De sus ventajas principales, destacan las siguientes:

- Permite una organización del trabajo flexible y con capacidad de reacción.
- Incluye valores y activos incuantificables.
- Se enfoca principalmente en la identificación de los eventos ocurridos o potenciales.

Por el contrario, también se pueden distinguir varias desventajas:

- Depende de la calidad, profesionalidad y habilidad de los profesionales participantes en el análisis.
- Según el nivel de conocimientos del profesional, es posible que se pasen por alto riesgos importantes desconocidos.
- Exige la opinión e intervención de un profesional.
- Identifica los eventos con mayor claridad, pero no puede determinar la probabilidad real de ocurrencia.

**Nota**

Al contrario que la metodología cuantitativa, la metodología cualitativa se considera sumamente subjetiva, al requerir la opinión de expertos basada en su formación y experiencia para estimar las probabilidades de riesgo de la organización.

## 7. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN

El proceso de análisis y gestión de riesgos está formado por una serie de fases.

FASES DEL PROCESO DE ANÁLISIS Y ,GESTIÓN DE RIESGOS	
1. Identificación de los activos.	
2. Valoración de los activos.	
3. Identificación de las amenazas.	
4. Determinación del impacto de una amenaza.	
5. Determinación del riesgo.	
6. Establecimiento de salvaguardas (atenuantes).	
7. Revisión del impacto y determinación del impacto residual.	
8. Revisión del riesgo y determinación del riesgo residual.	

Este apartado se va a centrar principalmente en las fases 1 y 2 del proceso, la identificación y valoración de los activos.

### 7.1.- Identificación de los activos involucrados en el proceso de análisis y gestión de riesgos

Como se ha comentado anteriormente, un activo es el conjunto de recursos del sistema de información o relacionados con este que son necesarios para el correcto funcionamiento de la organización y para que se alcancen los objetivos definidos por esta.

El activo más importante que maneja una organización es, sin duda, la información. No obstante, no hay que olvidar otros activos que también pueden ser relevantes, como por ejemplo:

- Los servicios prestados con la utilización de dicha información.
- Los servicios necesarios para poder utilizar y tratar la información.
- Los equipos y soportes de información que permiten almacenar la información: ordenadores, dispositivos de almacenamiento externos, etc.
- Los equipos informáticos que permiten la gestión de la información.
- Las aplicaciones que permiten gestionar la información y los servicios que se proporcionan a través de esta.
- Las redes de comunicaciones que permiten y facilitan el intercambio de información.
- Las instalaciones en las que se ubican y protegen los equipos informáticos, dispositivos, sistemas de almacenamiento y redes de comunicaciones necesarios para gestionar la información y ofrecer el servicio.
- Los recursos humanos que utilizan todos los elementos anteriores.

**Importante**

Cada organización debe conocer sus peculiaridades y analizar los activos que son más relevantes para el sistema de información. Las organizaciones no son homogéneas, por lo que lo que puede ser imprescindible para una organización puede ser completamente irrelevante para otra.

**7.2.- Valoración de los activos implicados en el análisis y gestión del riesgo**

La importancia de los activos de un sistema de información dependerá de su valoración. Si un activo no tiene valor, es completamente prescindible.

Por otra parte, si un activo es necesario para el correcto funcionamiento del sistema, es que tiene cierto valor. Lo que habrá que calcular es cuál es el valor de dicho activo.

La valoración del activo viene definida como el coste que implicaría recuperarse de un fallo del activo provocado por alguna incidencia.

Esta valoración depende de muchos factores que variarán, por supuesto, según la organización y el sistema de información implantado. Los factores más importantes a considerar son:

- Coste del personal especializado necesario para recuperar el activo (coste de mano de obra).
- Los ingresos perdidos por el fallo del activo.
- Coste de adquisición e instalación de un activo nuevo en caso de que el anterior haya resultado inservible (coste de reposición).
- Pérdida de percepción de confianza y calidad de los clientes y proveedores provocados por una interrupción del servicio provocada por el fallo del activo.
- Infracciones cometidas y sanciones correspondientes al incumplimiento de requerimientos legales o de obligaciones contractuales debidas al fallo del activo.
- Daños y efectos perjudiciales provocados por el activo a otros activos, tanto propios como ajenos a la organización.
- Daños medioambientales causados por el activo.
- Daños a otras personas causados por el activo.

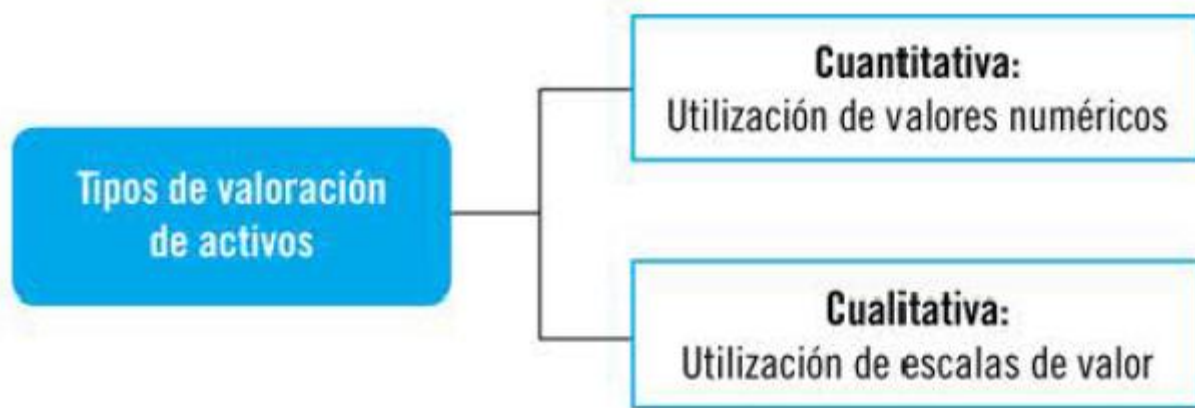
**Nota**

En el momento de la valoración de los activos, hay que tener en cuenta también que está la posibilidad de que un activo dependa de otro activo. En este caso, deberá calcularse el valor acumulado de ambos activos.

**7.3.- Tipos de valoraciones de activos**

La valoración de un activo, del mismo modo que la metodología de gestión de riesgos, puede realizarse de dos modos:

- **Valoración cuantitativa:** se calcula el valor del activo utilizando cantidades numéricas, valores exactos.
- **Valoración cualitativa:** se asigna el valor a los activos, utilizando una escala de niveles. Por ejemplo: puede utilizarse una escala tipo "valor nulo, valor bajo, valor medio, valor alto, valor muy alto" para clasificar los distintos activos en cada uno de los niveles de valoración.



Sea cual sea la metodología de valoración de activos utilizada, hay que tener en cuenta dos aspectos básicos:

- **Homogeneidad:** es necesario poder establecer comparaciones de los valores de los activos aunque sean de diferentes dimensiones para determinar la relevancia de cada uno de ellos.
- **Relatividad:** también es vital que exista la posibilidad de relativizar el valor de un activo cuando se compara con los demás. Es posible que un activo conlleve muchos costes de reposición y que tenga un valor elevado, pero que, al compararlo con los demás activos del

sistema de información, su valoración sea relativamente reducida (que los otros activos tengan costes de reposición mucho más elevados que este) .

#### 7.4.- Las dimensiones de valoración de los activos

Cuando se procede a realizar la valoración de los activos, no puede calcularse tomando solo una de sus dimensiones, sino que deben tenerse

en cuenta todas y cada una de ellas.

Las distintas dimensiones de un activo pueden observarse en la tabla siguiente.

DIMENSIONES DE VALORACIÓN DE LOS ACTIVOS	
Dimensión	Descripción
Disponibilidad	¿Cuál sería la importancia del activo si este no estuviera disponible?
Integridad	¿Qué importancia tendría que el activo sufriera modificaciones descontroladas?
Confidencialidad	¿Cuál sería la importancia del conocimiento del activo por usuarios no autorizados?
Autenticidad	¿Cuál sería la importancia del acceso al activo por parte de personas no autorizadas?
Trazabilidad	¿Cuál sería la importancia de la falta de constancia de la utilización del activo?

### 8. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE

Una amenaza es un conjunto de hechos y eventos que pueden ocurrir y que pueden provocar efectos perjudiciales a los activos del sistema de información. Por ello, tiene prioridad proteger a los activos de dichas amenazas.

En el momento de la identificación de amenazas, hay que tener en cuenta que pueden ser accidentales o, por el contrario, provocadas deliberadamente.

Como ejemplos de amenazas accidentales se pueden citar amenazas naturales (terremotos, inundaciones, etc.), amenazas industriales (fallos eléctricos, fallos de comunicación, etc.) o amenazas humanas (errores provocados sin deliberación previa u omisiones de acciones que son importantes para el funcionamiento del sistema).



Por otro lado, las amenazas deliberadas se realizan con intencionalidad y la mayoría son penalizadas por las leyes. Algunos ejemplos son la intrusión, el espionaje, el robo de información, el fraude, etc.



La manera de proteger los activos de las amenazas es reduciendo su riesgo, intentando reducir al máximo la posibilidad de que estas ocurran.

Para ello, será necesario identificar las posibles amenazas del sistema de información y valorarlas.

### 8.1.- Identificación de las amenazas

La identificación de las amenazas se lleva a cabo con el fin de conocer con mayor profundidad el entorno al que se enfrenta el sistema de información. Más concretamente, se pretende conocer qué es lo que puede ocurrir, cuáles serían sus consecuencias y cuál es la probabilidad de que estas ocurran.

Para identificar las amenazas, es necesario conocer los activos de que dispone la organización y sus características principales. Los principales activos son los siguientes:

- Tipo de activo (dispositivo de almacenamiento, red de comunicación, etc.).
- Las dimensiones del activo que hacen que tenga un valor considerable.
- La experiencia de la organización en relación a anteriores incidencias ocurridas con el activo.
- Los defectos del activo notificados por su fabricante de origen.

Una vez descritas las características del activo, habrá que registrar información detallada de la amenaza:

- Efectos de la amenaza debidamente explicados.
- Entrevistas realizadas que han aportado información para la detección de la amenaza.
- Historial de amenazas relevantes, tanto de la organización como de otras organizaciones.

### Ejemplos de amenazas frecuentes

Amenazas muy frecuentes en los sistemas de información que pueden tener efectos perjudiciales graves en caso de incidencia son:

- **Suplantación:** esta amenaza se produce cuando un usuario no autorizado suplanta la identidad de otro usuario haciéndose pasar por este.
- **Alteración:** modificación y alteración de la información o de algún dato concreto del sistema de información.
- **Repudio:** negación de la producción de un hecho. Es frecuente que un empleado realice alguna acción perjudicial para la organización y que, posteriormente, lo niegue.
- **Divulgación de información:** comunicación de información confidencial o de valor a terceros que no deberían conocerla.
- **Denegación del servicio:** incapacidad de acceder a un servicio determinado del sistema de información. Suele producirse por saturación de datos de entrada.
- **Elevación de privilegios:** utilización de privilegios de mayor nivel por usuarios no autorizados para ello.

En la tabla siguiente, se describen varios ejemplos de las amenazas más frecuentes ya descritas.

AMENAZA	EJEMPLO
<b>Suplantación</b>	Envío de correos electrónicos con la identidad de otro usuario.
<b>Alteración</b>	Modificación no autorizada de los datos de un archivo.
<b>Repudio</b>	Empleado que elimina datos importantes del sistema y que, posteriormente, niega este hecho.
<b>Divulgación de información</b>	Envío por error de correos electrónicos con datos confidenciales de los clientes de la organización.
<b>Denegación del servicio</b>	Ataque de denegación del servicio mediante el envío excesivo de datos al sistema de información, provocando su saturación y evitando el acceso de otros usuarios.
<b>Elevación de privilegios</b>	Obtención y utilización de los privilegios y permisos del administrador sin autorización.

## 8.2.- Valoración de las amenazas

Cuando se produce una amenaza, los efectos sobre los activos no son igual de perjudiciales para todas sus dimensiones, pudiendo, por ejemplo, afectar gravemente a la integridad de la información, pero no tener efectos sobre su confidencialidad.

Las amenazas se valorarán atendiendo a los efectos perjudiciales que pueden provocar a los activos del sistema de información o, lo que es lo mismo, a su impacto.

El impacto de una amenaza se define como la medición del daño provocado sobre uno o varios activos.

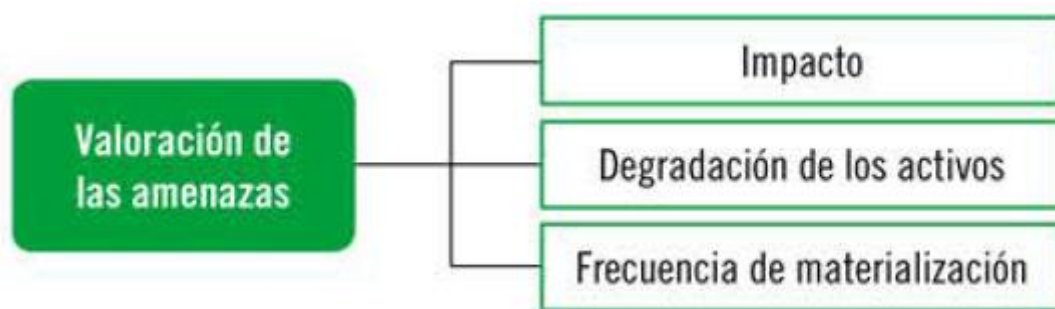
Su valoración se calculará tomando como referencia los siguientes elementos:

- Daños producidos en los activos de la organización.
- Capacidad de reproducción y expansión de la amenaza a otros activos del sistema.
- Capacidad de explotación de la amenaza.
- Usuarios que se pueden ver afectados en caso de producirse la amenaza.
- Capacidad de detección y descubrimiento de la amenaza cuando esta se produzca.

Además del impacto, la valoración de la amenaza vendrá también determinada por la vulnerabilidad del activo, que se verá afectado en dos aspectos:

- Degradación del activo: valoración del perjuicio sufrido por el activo por la ocurrencia de la amenaza.
- Frecuencia de la amenaza: cantidad de veces que se produce la amenaza en un período de tiempo determinado.

De este modo, la valoración de la amenaza vendrá dada por su impacto, la degradación de los activos afectados y su frecuencia.



Así, una amenaza con un impacto elevado, con efectos nocivos relativamente inofensivos y una frecuencia de materialización muy escasa, tendrá un valor inferior que una amenaza con el mismo impacto y los mismos efectos nocivos, pero que tenga una frecuencia de materialización elevada (que se materialice constantemente, por ejemplo).

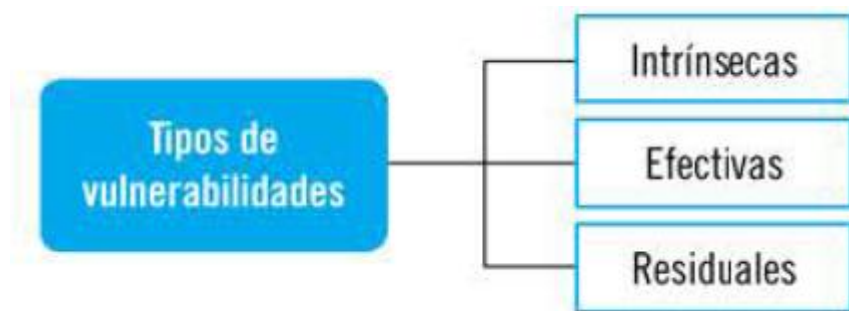
## 9. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

Una vulnerabilidad es la probabilidad de que una amenaza se materialice sobre un activo.

Para identificar y estimar una vulnerabilidad, debe participar un profesional que conozca profundamente los distintos activos del sistema de información y las amenazas y riesgos que pueden sufrir.

Se consideran tres tipos de vulnerabilidades:

- **Vulnerabilidad intrínseca:** vulnerabilidad que proviene directa y exclusivamente del activo y de la amenaza.
- **Vulnerabilidad efectiva:** que se ha generado a raíz de una salvaguarda ya existente en el sistema de información.
- **Vulnerabilidad residual:** generada por la aplicación de salvaguardas implantadas siguiendo el resultado del proceso de análisis y gestión de riesgos.



La vulnerabilidad se medirá considerando el periodo de tiempo transcurrido entre la amenaza potencial y su materialización real en el activo del sistema de información. Tendrá también que calcularse la frecuencia en la que se materializa la amenaza.

Algunos ejemplos de vulnerabilidades son:

- Vulnerabilidades de seguridad física:
  - Accesos de personal no autorizado al recinto.
  - Desastres naturales (rayos, inundaciones, etc.).
  - Incendios.
- Vulnerabilidades en las conexiones de red:
  - Fallos en el cortafuegos o *firewall*.
  - Intrusiones y accesos no autorizados a través de la red.
- Vulnerabilidades en la infraestructura de red:
  - Fallos y vulnerabilidades presentes en dispositivos de red como *routers*, *hubs*, *switches*, etc.
- Vulnerabilidades en el correo electrónico.
- Vulnerabilidades en las aplicaciones de gran valor y en sistemas operativos.

Para la medición de la vulnerabilidad se utilizan escalas que valorarán la frecuencia de ocurrencia y su probabilidad. Un ejemplo de tabla de valores de vulnerabilidades podría ser el siguiente:

Valor de la vulnerabilidad	Frecuencia	Probabilidad
<b>Muy frecuente</b>	Varias veces al día.	Entre el 75 y el 100 %.
<b>Bastante frecuente</b>	Una vez al día.	Entre el 50 y el 75 %.
<b>Frecuente</b>	Una vez en semana.	Entre el 25 y el 50 %.
<b>Poco frecuente</b>	Una vez al mes.	25% o menos.

Para detectar y analizar las vulnerabilidades de un sistema de información, se utilizan ciertas herramientas y técnicas de análisis de las que cabe destacar las siguientes:

- Análisis local.
- Análisis remoto de caja blanca.
- Análisis de caja negra.

### 9.1.- Análisis local para la detección de vulnerabilidades

El análisis local de vulnerabilidades en un sistema de información se realiza mediante la ejecución de pruebas de *software*. La finalidad de estas pruebas es obtener información objetiva sobre la calidad de las distintas aplicaciones y sistemas operativos del sistema de información.

Estas pruebas pueden ser de dos tipos:

- Pruebas estáticas: pruebas que no requieren la ejecución del código de la aplicación para poder realizarse.
- Pruebas dinámicas: al contrario que las estáticas, las dinámicas necesitan que se esté ejecutando la aplicación en el momento de la realización de la prueba. Su principal ventaja es su mayor precisión en el momento de evaluar el comportamiento de la aplicación analizada.

Tanto las pruebas estáticas como las dinámicas utilizan una serie de herramientas y métodos que permitirán la detección de las vulnerabilidades y su posterior medición.

### 9.2.- Análisis remoto de caja blanca

El análisis remoto de caja blanca se realiza con la ejecución de pruebas que examinan la estructura interna de la aplicación y de los componentes del sistema.

Antes de la ejecución de las pruebas de caja blanca, los auditores informáticos deberán recopilar toda la información que sea posible para la evaluación de la seguridad y de las vulnerabilidades del sistema de información: código fuente de las aplicaciones, archivos de configuración, etc.

Con esta información, además de detectar las vulnerabilidades más próximas, también se pueden detectar vulnerabilidades potenciales más profundas con una revisión extensa del sistema.

Estas pruebas suelen requerir más recursos por parte del auditor y de la organización, pero también ofrecen resultados más precisos.

En la tabla siguiente, se describen las ventajas y desventajas de los análisis de caja blanca.

ANÁLISIS DE CAJA BLANCA	
Ventajas	Desventajas
Las pruebas son muy minuciosas y los resultados obtenidos más precisos.	Requiere muchos y costosos recursos.
Las recomendaciones obtenidas de los resultados de estas pruebas también son más precisas y eficaces.	No hay simulación de intrusión para verificar su efectividad.
Detecta tanto las vulnerabilidades más inmediatas como las más profundas (de configuración y de diseño de la aplicación).	

### 9.3.- Análisis de caja negra

#### Desventajas

- Requiere muchos y costosos recursos.
- No hay simulación de intrusión para verificar su efectividad.

Los análisis de caja negra consisten en una serie de pruebas que evalúan exclusivamente las entradas y salidas del sistema de información.

Su finalidad principal es conseguir simular los ataques de un intruso: imitan lo que el intruso haría y obtienen información bastante real sobre los riesgos a los que se expone el sistema evaluado. La base de estas pruebas es que si un auditor de seguridad informática es capaz de detectar alguna vulnerabilidad con estas pruebas de caja negra, un intruso también podría detectarlas con facilidad.

Se pueden obtener datos del sistema como:

- Las funciones que realiza el sistema.
- El grado de cumplimiento de los objetivos del sistema.
- Las reacciones del sistema ante la presencia de intrusiones.

En la tabla siguiente, se distinguen las ventajas e inconvenientes de las pruebas de caja negra.

ANÁLISIS DE CAJA NEGRA	
Ventajas	Desventajas
Facilita información que permite realizar estimaciones reales de las amenazas.	Recopilar toda la información pública necesaria puede ser un trabajo bastante laborioso.
Obtiene la información a través del análisis de información pública (interna y externa).	Las vulnerabilidades más profundas y ocultas pueden ser pasadas por alto en el análisis.
Los recursos de la organización utilizados para este tipo de pruebas son bastante reducidos	Las recomendaciones formuladas a partir de los resultados de esta prueba son de carácter general.

## 10. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA

Una vez realizada la gestión del riesgo del sistema de información, ya se conocen con más profundidad las vulnerabilidades a las que está expuesto. Con esta información y las vulnerabilidades detectadas, se pueden proponer una serie de recomendaciones que las eliminen o que reduzcan su probabilidad de materialización.

De este modo, el proceso de auditoría en futuras evaluaciones se irá optimizando, ya que el número de vulnerabilidades y defectos del sistema detectados debería ser menor si las medidas correctoras se aplican correctamente.

Con la corrección de las vulnerabilidades detectadas y la continua evaluación de los sistemas de información, debe producirse un proceso de aprendizaje que deberá reflejarse en el informe de auditoría, permitiendo así una optimización constante y progresiva del proceso de auditoría.

El informe deberá contener el histórico de las vulnerabilidades detectadas, su progresión y las posteriores modificaciones del sistema de información implantadas siguiendo las recomendaciones de la auditoría.

### 10.1.-El informe de auditoría

El informe de auditoría es un documento formalizado que contiene los objetivos de la auditoría, las metodologías utilizadas, los resultados obtenidos y las conclusiones y recomendaciones aportadas por los auditores.

Este informe tiene que ser claro, conciso, oportuno, objetivo e imparcial y debe ser elaborado por auditores independientes.

En cuanto a la gestión de riesgos, el informe de auditoría deberá contener también los activos de la organización y su valoración, junto con las vulnerabilidades, amenazas y riesgos detectados en el sistema de información detectado.

Además, deberán formularse recomendaciones de políticas y medidas correctivas que permitan la reducción del riesgo y de posibles vulnerabilidades, además de proponer salvaguardas que reduzcan la incidencia de vulnerabilidades.

**Importante**

El informe de auditoría en ningún caso puede ser elaborado con criterios subjetivos. Se requiere que todas las conclusiones y recomendaciones propuestas estén debidamente fundamentadas en los resultados obtenidos del proceso de auditoría.

**11. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS**

Las medidas de salvaguarda o de seguridad son medidas cuya función fundamental es reducir o eliminar un riesgo de dos formas:

- La reducción de la probabilidad de materialización de las amenazas: son también salvaguardas preventivas. La salvaguarda ideal sería aquella que impidiese completamente que se materializara cualquier tipo de amenaza.
- La reducción del impacto de las amenazas sobre la organización: hay salvaguardas que limitan o reducen la degradación del activo ante la presencia de alguna amenaza, impidiendo que el daño ocasionado se expanda. En otras ocasiones, ciertas amenazas también pueden llegar a restaurar el sistema cuando alguna amenaza lo ha puesto en peligro o ha dañado alguno de sus activos.

•

Para que estas salvaguardas actúen, debe haberse materializado la incidencia o amenaza y, en cualquier caso, la salvaguarda limita los efectos nocivos y su expansión sobre los activos que forman parte del sistema dañado.

Estas medidas de salvaguarda se clasifican en varios tipos, atendiendo a criterios diferentes.

La primera de las clasificaciones es atendiendo al momento de actuación de la salvaguarda, distinguiendo:

- Salvaguardas activas: aquellas que reducen o eliminan el riesgo de una amenaza.
- Salvaguardas pasivas: aquellas que reducen el impacto sobre la organización, una vez ya se ha producido el incidente de seguridad.

Por otra parte, otra clasificación de las salvaguardas hace referencia a su composición y al tipo de protección que ofrecen:



- Salvaguardas físicas: aquellas que protegen el acceso físico a los activos y las condiciones ambientales en las que estos se utilizan.
- Salvaguardas lógicas: se encargan de proteger los activos a través de herramientas, técnicas y programas informáticos.



Una salvaguarda eficaz al 100% sería lo ideal, pero, para ello, debería cumplir una serie de preceptos:

- Su implantación, configuración y mantenimiento deben ser perfectos.
- Debe emplearse en todo momento.
- Su protocolo de uso normal debe ser claro y, en caso de ocurrir cualquier incidencia, el personal debe estar correctamente formado para reaccionar de un modo rápido y eficaz.
- Deben estar implantados una serie de controles que avisen cuando se detecte cualquier tipo de fallo.

Como estos preceptos no suelen ser fáciles de cumplir y menos todos a la vez, las organizaciones deben intentar conseguir unas salvaguardas que tengan un cierto grado de eficacia que permita el cumplimiento de los objetivos de seguridad marcados, calculando una estimación real cuando se quiera estimar la gestión de riesgos.

**Nota**

El objetivo de las salvaguardas es reducir el riesgo, pero existe la posibilidad de que estas tengan, a su vez, vulnerabilidades. Para reducirlas, las organizaciones deben realizar pruebas y evaluaciones que permitan un seguimiento continuo y la detección y corrección de las vulnerabilidades que puedan aparecer.

### 11.1.-Las salvaguardas y los activos

Existe la posibilidad de que algunas salvaguardas pasen a formar parte del equipamiento de un sistema de información. El coste de implantación de la salvaguarda hace que el activo al que protege aumente de valor, convirtiéndose en parte de él.

Hay que tener en cuenta que, en el momento en que pasa a formar parte de un activo, también está expuesto a los riesgos del sistema y puede tener vulnerabilidades, a la vez que puede sufrir las mismas amenazas que los otros activos.

Por eso, cuando se implantan salvaguardas que forman parte del activo, hay que realizar un nuevo análisis de riesgos con el nuevo sistema desplegado para asegurarse de que el riesgo al que se expone el sistema es inferior a aquel al que estaba expuesto antes de implantarse la salvaguarda.

Aunque se incorpore la salvaguarda al sistema, su finalidad debe ser la misma: reducir el riesgo del sistema general y de la organización.

#### Nota

Por muchas salvaguardas y medidas de seguridad que se implanten en las organizaciones, la seguridad absoluta es imposible de conseguir.

Por ello, las organizaciones deben ser capaces de asumir un nivel de riesgo que les permita trabajar con cierta seguridad y mantener sus estándares de calidad.

## 12. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE

Cuando ya se han identificado y valorado los activos, amenazas, vulnerabilidades y salvaguardas, la siguiente fase en el proceso de gestión del riesgo es el establecimiento de los escenarios de riesgo o, lo que es lo mismo, la estimación del estado del riesgo.

- El objetivo principal de esta fase se divide en dos puntos fundamentales:
  - Estimar el impacto potencial al que se somete el sistema de información.
  - Estimar el impacto residual al que se somete el sistema de información.

### 12.1.-Estimación del impacto potencial

El impacto potencial está formado por el conjunto de efectos perjudiciales que pueden sufrir los activos del sistema de información en el caso de materializarse una amenaza.

Para el cálculo del escenario activo-amenaza derivado del impacto potencial, deberán tenerse en cuenta los aspectos siguientes:

- Activos identificados y su valoración.
- Amenazas identificadas y su valoración.

#### Importante

Para el cálculo del impacto potencial y la estimación del escenario de riesgo, no se tienen en cuenta las salvaguardas implantadas en el sistema. Estas se incluirán en el impacto residual.

Teniendo en cuenta el par activo-amenaza, pueden establecerse una serie de escenarios de impacto teniendo en cuenta la degradación del activo provocada por la amenaza y la valoración de dicho activo.

Se categoriza el valor de los activos en:

- Muy alto.
- Alto.
- Medio.
- Bajo.
- Muy bajo.

Por otro lado, se categoriza su degradación provocada por la amenaza en:

- Degradación inferior al 1 % de su valor.
- Degradación entre el 1 y el 10% de su valor.
- Degradación de más del 10 % de su valor.

Con las distintas combinaciones de las categorías descritas arriba, se forma una tabla de escenarios como la siguiente:

		Degradación del activo		
IMPACTO		Inferior al 1 %	1-10 %	Superior al 10 %
Valor del activo	Muy alto	MEDIO	ALTO	MUY ALTO
	Alto	BAJO	MEDIO	ALTO
	Medio	MUY BAJO	BAJO	MEDIO
	Bajo	MUY BAJO	MUY BAJO	BAJO
	Muy bajo	MUY BAJO	MUY BAJO	MUY BAJO

Observando la tabla, la prioridad de actuación deberá ir de mayor a menor empezando por los activos de impacto muy alto y terminando por los activos de impacto bajo y muy bajo-

Por tanto, los activos de impacto muy alto requerirán una atención inmediata y pormenorizada para intentar disminuir al máximo las incidencias que puedan afectar a este tipo de activos\_

Sin embargo, los activos de impacto muy bajo no influirán considerablemente en el correcto funcionamiento del sistema, por lo que la actuación sobre estos puede aplazarse si surgen otras incidencias de mayor calibre.

Sea como sea, aunque unos tengan más prioridad que otros, todos los activos requieren atención; no hay que dejarlos desatendidos y desprotegidos ante amenazas de seguridad\_

## 12.2.-Estimación del impacto residual

El impacto residual, al contrario que el impacto potencial, tiene en cuenta la actuación de las salvaguardas sobre el riesgo del sistema de información.

Se define el impacto residual como los daños a los que se expone el sistema de información cuando este está protegido por las salvaguardas implantadas.

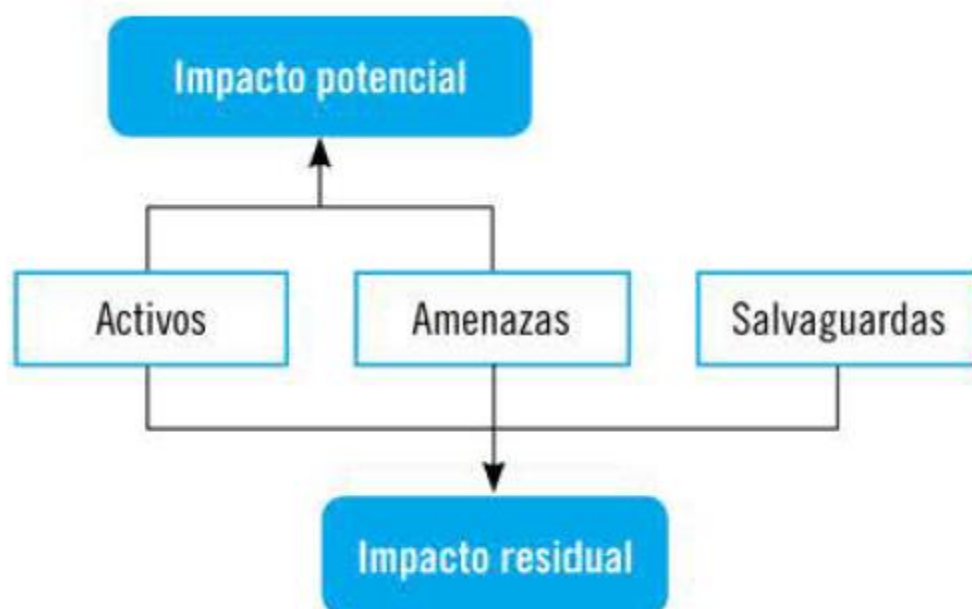
De este modo, para su estimación se añade un elemento más al cálculo, siendo sus elementos principales:

- La identificación y valoración de los activos.
- La identificación y valoración de las amenazas.
- La identificación y valoración de las salvaguardas.

Si la actuación de las salvaguardas fuese eficaz y correcta, el impacto residual de una amenaza sobre los activos del sistema de información deberá ser menor que su impacto potencial.

Si no fuese así, debería iniciarse una evaluación de las salvaguardas para conocer sus vulnerabilidades y los efectos de estas e implantar medidas correctoras que permitan una mayor eficiencia y un menor impacto ante incidencias de seguridad.

En el siguiente cuadro, se representa la diferencia del impacto residual y del impacto potencial.



### **13. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS**

Para establecer el nivel de riesgo de cada par de activo/amenaza, previamente hay que determinar la probabilidad y el impacto de materialización de los escenarios.

#### **13.1.-Probabilidad de materialización de los escenarios de riesgo**

Por una parte, la probabilidad de materialización de un escenario se define con las posibilidades reales que hay de producirse una incidencia de seguridad y la frecuencia con la que se puede producir.

Esta probabilidad viene clasificada en cinco categorías distintas:

- Raro: con probabilidades casi nulas de materializarse la amenaza; entre 0 y 20 % de probabilidad.
- Improbable: con pocas probabilidades de materializarse la amenaza: entre 20 y 40 %.
- Probable: tanto puede materializarse la amenaza como no materializarse; entre 40 y 60 %.
- Altamente probable: con elevadas posibilidades de materializarse la amenaza; entre 60 y 80 %.
- Casi certeza: es prácticamente seguro que se produzca la amenaza; entre 80 y 100 %.

En la siguiente tabla, se muestra la categorización de la probabilidad de materialización de la amenaza.

PROBABILIDAD	ESCALA	DESCRIPCIÓN	CALIFICACIÓN
Raro	0-20 %	Eventualidad casi nula	1
Improbable	20-40 %	Solo ocurre en ocasiones excepcionales	2
Probable	40-60 %	Puede ocurrir o no ocurrir	3
Altamente probable	60-80 %	Puede ocurrir bastantes veces	4
Casi certeza	80-100 %	Casi siempre ocurre	5

Se establece una puntuación numérica para calificar la probabilidad de materialización de una amenaza para que la estimación del riesgo pueda calcularse con mayor facilidad y objetividad.

### 13.2.- Impacto de materialización de los escenarios de riesgo

Por otro lado, el impacto vendrá determinado por los efectos negativos que puede producir la materialización de una amenaza y también se categorizará en las cinco tipologías ya mencionadas:

- **Muy bajo:** el valor de los activos afectados es muy bajo y la degradación que pueden sufrir ante incidencias es prácticamente nula.
- **Bajo:** el impacto de la materialización de la amenaza es bastante irrelevante para la organización.
- **Medio:** el impacto de materialización de la amenaza ya merece atención por parte de la organización, bien porque los activos tienen un valor considerable o bien porque su nivel de degradación también es bastante elevado.
- **Alto:** la materialización de la amenaza puede ocasionar daños importantes para el sistema de información y para la organización en general.
- **Muy alto:** los daños que puede ocasionar la amenaza si se materializa pueden ser muy graves, quedando la organización gravemente dañada; los activos afectados son de gran valor y su degradación es prácticamente total.

Impacto	DESCRIPCIÓN	CALIFICACIÓN
Muy bajo	Impacto insignificante.	1
Bajo	Efectos mínimos para la organización.	2
Medio	Efectos considerables sobre los activos.	3
Alto	Efectos muy considerables para la organización en general.	4
Muy alto	Efectos irreparables o difícilmente reparables para la organización.	5

**Nota**

El impacto que se categoriza para la gestión del riesgo puede ser tanto residual como potencial.

**14. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA**

Cuando ya se han categorizado los pares activo/amenaza y establecidos los distintos niveles de impacto y probabilidad de una amenaza, el siguiente paso es la estimación del riesgo.

Los datos de entrada que se deberán utilizar para la estimación del riesgo serán los siguientes:

- Identificación y valoración de los activos.
- Identificación y valoración de las amenazas.
- Identificación y valoración de las salvaguardas.
- Impacto estimado con los pares activo/amenaza identificados.

Del mismo modo que con los impactos, la estimación del riesgo puede ser de riesgo residual o de riesgo potencial:

- El riesgo potencial será el riesgo al que está sometido el sistema de información sin contar con las salvaguardas establecidas. Solo se tienen en cuenta los activos, las amenazas y el impacto potencial.
- El riesgo residual, por el contrario, se estimará tomando como factores de cálculo las salvaguardas establecidas en el sistema y el impacto residual, además de los activos y las amenazas.

**Nota**

La estimación del riesgo no puede hacerse de un modo global para la organización; deberá efectuarse activo por activo (valorando el impacto y probabilidad de materialización de las amenazas sobre todos y cada uno de los activos del sistema de información).

### 14.1.-Nivel de riesgo de los escenarios de los pares activo/amenaza

Los distintos escenarios que pueden producirse con las combinaciones de las categorías del impacto sobre los activos de una organización y la probabilidad de materialización de las amenazas establecen varias categorías de riesgo divididas en cinco niveles:

- Nivel de riesgo despreciable.
- Nivel de riesgo bajo.
- Nivel de riesgo moderado.
- Nivel de riesgo importante.
- Nivel de riesgo crítico.

La ubicación de cada riesgo en una u otra categoría se calculará con el producto de las calificaciones de su impacto y de su probabilidad:

$$\text{RIESGO} = \text{IMPACTO} \times \text{PROBABILIDAD}$$

Por ejemplo, una amenaza sobre un activo con un impacto calificado como **1** y una probabilidad de materialización calificada como **3** tendrá un nivel de riesgo 3 ( $1 \times 3 = 3$ ).

Es importante remarcar que la calificación del riesgo en sí se utiliza para priorizar ciertas amenazas de algunos activos frente a otras. No obstante, la categorización del riesgo en sí valora más la frecuencia y probabilidad en la que se produce una amenaza que el impacto que puede producir frente al activo.

La calificación mínima del nivel de riesgo será de valor 1 (impacto 1, probabilidad 1) y la máxima será de valor 25 (impacto 5, probabilidad 5).

De este modo, los niveles de riesgo para cada par activo/amenaza (impacto/ probabilidad) se ven reflejados en la tabla siguiente.

		Probabilidad				
Nivel de riesgo		Raro	Improbable	Probable	Altamente probable	Casi certeza
Impacto	Muy bajo	D	D	D	B	B
	Bajo	D	B	B	M	M
	Medio	B	M	M	I	I
	Muy alto	M	I	I	C	C
	Alto	I	C	C	C	C



Las siglas y colores de las tablas se corresponden con los niveles de riesgos siguientes:

- D - Verde claro: Nivel de riesgo despreciable.
- B - Verde oscuro: Nivel de riesgo bajo.
- M - Amarillo: Nivel de riesgo moderado.
- I - Naranja: Nivel de riesgo importante.
- C - Rojo: Nivel de riesgo crítico.

Atendiendo al nivel de riesgo estimado para cada amenaza y activo, la actuación de la organización sobre estos deberá ser diferente, dando prioridad a aquellos pares con mayor riesgo y aplazando la actuación de aquellos pares cuyo nivel de riesgo sea inferior .

### **15. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO**

Para evaluar el riesgo estimado de cada par activo/amenaza, deberá tenerse en cuenta su ubicación dentro de la matriz impacto/probabilidad mostrada en el epígrafe anterior.

Los criterios a tener en cuenta son los siguientes:

- Si el riesgo está situado en una zona de riesgo crítico, su probabilidad es "improbable": "probable", "altamente probable" o "casi certeza" y su impacto es "alto" o "muy alto": Esto significa que los efectos para la organización pueden ser muy perjudiciales para el correcto desarrollo de su actividad y se aconseja eliminar la actividad que ocasiona el riesgo siempre que sea posible o, por lo menos, reducirla.

Además, la organización deberá diseñar planes de contingencia que permitan la restauración del sistema de información lo antes posible en caso de materializarse la amenaza.

- Por otro lado, si el riesgo está situado en una zona de riesgo despreciable, su probabilidad será "raro": "improbable" o "probable" y su impacto "muy bajo" o "bajo": En este caso, será un riesgo asumible por la organización y no será necesaria la implantación de medidas adicionales que lo reduzcan o lo eliminen.

En el caso de que el riesgo esté ubicado en las otras zonas (niveles de riesgo "bajo": "moderado" o "importante"), la organización deberá valorar la importancia y el coste de establecer medidas correctivas que disminuyan o eliminen los riesgos de cada activo.

Se tendrá que evaluar caso por caso para determinar si la implantación de la medida correctiva compensa para la reducción de riesgo que se puede obtener con ello. Es decir, deberá realizarse un análisis costes/beneficios que permita tomar decisiones sobre si eliminar, reducir o compartir el riesgo evaluado.

Por ejemplo, si la implantación de una medida reductora conlleva un coste muy elevado y solo consigue reducir levemente el nivel de riesgo, no compensará implantarla y deberá omitirse. Por el contrario, si con una medida correctiva de bajo coste se consiguen eliminar considerablemente

riesgos importantes, la organización no deberá dudar en implantarla e incluirla dentro del sistema de información.

**Nota**

A medida que se aumente el nivel de riesgo de cada par amenaza/activo, mayor atención deberá prestar la organización para evaluar los posibles daños de su ocurrencia y valorar las posibles medidas de seguridad que puedan reducirlos.

Con la evaluación de cada riesgo por separado, la organización obtendrá información valiosa que le permitirá:

- Establecer la probabilidad de materialización de amenazas que puedan afectar a la correcta actividad de la organización y que puedan obstaculizar el cumplimiento de sus objetivos.
- Calcular y estimar el impacto de las amenazas sobre las personas y los demás activos y recursos de la organización. Con ello, podrá seleccionar los activos con más impacto y establecer medidas que les otorguen una mayor protección ante posibles amenazas.
- Establecer criterios de valoración, calificación y evaluación de los riesgos que permita realizar una toma de decisiones de seguridad adecuadas para garantizar el correcto funcionamiento de la organización.

**15.1.-Visión general de la gestión de riesgos**

A estas alturas del capítulo, se han detallado muchas fases y conceptos referentes a la gestión de riesgos. Por eso, es necesario englobarlos todos para obtener una visión global que facilite su comprensión y permita seguir avanzado con las medidas correctivas y las distintas metodologías de análisis de riesgo.

A modo de resumen, en el siguiente cuadro se relacionan todos los conceptos que han sido mencionados y descritos con detenimiento a lo largo del capítulo.



El gráfico se concreta en una serie de puntos clave

1. Las amenazas se materializan sobre los activos, a los que degradan, y ocurren con una frecuencia estimada.
2. El valor de los activos es lo que les da importancia dentro de una organización.
3. El valor de los activos y su degradación son los que permiten calcular el impacto de una amenaza.
4. Por otro lado, la frecuencia con la que se materializa la amenaza y el impacto de esta sobre un activo determinarán su nivel de riesgo.
5. Para mitigar el riesgo están las salvaguardas, que lo llevarán a cabo limitando el impacto o reduciendo la frecuencia de la amenaza, llegando así a la estimación del riesgo residual (nivel de riesgo reducido por la protección de las salvaguardas).

## 16. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS

En función del nivel del riesgo al que se someten los distintos activos del sistema de información de una organización, se encuentran varias alternativas para proceder a su gestión.

Estas alternativas se fundamentan en los controles, definidos como aquellas medidas de seguridad cuyo objetivo fundamental es reducir o limitar el riesgo todo lo posible.

La política de gestión de riesgos de la organización decidirá qué tipo de control se va a implantar en su sistema de información, distinguiendo entre:

- **Controles disuasorios:** se trata de controles cuya función principal es reducir la probabilidad de ocurrencia del incidente (de materialización de la amenaza). Un ejemplo sería el establecimiento de controles de acceso para evitar intrusiones no deseadas.
- **Controles preventivos:** tienen como objetivo reducir la vulnerabilidad de los activos y de sus salvaguardas para limitar las posibilidades de entrada de cualquier amenaza. Ejemplo de ello son las actualizaciones y parches de las aplicaciones que, instalándolos periódicamente, permiten la reducción de sus vulnerabilidades lo máximo posible.
- **Controles detectores:** detectan el incidente cuando este se está produciendo o ya se ha producido. Por ejemplo, cuando un antivirus detecta la entrada de un virus en el sistema, la incidencia ya se ha producido, pero ha sido identificada por un control (en este caso, el antivirus).
- **Controles correctivos:** su actuación se limita a momentos posteriores del incidente. Se encargan de limitar sus efectos perjudiciales, de intentar recuperar la situación anterior a la materialización de la amenaza. Un ejemplo claro de control correctivo es la utilización de copias de respaldo.

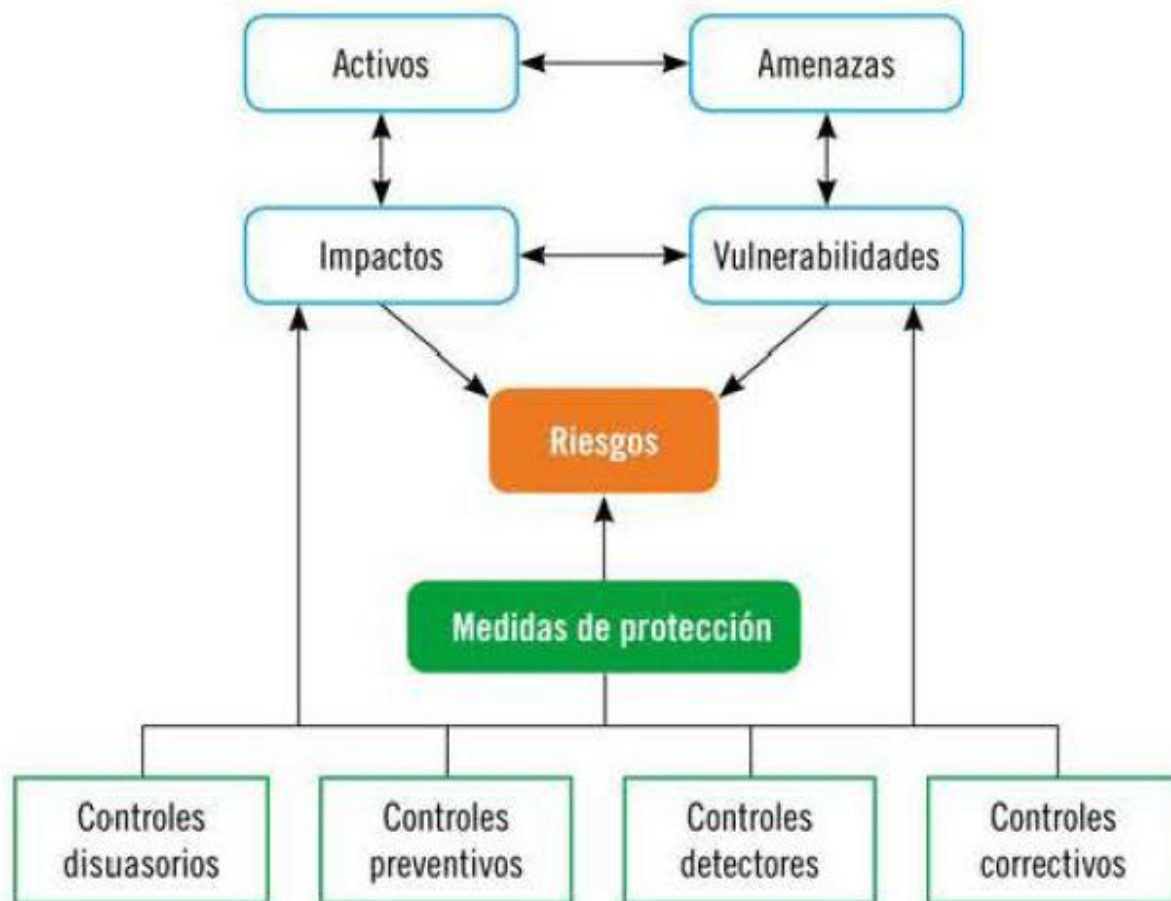


Cualquiera de estos controles permite la reducción del riesgo de los activos y de la organización. Aunque una estrategia sería seleccionar un tipo de control e implantarlo, no es lo adecuado.

Se recomienda utilizar todos los controles según el tipo de activo/amenaza y la estrategia que se pretenda seguir con cada uno de ellos.

Por ejemplo, si un activo tiene numerosas vulnerabilidades, requerirá la implantación de un control preventivo. Pero, aun así, se recomienda el establecimiento de controles detectores que puedan detectar a tiempo la incidencia (si el control preventivo no ha funcionado) y de controles correctivos que restauren el sistema con la mayor brevedad posible.

De este modo, el establecimiento conjunto de todas las tipologías de controles permitirá la reducción del riesgo general de la organización al reducir todos *sus* componentes fundamentales, como se observa en la siguiente tabla.



Al reducir el impacto de las amenazas y la aparición de vulnerabilidades, se reduce la probabilidad de materialización de amenazas y, como consecuencia, la degradación de los activos, disminuyendo así el nivel general de riesgo del activo.

## 17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Sea cual sea la metodología que se utilice para diseñar e implantar el plan de gestión de riesgos, siempre hay una serie de recomendaciones aconsejables para que el desarrollo se adecúe a los objetivos de la organización y se consigan unos resultados óptimos.

### 17.1.-Recomendaciones básicas para la elaboración del plan

Las recomendaciones básicas para la elaboración del plan de gestión de riesgos se describen a continuación.

### 1. Conocer y entender el funcionamiento de la administración de riesgos activo, salvaguarda, etc.

Sobre todo, debe conocer todos los factores necesarios para la definición y estimación de los riesgos:

- Amenaza: ¿qué puede suceder?
- Probabilidad: ¿qué posibilidades hay de que suceda? ¿Con qué frecuencia?
- Impacto: ¿qué efectos perjudiciales puede ocasionar la amenaza si se materializa?
- Activo: ¿qué recursos pueden verse afectados?
- Salvaguarda: ¿cómo puede reducirse el riesgo?

### 2. Definir las acciones del plan de gestión de riesgos

Deben establecerse acciones como los activos que se quieren evaluar, las posibles amenazas que se pueden materializar, qué metodología se va a utilizar, cuáles serán los umbrales de riesgo aceptables, etc.

#### Importante

Aunque las organizaciones tienen puntos en común, cada una de ellas debe diseñar un plan de gestión de riesgos propio. Mientras que un equipo no tiene valor para una organización, puede ser de gran valor para otra. En este caso, el impacto asignado para el mismo activo será diferente según la organización que lo asigne.

### 3. Conseguir el apoyo de la dirección y de profesionales externos

En casos en los que la reducción o eliminación del riesgo conlleva un coste elevado, se recomienda recurrir a profesionales externos que permitan la gestión del riesgo con menores costes y delegación de responsabilidades.

Por otro lado, los encargados de la gestión de riesgos deben contar con el apoyo de la dirección para que la actuación sea acorde con la misión global de la dirección y se integre como una actividad de esta.

### 4. Identificar las consecuencias de cada riesgo

Teniendo en cuenta que cada riesgo conlleva consecuencias con perjuicios distintos, deben poder identificarse y valorar para conocer qué riesgos es necesario priorizar y atajar con más inmediatez.

## **5. Eliminar las amenazas irrelevantes**

Deberán descartarse aquellas amenazas cuyo impacto y probabilidad de ocurrencia sean mínimos para concentrar los recursos y esfuerzos en amenazas que puedan afectar a activos de alto valor, con la elaboración de un plan de contingencia.

## **6. Inventariar los activos susceptibles de riesgo**

Para tener controlados los riesgos, se recomienda tener un inventario de todos los activos de valor susceptibles de sufrir alguna amenaza. El inventario deberá actualizarse con cierta periodicidad.

## **7. Asignar probabilidades**

Para cada activo, deberán asignarse las probabilidades de materialización de cada activo y la frecuencia con la que se pueden producir.

## **8. Asignar el impacto**

Una vez asignadas las probabilidades, hay que asignar el grado de degradación que sufriría cada activo en caso de producirse la amenaza.

### **Recuerde**

Las probabilidades y el impacto designados para cada amenaza pueden darse en valores numéricos o en escalas cualitativas tipo "muy alto", "alto", "medio", "bajo", etc.

## **9. Determinar el riesgo para cada activo**

Con las probabilidades y los impactos estimados para cada activo, deberá calcularse una combinación de ambos factores para estimar el riesgo potencial de cada activo.

## **10. Clasificar los riesgos**

Con los riesgos calculados para cada activo, deberá elaborarse una lista con todos ellos siguiendo un orden de prioridad de actuación: a mayor riesgo, mayor prioridad de actuación y viceversa.

## **11. Calcular el riesgo total**

Se calculará el riesgo total del sistema de información de la organización haciendo un promedio aritmético de todos los riesgos calculados de cada activo.

Por ejemplo, una organización con unos activos de riesgo 0,5, 0,8 y 0,9 tendrá un riesgo global de 0,73  $(0,5+0,8+0,9)/3$ .

## **12. Diseñar estrategias de reducción de riesgos**

Para reducir el riesgo global de la organización, deberán tomarse decisiones de actuación sobre qué tipos de controles se pueden implantar y qué efectos pueden tener sobre los riesgos de la organización.

## **13. Desarrollar planes de contingencia**

Para los riesgos más importantes (que afectan a activos más valiosos y ocurren con más frecuencia) deberá diseñarse un plan de contingencia que permita reducirlos en el menor tiempo posible y restituir la situación previa, evitando que los daños ocasionados se expandan.

### **Nota**

Los planes de contingencia solo se utilizarán para riesgos de gran valor. No tiene sentido malgastar recursos para riesgos que no afectan a la actividad habitual de una organización.

## **14. Analizar la efectividad de las estrategias implantadas**

Una vez puesta en marcha la gestión de riesgos y las salvaguardas y controles previstos, deberá analizarse de nuevo el riesgo para cada activo y el riesgo global de la organización. Si los riesgos no se han reducido o la reducción ha sido mínima, significará que las medidas implantadas no son eficaces y será necesaria una nueva evaluación para detectar en qué fallan y cómo pueden solucionarse.

Por el contrario, si se consigue reducir aceptablemente el riesgo, significará que los controles y salvaguardas son los correctos y que la gestión de riesgos se está llevando a cabo de un modo adecuado.

## **18. EXPOSICIÓN DE LA METODOLOGÍA NIST SP 800-30**

El Instituto Nacional de Normas y Tecnología (*National Institute of Standards and Technology* o NIST) lleva editando desde los años noventa una serie de publicaciones referidas a la seguridad de la información.



**Sabía que...**

El Instituto Nacional de Normas y Tecnología está establecido en Estados Unidos y su función principal es la promoción de la innovación y de la competencia industrial del país.

Dentro de estas publicaciones, está incluida la metodología NIST SPS00-30, una metodología específica para el análisis y gestión de riesgos, acorde con las demás publicaciones que forman parte de la serie.

Esta metodología desarrolla la gestión y análisis de riesgo a través de nueve pasos básicos:

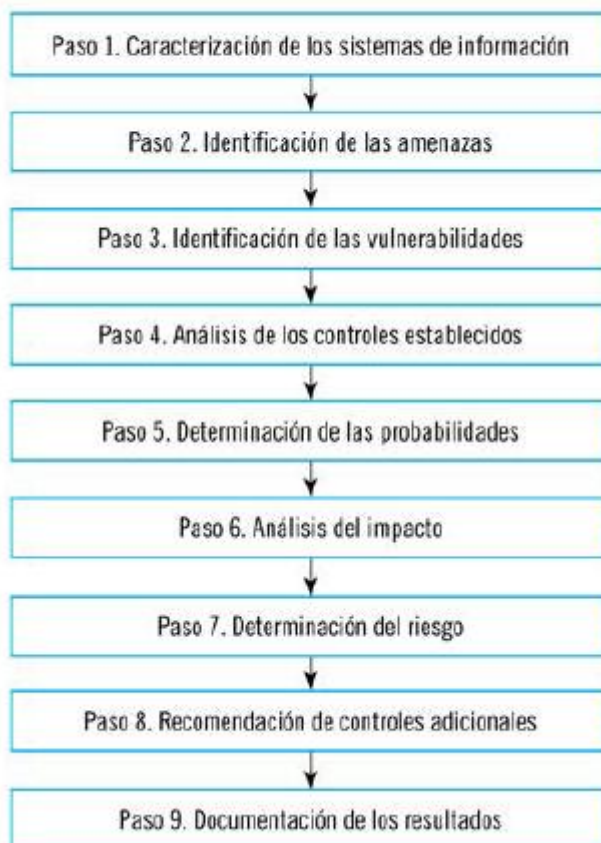
1. Caracterización del sistema: en la primera fase de la gestión del riesgo debe estudiarse el sistema de información para conocer los activos que se van a evaluar (*hardware, software, información, recursos humanos, etc.*) y las funciones de cada uno de ellos.
2. Identificación de la amenaza: con un estudio de las amenazas materializadas en veces anteriores se pueden definir las amenazas que pueden producirse nuevamente en el sistema.
3. Identificación de las vulnerabilidades del sistema: para ello, se deben analizar los informes de evaluación de riesgos anteriores, los informes de auditoría, los requerimientos de seguridad, etc.
4. Análisis de los controles establecidos: se elabora una lista con todos los controles implantados en el sistema y con los que se prevé que se van a implantar en momentos posteriores.

**Nota:** En la fase de análisis de controles, también se analizan las salvaguardas establecidas y sus vulnerabilidades para poder estimar el impacto y el riesgo residuales de la organización.

5. Determinación de las probabilidades: con el análisis de las amenazas y de las vulnerabilidades se determinarán la probabilidad de materialización de amenazas potenciales y su probabilidad estimada de frecuencia.
6. Análisis del impacto de la amenaza: se analiza el grado de degradación del activo en términos de pérdidas de integridad, confidencialidad y disponibilidad en el caso hipotético de producirse una amenaza para priorizar los activos más valiosos y susceptibles.
7. Determinación del riesgo: con la combinación de los impactos y probabilidades estimadas se calculan los riesgos de cada activo y se asigna un nivel de riesgo a cada uno de ellos para priorizar los que requieren más atención.
8. Recomendación de controles adicionales: analizados los resultados obtenidos en la evaluación de riesgo, se proponen una serie de controles adicionales que puedan reducir el nivel de riesgo de cada activo y el global de toda la organización.

9. Documentación de los resultados del análisis: todas las acciones ejecutadas en el proceso de gestión de riesgos debe documentarse debidamente para poder elaborar un informe de valoración de riesgos con los resultados obtenidos en el análisis.

**Fases del análisis y gestión de riesgos según la metodología NIST SP800-30**



## 19. EXPOSICIÓN DE LA METODOLOGÍA MAGERIT VERSIÓN 2

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas o Metodología Magerit fue diseñada por el CSAE (Consejo Superior de Administración Electrónica) y es de carácter público.

Su primera versión data de 1997, la segunda de 2005 y la tercera (que es la vigente en la actualidad) fue publicada en 2012, convirtiéndose en un referente para el desarrollo de planes de riesgo de las organizaciones a nivel nacional.

Entre los principales objetivos de esta metodología, cabe destacar los siguientes:

- La concienciación de los encargados de los sistemas de información de la existencia de riesgos y de la importancia de una gestión de riesgos adecuada.

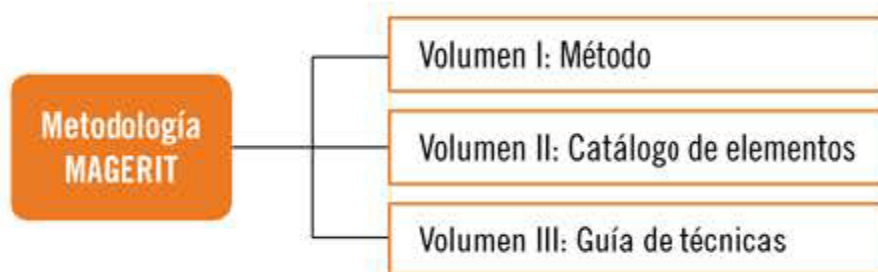
- Facilitar una metodología que permita analizar sistemáticamente los riesgos de las organizaciones.
- Proporcionar un apoyo a las organizaciones para que sean capaces de diseñar sus propias medidas para combatir los riesgos de sus activos.

Además, hay que añadir un objetivo indirecto: Magerit fue diseñada para que las organizaciones sean capaces de adaptar sus tareas a los procesos de evaluación, certificación, auditoría o acreditación necesarios, según el caso, para conseguir mantener unos estándares de calidad en sus actividades.

### 19.1.-Estructura de las guías Magerit

Las guías Magerit ofrecen un marco de trabajo para que las organizaciones sean capaces de gestionar sus riesgos eficientemente. Esta metodología está formada por tres volúmenes:

- **Volumen I: Método.** Se considera el volumen principal de la metodología Magerit, ya que se explica con detalle cómo desarrollarla.
- **Volumen II: Catálogo de elementos.** Es un complemento del volumen I y en este se incluyen ejemplos y tipos de elementos que pueden ser activos, salvaguardas, amenazas y vulnerabilidades. También se incluyen dimensiones de valoración y criterios de valoración.
- **Volumen III: Guía de técnicas.** También es un complemento del volumen I y en él se describen algunas técnicas que pueden utilizarse en cada fase del proceso de análisis y gestión de riesgos.



### Metodología Magerit

Como se ha dicho, la metodología Magerit está incluida en su volumen I. Este volumen se divide en ocho capítulos y seis epígrafes.

#### Capítulo I: Introducción

Se trata de un capítulo introductorio, en el que se describen los organismos que elaboraron y promulgaron esta metodología. También se destaca la importancia de la gestión de riesgos para las organizaciones.

### *Capítulo II: Visión de conjunto*

Se describen los conceptos referentes a la gestión de riesgos de un modo introductorio para ofrecer una visión global de la importancia de la materia.

### *Capítulo III: Método de análisis de riesgos*

Aquí ya se describe con profundidad la metodología para identificar y valorar los activos, amenazas, vulnerabilidades y salvaguardas, además de ofrecer una guía para estimar adecuadamente el impacto y el riesgo (tanto residuales como potenciales) de los sistemas de información.

En este capítulo se ofrece la suficiente información para que la organización, además de estimar los riesgos de cada activo, sea capaz de estimar su nivel de riesgo global.

### *Capítulo IV: Proceso de gestión de riesgos*

El capítulo IV de Magerit incluye todas las actividades que se realizan en el proceso de gestión de riesgos. Cabe destacar las siguientes actividades:

- Evaluación de los niveles de impacto y riesgos residuales.
- Determinación de los niveles aceptables de riesgo.
- Estudios cualitativos y cuantitativos de costes/beneficios.
- Estrategias de tratamiento del riesgo: eliminación, mitigación, compartición y financiación.
- Documentación del proceso.

### *Capítulo V: Proyectos de análisis de riesgos*

Este capítulo está centrado en los proyectos que se efectúan cuando las organizaciones desarrollan su primer análisis de riesgos y en sus posteriores revisiones y actualizaciones.

### *Capítulo VI: Plan de seguridad*

En el capítulo VI se hace referencia a las actividades necesarias para desarrollar un plan de seguridad por parte de las organizaciones. Este plan de seguridad se debe desarrollar una vez finalizadas las tareas de análisis y gestión de riesgos e incluye recomendaciones para una toma de decisiones apropiada.

**Nota**

El capítulo VI hace referencia más concretamente a las tareas necesarias para identificar, planificar y ejecutar los proyectos de seguridad de la organización. Además, facilita una tabla que puede ayudar para comprobar si los planes de seguridad definidos son adecuados y pertinentes.

*Capítulo VII: Desarrollo de sistemas de información*

Este capítulo se enfoca específicamente en los sistemas de información y aplica las tareas y conceptos de gestión de riesgos descritos hasta el momento a las particularidades de las tecnologías de la información y comunicación para una mayor eficacia y reducción de los riesgos de estos sistemas.

*Capítulo VIII: Consejos prácticos a lo largo de toda la guía.**Epígrafes:*

Son seis epígrafes en los que se incluyen:

- Un glosario con los términos principales de la gestión de riesgos tanto en español como en inglés.
- Las referencias de la bibliografía utilizada para la elaboración de la guía.
- El marco legal de la seguridad de los sistemas de información.
- El marco de evaluación y certificación de los sistemas de gestión de la seguridad de la información.
- La herramienta Pilar: herramienta para la gestión de riesgos que utilizan las Administraciones Públicas en España.
- La evolución de la metodología Magerit en sus versiones v1 y v2 respecto a la última versión.

**20. RESUMEN**

Un riesgo es cualquier tipo de evento o conjunto de eventos que puede poner en riesgo un proyecto de la organización o impedir el cumplimiento de sus objetivos.

A pesar de existir varios tipos de riesgo, la gestión de riesgos es un conjunto de procesos con la finalidad de disminuir la probabilidad de amenazas y ataques sobre los activos más importantes de la organización.

El procedimiento de gestión de riesgos sigue unas fases bien marcadas. En primer lugar, se identifican y valoran los activos de la organización y la degradación que pueden sufrir en caso de materializarse una amenaza (impacto).

Una vez identificados los activos y los impactos, se deben identificar y analizar las vulnerabilidades de estos con el fin de estimar la frecuencia y probabilidad de materialización de amenazas y cómo poder reducirlas.

Con el impacto y las probabilidades estimadas, se puede proceder a calcular el riesgo potencial de cada activo y, conjuntamente, el riesgo potencial global de la organización.

Además, con el análisis de las salvaguardas se podrá conocer el riesgo residual y evaluar si estas están cumpliendo con su cometido o si, por el contrario, necesitan tareas de revisión.

El análisis y gestión de riesgos permite a las organizaciones definir estrategias para reducir la probabilidad de ocurrencia de amenazas y el daño que estas pueden causar en caso de materializarse. Por ello, no son pocos los organismos encargados de diseñar herramientas y metodologías que sirvan de guía a las organizaciones para que estas elaboren políticas propias de gestión de riesgos; a destacar la metodología Magerit (de carácter nacional) y la metodología NIST SP 800-30 (de carácter internacional).

## **CAPÍTULO 4 USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS**

### **1. INTRODUCCIÓN**

Los auditores de seguridad informática, para desarrollar sus tareas y buscar posibles fallos y amenazas del sistema de información, muy frecuentemente se apoyan en herramientas que analizan cada uno de los distintos aspectos de la auditoría.

Debido a la gran variedad de vulnerabilidades existentes, las herramientas encargadas de su detección y análisis son abundantes y variadas.

Aunque la experiencia y los conocimientos del auditor son imprescindibles para el correcto desarrollo de la auditoría, siempre es recomendable que el auditor disponga de herramientas de análisis de red, puertos y servicios, herramientas de análisis de protocolos, herramientas de ataque de diccionario y de fuerza bruta, etc., además de las herramientas internas de cada sistema operativo.

En este capítulo, se describen las herramientas principales para la auditoría de sistemas y las funcionalidades destacadas de varias de ellas.

### **2. HERRAMIENTAS DEL SISTEMA OPERATIVO TIPO PING, TRACEROUTE, ETC.**

Dentro de las tareas de la auditoría informática, está la comprobación del correcto funcionamiento de las redes del sistema de información.

Para ello, hay dos herramientas fundamentales: ping y traceroute, entre otras.

En ambas herramientas, se puede detectar si existe alguna anomalía de red, comprobar el alcance de esta anomalía y, además, cuáles han sido los servicios que se han hecho inaccesibles por la incidencia.

#### **2.1.- Herramienta ping**

El nombre de la herramienta ping proviene de packet internet groper (rastreador de paquetes de red) y se puede utilizar en cualquier sistema operativo accediendo mediante comandos.

Se utiliza fundamentalmente para comprobar la calidad y la velocidad de una red determinada y para comprobar la latencia entre dos equipos.

**Nota**

La latencia es el tiempo de respuesta existente entre dos equipos. El comando ping mide el tiempo que tarda el equipo de destino en devolver una respuesta ante el envío de paquetes de datos.

Su funcionamiento es bastante simple: a través del comando ping, la herramienta envía una serie de paquetes ICMP de solicitud y respuesta y devuelve unos resultados en los que se permite verificar si el destino de los paquetes está activo.

Utilizando Microsoft Windows, habrá que abrir MS-DOS seleccionando el acceso directo de Símbolo del sistema o escribiendo el comando cmd en el cuadro de texto del desplegable.



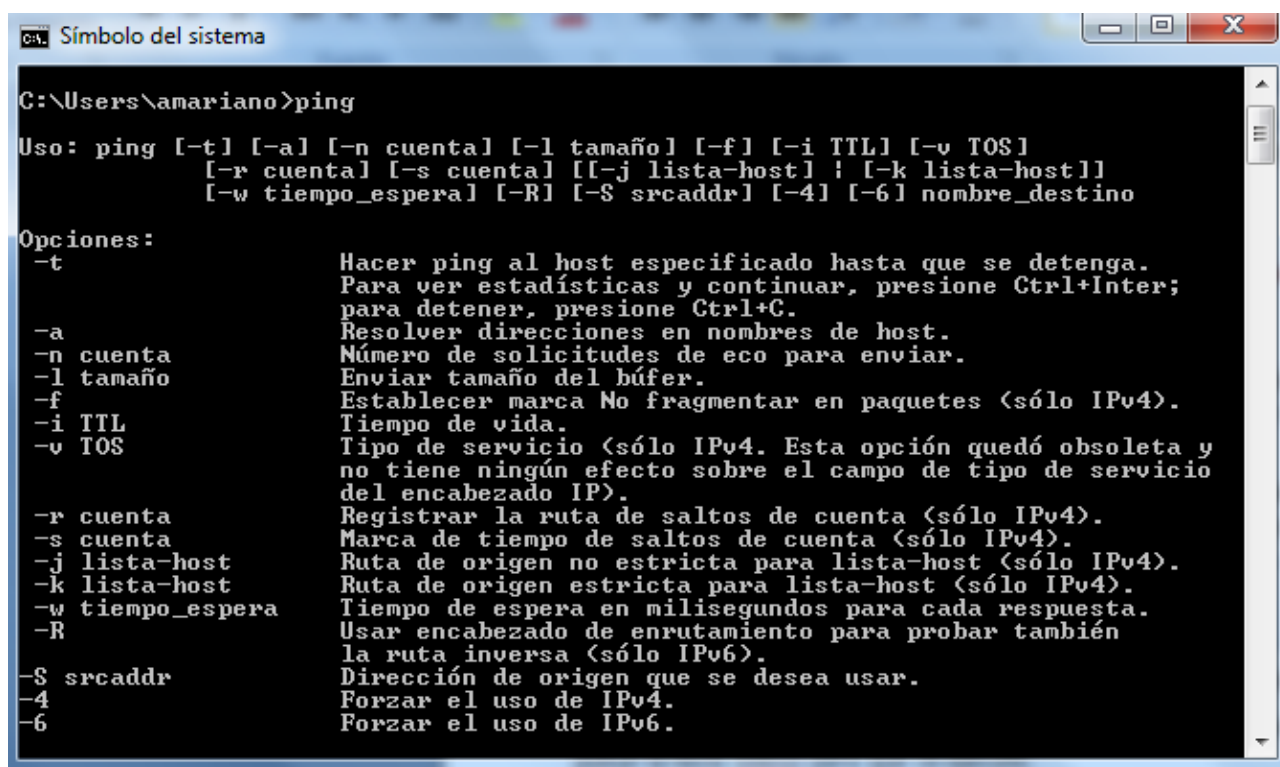
## Símbolo del sistema

Microsoft Windows, Acceso directo de Símbolo del sistema

Al introducir el comando, se abrirá la ventana de MS-DOS y bastará con escribir el comando ping y pulsar la tecla [Intro] para que se ejecute.

En Linux y otros sistemas operativos, el procedimiento será el mismo desde la consola de comandos de cada uno de ellos.





```

C:\Users\amariano>ping

Uso: ping [-t] [-a] [-n cuenta] [-l tamaño] [-f] [-i TTL] [-v TOS]
        [-r cuenta] [-s cuenta] [[-j lista-host] ! [-k lista-host]]
        [-w tiempo_espera] [-R] [-S srcaddr] [-4] [-6] nombre_destino

Opciones:
-t          Hacer ping al host especificado hasta que se detenga.
            Para ver estadísticas y continuar, presione Ctrl+Inter;
            para detener, presione Ctrl+C.
-a          Resolver direcciones en nombres de host.
-n cuenta  Número de solicitudes de eco para enviar.
-l tamaño  Enviar tamaño del búfer.
-f          Establecer marca No fragmentar en paquetes (sólo IPv4).
-i TTL     Tiempo de vida.
-v TOS     Tipo de servicio (sólo IPv4. Esta opción quedó obsoleta y
            no tiene ningún efecto sobre el campo de tipo de servicio
            del encabezado IP).
-r cuenta  Registrar la ruta de saltos de cuenta (sólo IPv4).
-s cuenta  Marca de tiempo de saltos de cuenta (sólo IPv4).
-j lista-host Ruta de origen no estricta para lista-host (sólo IPv4).
-k lista-host Ruta de origen estricta para lista-host (sólo IPv4).
-w tiempo_espera Tiempo de espera en milisegundos para cada respuesta.
-R          Usar encabezado de enrutamiento para probar también
            la ruta inversa (sólo IPv6).
-S srcaddr Dirección de origen que se desea usar.
-4          Forzar el uso de IPv4.
-6          Forzar el uso de IPv6.
  
```

Ejecución del comando ping

Como se puede comprobar en la imagen, todos los paquetes enviados han sido recibidos correctamente (tal como se indica en 0% perdidos), por lo que no se detecta ningún fallo de la red.

El comando también muestra el tiempo máximo de ida y vuelta del paquete de datos. Se considera un tiempo de respuesta lento y un posible fallo en la red cuando el tiempo de ida y vuelta supera los 200 ms.

En esta ocasión, el tiempo de respuesta está entre 62 y 66 ms, lo que se considera un tiempo correcto y una velocidad adecuada de transmisión de datos.

### Verificación del funcionamiento de la red con el comando ping

El comando ping debe ir seguido de una dirección (IP, una URL, el IP de una red local, etc.) para comprobar el correcto funcionamiento de la red.

Según la dirección que se introduzca, se verificará su funcionamiento en unos puntos específicos u otros, como se muestra en la tabla siguiente.

Comando	Verificación
<b>ping localhost</b>	Se verifica si los protocolos TCP/IP están instalados y si funcionan correctamente.
<b>ping 192.168.1.1</b>	Permite verificar el correcto funcionamiento del cableado general de la red.
<b>ping www.google.es</b>	Introduciendo la dirección URL de una web, se puede verificar el correcto funcionamiento de las direcciones IP de los servidores DNS

Además, añadiendo después del comando ping la dirección IP del equipo local, se puede verificar si este ha sido agregado correctamente a la red evaluada.

## 2.2.- Herramienta traceroute

La herramienta traceroute se utiliza para seguir la ruta de los paquetes en una red IP y el retardo que se produce en este tránsito.

Se puede utilizar en varios sistemas operativos, pero hay que tener en cuenta que en Microsoft Windows esta herramienta se llama tracert.

En Linux, se ejecuta el comando traceroute en la consola de comandos y, en Windows, se escribirá el comando tracert dentro de la ventana de MS-DOS que surge al escribir cmd en el símbolo del sistema.

Sea en el sistema operativo que sea, después del comando debe escribirse la dirección URL o el host destino que se quiera utilizar para comprobar la ruta que sigue el paquete de datos.

Por ejemplo, si se quiere verificar la ruta hasta la URL www.google.es en Microsoft Windows, solo debe escribirse tracert www.google.es. El resultado será el que muestra la siguiente imagen.

```

C:\Users\amariano>tracert www.google.es

Traza a la dirección www.google.es [216.58.214.163]
sobre un máximo de 30 saltos:

  1      1 ms    <1 ms    1 ms    192.168.9.1
  2      2 ms    2 ms     2 ms    192.168.144.1
  3      *      *      *      Tiempo de espera agotado para esta solicitud.
  4     25 ms    27 ms    27 ms    225.red-80-58-106.staticip.rima-tde.net [80.58.1
06.225]
  5     24 ms    24 ms    24 ms    176.52.253.97
  6     25 ms    25 ms    26 ms    5.53.1.82
  7     25 ms    26 ms    25 ms    216.239.50.28
  8     25 ms    29 ms    25 ms    216.239.40.219
  9     26 ms    25 ms    25 ms    mad01s26-in-f3.1e100.net [216.58.214.163]

Traza completa.
  
```

Ejecución del comando tracert

Como se observa en la imagen, traceroute o tracert muestra todos los routers y cortafuegos que se ha encontrado el paquete de datos hasta llegar al destino (en este caso han sido 12).

Si en alguno de estos obstáculos se produjera algún fallo o hubiera un retardo excesivo, podría comprobarse con un simple visionado de los resultados ofrecidos por esta herramienta.

Aunque tanto ping como traceroute son herramientas de diagnóstico muy valiosas para conocer el correcto funcionamiento de la red, traceroute tiene una ventaja adicional: si hay algún fallo en la comunicación, la herramienta indica en qué momento se produce dicho fallo y en qué obstáculo (o host) sucede, mientras que ping solo reporta que se ha producido un fallo sin dar muchos más detalles.

### **2.3.- Herramienta whois**

La herramienta whois se utiliza para realizar consultas en una base de datos de Internet con la finalidad de obtener información sobre alguna IP, algún dominio o alguna organización determinados.

Esta herramienta no solo facilita información sobre dominios, IP y organizaciones, sino que también puede llegar a proporcionar información sobre a quién pertenece la IP y hasta dónde se localiza físicamente.

### **2.4.- Herramienta NSLookup**

La herramienta Name System Lookup o NSlookup se utiliza como herramienta de diagnóstico para la detección de problemas de configuración en el DNS.

Esta detección la realiza mediante consultas a un servidor DNS para la obtención de información sobre algún dominio o host de una red determinada.

## **3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS TIPO NMAP, NETCAT, NBTSCAN, ETC.**

En las tareas de auditoría de seguridad informática, también es útil conocer el tráfico de red del sistema de información que se está auditando, además de los puertos y servicios que se utilizan cada vez que se transmiten datos e información.

La variedad de herramientas con funciones de análisis de red, puertos y servicios es muy amplia, siendo muchas de ellas gratuitas, de código abierto y compatibles con varios sistemas operativos (Windows, Linux, etc.).

De estas herramientas, cabe destacar Nmap, Netcat y NBTScan, que se describen a continuación.

### 3.1.- Herramienta Nmap

La aplicación Nmap es gratuita y de código abierto y se utiliza principalmente para la evaluación de la seguridad de sistemas de información.

Su función principal es el rastreo de puertos a través de tareas como:

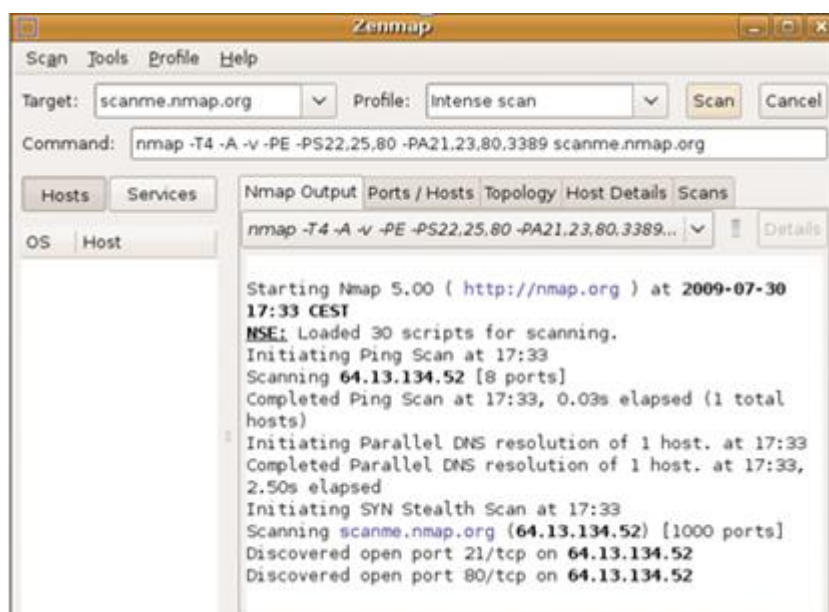
- Identifica los equipos que forman parte de una red y descubre servidores desconocidos.
- Identifica aquellos puertos abiertos de un equipo en concreto.
- Facilita información sobre los servicios que se están ejecutando en el sistema de información.
- Proporciona información sobre el sistema operativo instalado en el equipo indicado.
- También facilita algunas características específicas de los componentes hardware que forman parte de dicho equipo.

Viendo sus tareas, queda bastante claro el objetivo y la utilidad principal de la herramienta Nmap: el descubrimiento e identificación de posibles aplicaciones y equipos no autorizados en el sistema de información.

#### **Nota**

Aunque no es su cometido principal, la herramienta Nmap también se puede utilizar para confeccionar un inventario de los componentes físicos del sistema de información.

En la siguiente imagen, se muestra el funcionamiento de esta herramienta.



Herramienta Nmap

Es necesario remarcar que Nmap no solo se puede utilizar con fines de auditoría de seguridad. Se trata de una herramienta bastante utilizada por hackers: suelen utilizarla para preparar ataques (a los dispositivos detectados) que pueden tener efectos perjudiciales en el sistema de información.

#### Nota

Nmap está solo en inglés y puede conseguirse gratuitamente (junto con manuales de uso) en su sitio web oficial <http://www.insecure.org/nmap>.

### 3.2.- Herramienta Netcat

La herramienta Netcat se ha hecho casi imprescindible en el ámbito de la seguridad informática, hasta tal punto que se denomina comúnmente la "navaja suiza de la seguridad de la red" por sus innumerables posibilidades de uso.

Esta herramienta fue creada en 1995 por Hobbit y sus funciones destacan principalmente en las redes de un sistema, pudiendo realizar casi cualquier cosa con el protocolo TCP/IP.

Netcat funciona a través de comandos y tiene como función principal la apertura de puertos TCP/UDP y la escucha de los datos que se transmiten a través de ellos.

No obstante, cabe destacar también otras funciones como:

- Chat: poniendo uno de los equipos en modo servidor y otro equipo en modo cliente.

- Envío y recepción de ficheros: transmitir ficheros de un equipo cliente a un servidor.
- Escaneo de puertos: se puede optar por escanear todos los puertos de un equipo determinado o decidir qué puertos concretos escanear.
- Servidor web: con Netcat, puede utilizarse el equipo servidor un solo fichero HTML de forma puntual.
- Ejecución de la herramienta en modo silencioso.
- Obtención de una shell para conocer las conexiones del equipo con el sistema operativo Unix.

### Definición

#### Shell

Intérprete de comandos para sistemas operativos Unix y Linux. Conociendo la shell de un equipo, un usuario puede hacer prácticamente de todo en el otro equipo: eliminar, ejecutar o introducir archivos, controlar el comportamiento del equipo, etc.

La línea básica de comandos para Netcat es:

`nc [parámetros] [ip o puerto/rango de puertos que se quieren analizar]`

Entre los parámetros de Netcat cabe destacar los que se muestran en la siguiente tabla.

Parámetros Netcat	
Parámetro	Descripción
<b>-d</b>	Permite que Netcat actúe en modo silencioso.
<b>-l</b>	Activa el modo escucha
<b>-p puerto</b>	Especifica el puerto que se quiere analizar.
<b>-v</b>	Facilita información sobre la conexión.
<b>-u</b>	Indica a Netcat que utilice el protocolo UDP en lugar del TCP (protocolo utilizado por defecto).
<b>i segundos</b>	Define un retraso (delay) de tiempo antes de enviar o recibir datos.

<b>-w segundos</b>	Controla cuánto tiempo debe esperar Netcat antes de terminar una conexión.
<b>-r</b>	Permite a Netcat elegir aleatoriamente los puertos locales y remotos.
<b>-z</b>	Escanea puertos.

En la siguiente imagen, se muestra la formulación del comando *Netcat* (nc) junto con los posibles parámetros que se pueden añadir.

```
C:\Netcat-Eq.A>nc -h
[vi.11 NT www.vulnwatch.org/netcat/]
connect to somewhere: nc [-options] hostname port[s] [ports] ...
listen for inbound:  nc -l -p port [options] [hostname] [port]
options:
  -d          detach from console, background mode
  -e prog     inbound program to exec [dangerous!!]
  -g gateway  source-routing hop point[s], up to 8
  -G num      source-routing pointer: 4, 8, 12, ...
  -h          this cruft
  -i secs     delay interval for lines sent, ports scanned
  -l          listen mode, for inbound connects
  -L          listen harder, re-listen on socket close
  -n          numeric-only IP addresses, no DNS
  -o file     hex dump of traffic
  -p port     local port number
  -r          randomize local and remote ports
  -s addr     local source address
  -t          answer TELNET negotiation
  -u          UDP mode
  -v          verbose [use twice to be more verbose]
  -u secs     timeout for connects and final net reads
  -z          zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
```

Parámetros Netcat

Y, a continuación, se muestra un ejemplo de un comando en el que se ejecuta Netcat y los resultados obtenidos.

```

C:\>nc -v -w2 -z 192.168.248.128 120-140
192.168.248.128: inverse host lookup failed: h_errno 11004: NO_DATA
<UNKNOWN> [192.168.248.128] 140 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 139 <netbios-ssn>: TIMEDOUT
<UNKNOWN> [192.168.248.128] 138 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 137 <netbios-ns>: TIMEDOUT
<UNKNOWN> [192.168.248.128] 136 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 135 <epmap>: TIMEDOUT
<UNKNOWN> [192.168.248.128] 134 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 133 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 132 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 131 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 130 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 129 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 128 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 127 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 126 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 125 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 124 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 123 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 122 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 121 (?): TIMEDOUT
<UNKNOWN> [192.168.248.128] 120 (?): TIMEDOUT
  
```

Comando Netcat

Viendo el ejemplo, se puede observar que el comando está formado por:

- Nc.
- Parámetros:
  - v: ofrece información de la conexión.
  - w2: Netcat debe esperar 2 segundos antes de terminar una conexión.
  - z: escanea los puertos definidos.
- Dirección IP: 192.168.248.128.
- Puertos a escanear: 120-140 (todos los comprendidos en este intervalo).

La herramienta es de libre distribución y se puede utilizar en varios sistemas operativos como Windows o Linux.

- Parámetro en el que se ordena el modo silencioso: -d.
- Dirección IP a analizar: 192.168.346.110.
- Puertos que se quieren escanear: 115- 135.

Teniendo en cuenta todos estos conceptos, el comando a introducir sería el conjunto de todos ellos:

```
nc -v -z -d 192.168.346.110 115-135
```

### 3.3.- Herramienta de red NBTScan

NBTScan es una herramienta que funciona con comandos y que escanea los servidores NetBIOS en una red TCP/IP local o remota.

Se puede utilizar en Windows y Linux, entre otros sistemas operativos, y es gratuita. No obstante, no es una aplicación de código libre, ya que su creador no ha publicado su código fuente.



**Nota**

NBTScan puede encontrarse en la web de su creador:

<http://www.unixwiz.net/tools/nbtscan.html>.

Del mismo modo que Netcat, también ofrece multitud de funcionalidades, destacando:

- Escaneo de puertos.
- Búsqueda de servidores de nombres NetBIOS.
- Identificación de sistemas GNU/Linux que ejecutan servidores SAMBA.
- Construcción de listas compuestas exclusivamente por los servidores que comparten recursos.
- Acceso a un recurso compartido.
- Envío de archivos al recurso compartido.

**Definición****NetBIOS**

Capa de software que permite la comunicación entre una red y un dispositivo de hardware. La dirección NetBIOS es aquella que permite identificar a cada equipo dentro de una red local.

Su funcionamiento básico es bastante simple: se envían peticiones de estados de *NetBIOS* a una dirección o a un rango de estas y para cada servidor que responde se obtiene la siguiente información:

- Su dirección.
- Su nombre *NetBIOS*.
- El nombre de usuario con la sesión iniciada en el equipo.
- Su dirección MAC.

## Definición

### Dirección MAC

Dirección física que permite identificar cada dispositivo de una red de forma única. Las direcciones MAC son únicas a nivel mundial.

En la siguiente imagen, se muestra la utilización del comando de la herramienta *NBTScan* junto con sus posibles parámetros.

```

C:\Users\abento>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a <adapter status> Lists the remote machine's name table given its name
-A <Adapter status> Lists the remote machine's name table given its
                    IP address.
-c <cache>          Lists NBT's cache of remote [machine] names and their IP
addresses
-n <names>          Lists local NetBIOS names.
-r <resolved>       Lists names resolved by broadcast and via WINS
-R <Reload>         Purges and reloads the remote cache name table
-S <Sessions>       Lists sessions table with the destination IP addresses
-s <sessions>       Lists sessions table converting destination IP
                    addresses to computer NETBIOS names.
-RR <ReleaseRefresh> Sends Name Release packets to WINS and then, starts Refr
esh

RemoteName  Remote host machine name.
IP address   Dotted decimal representation of the IP address.
interval    Redisplays selected statistics, pausing interval seconds
            between each display. Press Ctrl+C to stop redisplaying
            statistics.

C:\Users\abento>
  
```

Parámetros de la herramienta NBTScan

En la siguiente imagen, se muestra un ejemplo de la utilización de la herramienta.

```

C:\Rix World\apps\nbtscan\nbtscan_1_0_3\nbtscan -r 10.0.0.0/24
Warning: -r option not supported under Windows. Running without it.

Doing NBT name scan for addresses from 10.0.0.0/24

IP address      NetBIOS Name    Server    User          MAC address
-----
10.0.0.1        APP1             <server>   APP1          00-50-8b-a0-f7-c2
10.0.0.2        PRINT1           <server>   PRINT1        00-00-00-00-00-00
10.0.0.5        Recvfrom failed: Connection reset by peer
10.0.0.6        Recvfrom failed: Connection reset by peer
10.0.0.13       S-RMV2           <server>   <unknown>     00-53-45-00-00-00
10.0.0.8        EXCH-SRU         <server>   EXCH-SRU      00-08-c7-5d-1f-e2
10.0.0.9        PERSUASIVE-WEB1 <server>   ADC           00-a0-81-05-46-55
10.0.0.12       VER3             <server>   RODGERSJ      00-00-24-c8-83-6f
10.0.0.28       BEN_XL_POWER     <server>   BEN_XL_POWER  00-a0-cc-26-77-99
10.0.0.54       SAMIAM           <server>   SAMIAM        00-a0-c7-5a-a7-fa
10.0.0.58       U-STEWARDIF      <server>   STEWARDIF     00-a0-cc-26-7b-5c
10.0.0.65       L-CLARKET        <server>   CLARKET       00-10-a4-f8-2a-14
10.0.0.75       US9066114-UP01   <server>   JENKINSI      00-50-01-c7-78-e6
10.0.0.81       W-RICHARDS       <server>   RICHARDSE     00-a0-cc-26-78-cb
10.0.0.101      APP2             <server>   APP2          00-02-a5-37-7c-ad
10.0.0.104      U-QUEBKERC       <server>   QUEBKERC      00-c0-a8-f1-48-a8
10.0.0.108      U-MURCHJ         <server>   MURCHJ        00-c0-a8-f1-49-1c
10.0.0.109      U-MILLERJ        <server>   MILLERJ       00-c0-a8-57-74-f9
10.0.0.127      L-DONAHUE        <server>   DONAHUEX      00-10-a4-7b-b5-d3
10.0.0.135      CAROLLAPTOP      <server>   CSTERBINS     00-20-e0-a0-6a-82
10.0.0.203      Recvfrom failed: Connection reset by peer
10.0.0.204      Recvfrom failed: Connection reset by peer
  
```

Parámetros de la herramienta NBTScan

En el ejemplo, se ve claramente la información que facilita la herramienta: dirección IP, nombre NetBios, servidor, usuario con la sesión iniciada y dirección MAC.

Otras herramientas de red: Snort y Network Miner

Además de las herramientas de escaneo de red mencionadas anteriormente, también merece la pena comentar otras dos más:

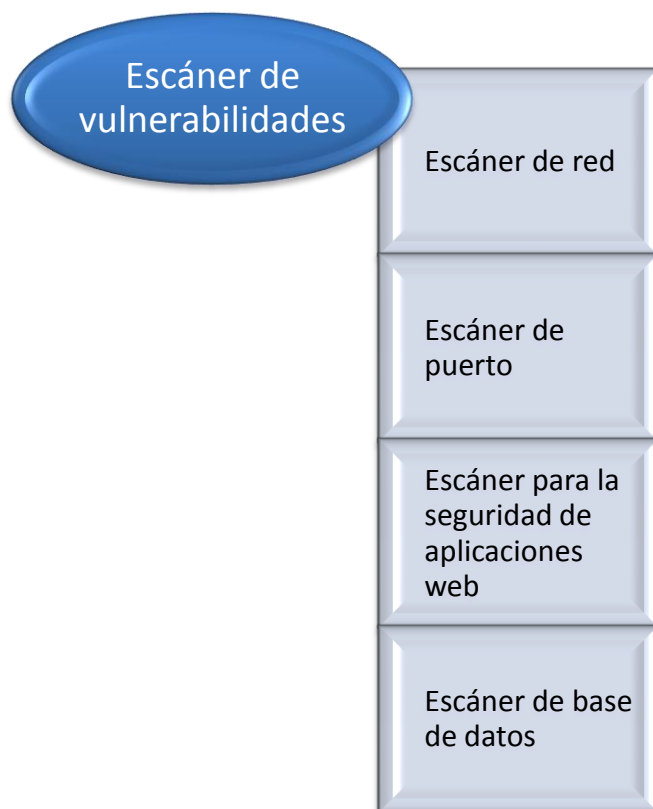
- Snort: se trata de una de las herramientas más utilizadas para detectar intrusiones en la red, aunque también es frecuentemente utilizada como analizador. Dispone de un motor bastante potente para la detección de intrusiones, ataques y realizar escaneos de puertos para registrar todos los eventos destacables y generar alertas en aquellos eventos que supongan un peligro para el sistema de información.
- Network Miner: es actualmente una de las herramientas más utilizadas para el análisis forense digital. Su funcionamiento consiste en la captura y análisis de los paquetes de datos que circulan por una red local (o red LAN).

#### 4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES TIPO NESSUS

Las herramientas de análisis de vulnerabilidades se utilizan para conocer las vulnerabilidades de un sistema de información. Se utilizan sobre todo en las auditorías de seguridad informática, ya que permiten descubrir los puntos débiles del sistema y proponer medidas correctivas que cubran las vulnerabilidades.

Los escáneres de vulnerabilidades se distinguen según el elemento que escanean para detectarlo, distinguiendo entre:

- Escáner de red: se utiliza para encontrar vulnerabilidades de una red de un sistema de información.
- Escáner de puerto: busca los puertos abiertos de una red que puedan ser utilizados por intrusos como vías de entrada.
- Escáner para la seguridad de aplicaciones web: detecta e identifica las vulnerabilidades de las aplicaciones web para estimar su riesgo y poder mitigarlo.
- Escáner de base de datos: detecta vulnerabilidades de las bases de datos, protegiendo uno de los activos más importantes de una organización, la información.

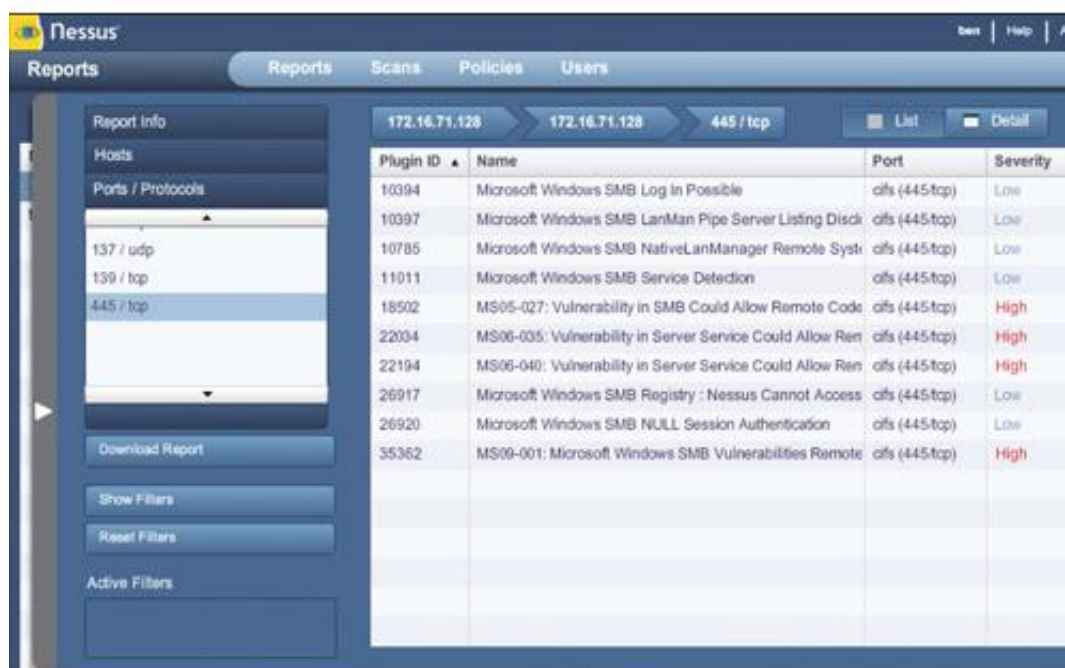


#### 4.1.- Herramienta Nessus

Nessus Security Scanner es una de las herramientas más utilizadas para el análisis de vulnerabilidades de un sistema. Está basada en un modelo cliente/ servidor, lo que permite escanear las vulnerabilidades del equipo cliente desde un equipo servidor.

Su funcionamiento es bastante simple: escanea los puertos para detectar aquellos que están abiertos e intenta enviar ataques a dichos puertos para identificar sus vulnerabilidades.

Una vez detectadas las vulnerabilidades, Nessus emite un informe con las vulnerabilidades identificadas: seleccionando una de ellas, Nessus muestra una descripción de la vulnerabilidad y su posible solución.



Nessus Security Scanner

Esta herramienta está disponible en inglés para varios sistemas operativos en su página web: <http://www.tenable.com/products/nessus>.

## 5. ANALIZADORES DE PROTOCOLOS TIPO WIRESHARK, DSNIFF, CAIN & ABEL, ETC.

Los analizadores de protocolos, también llamados analizadores de red, son herramientas que analizan el tráfico de datos de una red en tiempo real o en momentos posteriores a la captura de los datos. Este análisis lo efectúan mediante la captura, decodificación y transmisión de paquetes.

Un analizador de protocolos se utiliza en auditorías de seguridad, ya que trata de identificar fallos o problemas analizando paquetes de datos que se transmiten en la red. Además, genera informes y estadísticas que permiten obtener una visión global del funcionamiento de la red.

Algunos de los datos que facilitan estas herramientas son:

- Componentes defectuosos de la red.
- Errores de configuración.
- Errores de conexión.
- Problemas de protocolo.
- Tráfico de datos inusual en el servidor de la red.
- Aplicaciones que pueden entrar en conflicto.
- Fluctuaciones del tráfico de datos de la red.
- Monitorización de una o varias redes.

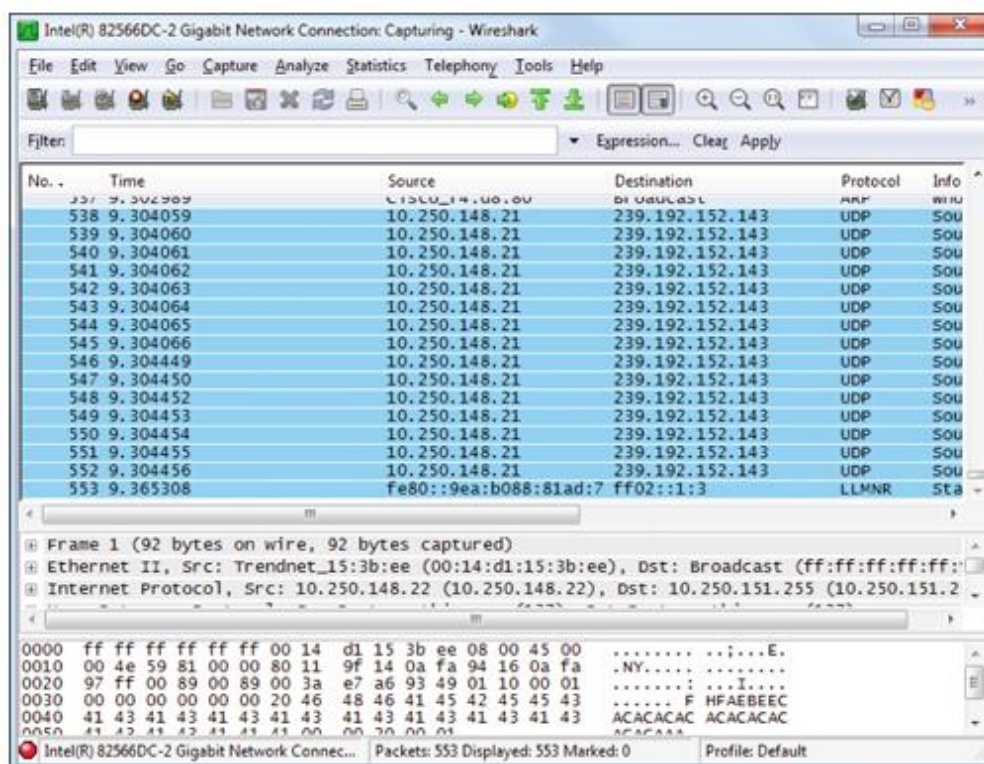


### 5.1.- Analizador de protocolos Wireshark

Uno de los analizadores más populares es el analizador de protocolos Wireshark, que antiguamente se denominaba Ethereal. Se trata de una herramienta que se gestiona a través de una interfaz gráfica.

Permite identificar y analizar el tráfico de red en un momento determinado y entre sus características principales destacan:

- Permite analizar más de 480 protocolos.
- Captura directamente los paquetes de datos desde una interfaz de red.
- Con el análisis del paquete capturado, se obtiene información del protocolo utilizado.
- Permite importar y/o exportar los paquetes de datos capturados a otras aplicaciones.
- Filtra los paquetes de datos atendiendo a unos criterios definidos por el usuario.
- Ofrece estadísticas del tráfico de red.
- Es una herramienta gratuita.
- Se puede utilizar en varios sistemas operativos como Windows, Linux, Unix, etc.
- No está disponible en español.



Analizador de protocolos Wireshark

## 5.2.- Analizador DSniff

DSniff es un conjunto de herramientas que tiene como finalidad introducirse en una red. Muy utilizado también en auditorías de seguridad informática. Puede utilizarse en varios sistemas operativos como Windows, Linux, etc.

Este analizador de protocolos funciona por comandos y está formado por las siguientes herramientas con funciones distintas:

- Dnsijf: sniffer de contraseñas (detecta las contraseñas que circulan por una red).

### Definición

#### Sniffer

Es lo mismo que un analizador de paquetes. Se trata de una aplicación que tiene como función principal la captura de tramas de la información que circula por una red.

- Filesnarf captura y almacena ficheros.
- Msgsnarf registra mensajes enviados/recibidos por mensajería instantánea.
- Tcpcat: cierra una conexión establecida.
- Tcpcat: disminuye la velocidad de las conexiones.
- Webspies: visualiza el tráfico de red de un equipo víctima a tiempo real.

Con estos comandos, se puede observar el peligro que supone una herramienta de este tipo, ya que, aunque permita evaluar la red interna de un sistema de información, también es una herramienta muy atractiva para intrusos que quieren obtener información de redes en las que no están autorizados.

```
root@bt:~# dsniff -m -i eth0
dsniff: listening on eth0
-----
07/13/12 13:45:17 tcp 192.168.232.170.52177 -> 192.168.232.172.23 (telnet)
administrator
12345
ls
dir
md hackingDNA
exit
-----
07/13/12 13:46:15 tcp 192.168.232.128.49673 -> 192.168.232.170.23 (telnet)
msfadmin
msfadmin
exit
-----
07/13/12 14:11:22 tcp 192.168.232.172.1217 -> fto.netfast.org.21 (ftp)
USER b6_7224895
PASS un10ck
-----
07/13/12 14:25:23 tcp 192.168.232.170.41503 -> 192.168.232.172.23 (telnet)
msfadminadministrator
12345
```

Analizador de protocolos DSniff

### 5.3.- Analizador Caín & Abel

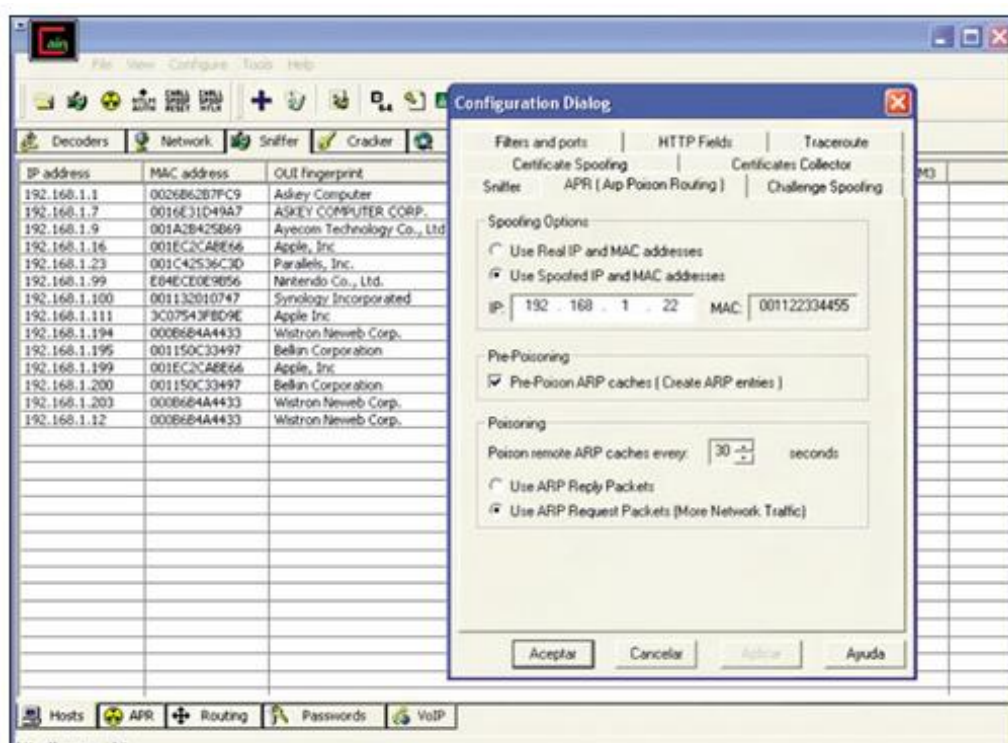
Cain & Abel también es conocido como Caín y es una herramienta que se utiliza fundamentalmente para la recuperación de las contraseñas del sistema operativo Microsoft Windows. Actualmente, no existe versión en español.

Es también un analizador de protocolos o sniffer con el potencial especial de descifrar contraseñas. Algunas de las contraseñas de las que es capaz de descifrar mediante la escucha de paquetes de datos son:

- Contraseñas de inicio de sesión en el sistema operativo.
- Contraseñas comunes.
- Contraseñas del protector de pantalla.
- Contraseñas de clientes de telefonía VoIP.

Además, puede interceptar paquetes de datos con datos de voz (recuperando conversaciones grabadas).





Analizador de protocolos Cain

Caín & Abel fue diseñada para convertirse en una herramienta de auditoría útil cuando los usuarios han olvidado o perdido las contraseñas y desean recuperarlas. No obstante, esta herramienta en manos de intrusos también tiene cierto peligro, ya que pueden conocer las principales contraseñas de los equipos que forman el sistema de información y utilizarlas con fines malintencionados.

#### 5.4.- Otros analizadores de protocolos: IP Sniffer y Tcpdump

Además de los analizadores de protocolos descritos en epígrafes anteriores, es importante mencionar dos más cuyo uso es bastante frecuente y extendido:

- IP Sniffer.
- Tcpdump.

##### IP Sniffer

IP Sniffer es un analizador de protocolos que realiza un examen profundo del tráfico de red que pasa por un sistema de información.

Permite establecer reglas de filtrado, seleccionar el adaptador de red y decodificar paquetes de datos, entre otras opciones.

Esta herramienta, además, elabora estadísticas de los paquetes de entrada y salida seleccionados y permite monitorizar el tráfico de una IP determinada.

### **Tcpdump**

El analizador Tcpdump es muy similar a WireShark y su función principal es el análisis del tráfico de datos que circula por una red determinada.

También funciona en numerosos sistemas operativos y destaca por su capacidad de capturar y mostrar los paquetes que se transmiten y reciben en una red concreta a tiempo real.

## **6. ANALIZADORES DE PÁGINAS WEB TIPO ACUNETIX, DIRB, PAROSPROXY, ETC.**

Como se ha comentado en epígrafes anteriores, los analizadores de vulnerabilidades de páginas web realizan pruebas en sitios web o en aplicaciones web para detectar sus fallos y vulnerabilidades y evitar posibles ataques de seguridad.

En la actualidad, hay numerosos analizadores de páginas web en el mercado y cada uno tiene características distintas y detecta fallos diferentes, por lo que se recomienda utilizar varios de ellos para detectar el mayor número de vulnerabilidades posible.

En este apartado, se van a describir cinco analizadores en concreto:

- Acunetix.
- Dirb.
- Parosproxy.
- Virus Total.
- URLVoid.

### **6.1.- Analizador Acunetix**

Acunetix Web Vulnerability Scanner es una herramienta encargada de escanear y analizar páginas web para detectar fallos y vulnerabilidades de seguridad que puedan poner en peligro su integridad.

El escaneo lo realiza a través de varias pruebas (que puede definir y configurar el usuario) por las que puede detectar fallos como:

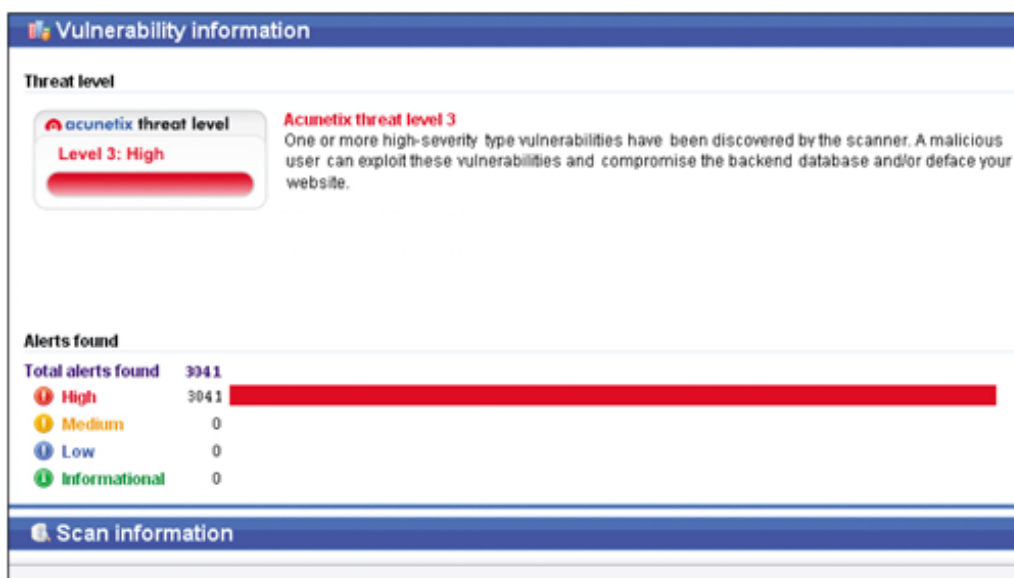
- Ataques de autenticación.
- Ataques de ejecución de código.
- Ataques de inyección SQL.

Tampoco está en español y puede descargarse gratuitamente en su web oficial: <http://www.acunetix.com/vulnerability-scanner/download.htm>.

Su funcionamiento es bastante sencillo, simplemente hay que:

- Escribir el sitio web que se pretende analizar.
- Presionar Next.
- Seleccionar las páginas vinculadas que se quieren también escanear.
- Presionar Finish.

Con estos pasos, Acunetix mostrará una lista con las vulnerabilidades detectadas en el sitio web que deberán ser analizadas y explotadas en el proceso de auditoría.



Acunetix

## 6.2.- Analizador Dirb

Dirb es una herramienta de análisis de vulnerabilidades web que se utiliza para descubrir directorios con información sensible a los que el administrador ha dejado de prestarles atención. Más que un escáner de vulnerabilidades, es un escáner de contenidos.

También se utiliza para obtener una imagen global de la estructura de un servidor web.

La detección de estos directorios se realiza mediante ataques fuzzing (envíos automáticos de datos al sitio web que se desea analizar). Una vez realizado el envío, el fuzzing remite unos resultados que deberán ser analizados para comprobar si el sitio web sigue un comportamiento normal o si, por el contrario, el ataque ha tenido éxito y la web ha quedado inestable.

En caso de obtener resultados de inestabilidad de la página web, deberán tomarse medidas para elevar su nivel de seguridad y eliminar las vulnerabilidades detectadas.

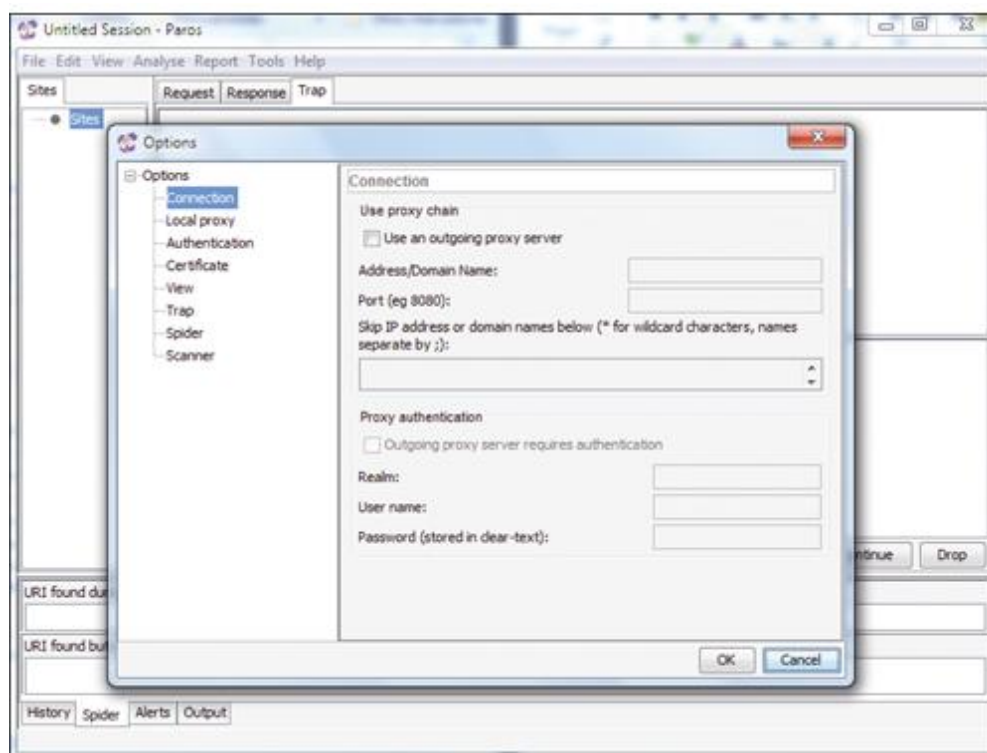
El analizador Dirb puede descargarse gratuitamente a través de su web oficial: [http:// dirb.sourceforge.net](http://dirb.sourceforge.net) y funciona con una consola de comandos.

### 6.3.- Analizador Parosproxy

Parosproxy (o el proxy Paros) es una aplicación de Java gratuita que intercepta los datos HTTP y HTTPS que se han transferido entre un equipo servidor y otro cliente.

Además, también incorpora otras funciones que permiten realizar comprobaciones de seguridad como:

- Spider: navega por una URL definida por el usuario y ofrece la estructura de su árbol web (su conjunto de directorios).
- Sean: analiza la URL especificada para buscar problemas de seguridad en aspectos como:
  - Problemas de seguridad en el navegador del equipo cliente.
  - Recopilación de información de archivos obsoletos.
  - Problemas de seguridad en el servidor.
  - Inyecciones de códigos (SQL, etc.).



Analizador de protocolos Cain

Se trata de una herramienta gratuita para varios sistemas operativos que puede descargarse en: <http://www.parosproxy.org/index.shtml>.

### 6.4.- Otros analizadores de páginas web: Virus Total y URLVoid

Actualmente, existe una gran variedad de herramientas que permiten detectar amenazas y virus en las páginas web, muchas de ellas on-line.

Además de las ya mencionadas anteriormente, merece la pena destacar dos de ellas muy utilizadas:

- Virus Total.
- URLVoid.

### Virus Total

Virus Total es una de los analizadores de páginas web más utilizados en la actualidad por el elevado grado de información que facilita sobre las URL introducidas.

Es conocido sobre todo porque permite al usuario el envío de archivos para un análisis posterior, además de la funcionalidad clásica de analizar URL de los enlaces introducidos.

Además, utiliza una gran variedad de analizadores para verificar la seguridad de la web introducida y reporta un informe detallado por cada uno de ellos.

Se puede acceder a esta herramienta a través de su página web: <<http://www.virustotal.com>>.



Virus Total

### URLVoid

URLVoid es una herramienta de análisis de páginas web muy similar a las ya mencionadas, pero destaca por su gran facilidad de utilización.

Es de utilización gratuita y permite el escaneo de URL con múltiples analizadores web de calidad y con una cierta reputación, con la finalidad de detectar sitios web potencialmente peligrosos.

## **7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA TIPO BRUTUS, JOHN THE RIPPER, ETC.**

Otras herramientas utilizadas frecuentemente en las auditorías de seguridad informática son aquellas relacionadas con el descubrimiento de contraseñas. Si la aplicación es capaz de descubrir una contraseña con facilidad, hay más riesgo de sufrir ataques y, por tanto, será necesaria una nueva contraseña con más complejidad.

Las técnicas de descubrimiento de contraseñas se clasifican en:

- Ataques de fuerza bruta: aquellos que pretenden recuperar una contraseña probando todas las combinaciones posibles hasta dar con la correcta. Al ser muy numerosas las posibles combinaciones, este tipo de ataques son muy costosos y conllevan bastante tiempo hasta que se descubre la contraseña correcta. Debido a estos costes elevados, se suelen combinar con ataques de diccionario.
- Ataques de diccionario: estos, por el contrario, no encuentran la contraseña probando todas las combinaciones posibles, sino que intentan averiguarla probando todas las palabras del diccionario.

### **Nota**

Los ataques de diccionario suelen ser más eficientes que los de fuerza bruta, ya que los usuarios muy frecuentemente utilizan como contraseña palabras existentes y fáciles de recordar (que, por regla general, están contenidas en los diccionarios).

Cuando se utilizan contraseñas complejas (por ejemplo: compuestas por mayúsculas, minúsculas, signos de puntuación y números), los ataques de diccionario son poco efectivos, ya que difícilmente una contraseña con todos estos elementos estará contenida en algún diccionario. En estos casos, se recomienda ejecutar ataques de fuerza bruta aunque conlleven mayores costes.

En los siguientes epígrafes, se analizan varias herramientas muy potentes de descifrado de contraseñas:

- John the Ripper.
- Brutus.
- Bruter.
- OphCrack.

### 7.1.- John the Ripper

John the Ripper es una aplicación que utiliza el método de fuerza bruta para adivinar las contraseñas.

Es una herramienta muy popular en la actualidad y se utiliza frecuentemente en auditorías de seguridad informática para comprobar el nivel de seguridad de las contraseñas de un sistema de información.

Para detectar contraseñas más simples, también tiene la opción de utilizar ataques de diccionario.

Sus características principales son:

- Puede ejecutarse en numerosos modelos de procesador.
- Funciona en muchas arquitecturas de los sistemas de información.
- Soporta varios sistemas operativos (Windows, Linux, MS-DOS, etc.).
- Es una aplicación libre y de distribución gratuita.
- Ofrece la opción de detener el proceso de búsqueda de contraseña y proseguirlo posteriormente.
- Ofrece la opción de definir las letras o rango de letras que se quieren utilizar para construir las posibles palabras.
- También permite que el usuario decida la longitud que deben tener las contraseñas a probar.

```
[root@practiceLinux run]# ./john
John the Ripper password cracker, version 1.7.6
Copyright (c) 1996-2018 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single                "single crack" mode
--wordlist=FILE --stdin  wordlist mode, read words from FILE or stdin
--rules                 enable word mangling rules for wordlist mode
--incremental[=MODE]    "incremental" mode [using section MODE]
--external=MODE         external mode or word filter
--stdout[=LENGTH]       just output candidate passwords [cut at LENGTH]
--restore[=NAME]        restore an interrupted session [called NAME]
--session=NAME          give a new session the NAME
--status[=NAME]         print status of a session [called NAME]
--make-charset=FILE     make a charset, FILE will be overwritten
--show                 show cracked passwords
--test[=TIME]           run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..] [do not] load this (these) user(s) only
--groups=[-]GID[,...]   load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT      load salts with[out] at least COUNT passwords only
--format=NAME           force hash type NAME: DES/BSDB1/MD5/BF/AFS/LM/crypt
--save-memory=LEVEL     enable memory saving, at LEVEL 1..3
[root@practiceLinux run]# _
```

Parámetros de John the Ripper

Su tarea inicial es intentar descubrir la contraseña con ataques simples de diccionario. Si no la descubre, John the Ripper también puede intentar descifrarla con modificaciones del diccionario



como, por ejemplo, cambiando mayúsculas y minúsculas, añadiendo números, añadiendo símbolos, cambiando letras, etc.

Si aun así no se descubriese la contraseña, la aplicación ya utilizaría el método de ataque de fuerza bruta. Por su coste y elevado tiempo de ejecución, solo se recomienda el ataque de fuerza bruta en casos muy concretos y contraseñas de gran complejidad.

## **7.2.- Brutus**

Brutus es otra herramienta utilizada para descubrir contraseñas, esta vez a través de una interfaz gráfica.

Se caracteriza por su rapidez y sencillez de utilización y destaca además por la gran variedad de tipos de autenticación en los que puede ser utilizada.

### **Definición**

#### **Tipos de autenticación**

Los distintos métodos por los que un usuario se puede identificar y acceder a una aplicación o a algún recurso del sistema de información.

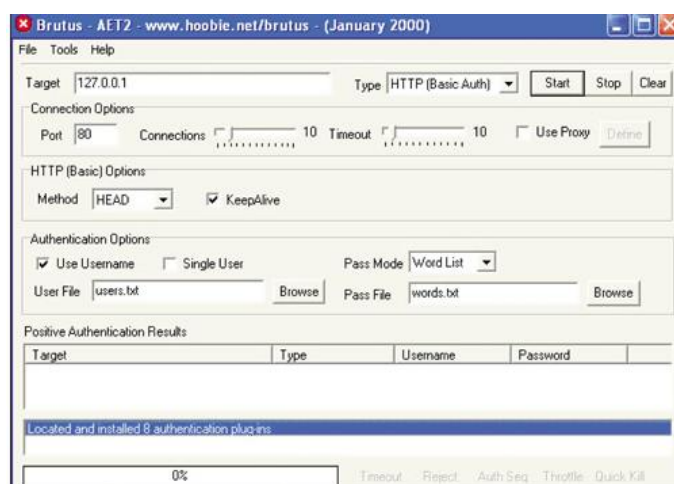
Algunos ejemplos son HTTP, POP3, SMB, TELNET, IMAP, etc.

En su funcionamiento utiliza ataques de fuerza bruta, aunque también da la opción de ejecutar ataques de diccionarios (almacenados en un documento con extensión ".doc") que pueden ser creados directamente por el usuario.

A pesar de ser una de las herramientas más rápidas de su ámbito, Brutus solo está disponible para Microsoft Windows en inglés y es de distribución gratuita.

Puede descargarse a través de su página oficial: <<http://www.hoobie.net/brutus>>.





Brutus

### 7.3.- Otras herramientas de ataques de fuerza bruta y diccionario

Además de Brutus y John the Ripper, hay una gran variedad de herramientas que realizan tanto ataques de fuerza bruta como ataques de diccionario. Conviene describir brevemente dos de ellas:

- OphCrack: permite descifrar contraseñas en el sistema operativo Windows. Su utilización es bastante sencilla y dispone de una interfaz gráfica que añade simplicidad a su uso. Para la obtención de las contraseñas, utiliza ataques de diccionario.
- Bruter: este, sin embargo, utiliza ataques de fuerza bruta para descifrar las contraseñas en el sistema operativo Microsoft Windows (actualmente no funciona en otros sistemas operativos, aunque no se descarta en futuras actualizaciones). Soporta una gran variedad de servicios, entre los que destacan los siguientes:
  - FTP.
  - HTTP.
  - MySQL.
  - POP3.
  - SMTP.

## 8. RESUMEN

En la auditoría de sistemas, frecuentemente (por no decir siempre) se utilizan herramientas que ayuden en la detección de fallos y vulnerabilidades que permitan estimar el riesgo del sistema de información y formular medidas correctivas y controles.

Por una parte, dentro del mismo sistema operativo de los equipos se encuentran varias herramientas de auditoría, como ping, traceroute, que permiten detectar fallos y anomalías en su red.

Además, se recomienda que el auditor disponga de herramientas que analicen la red, los puertos y los servicios configurados en esta para detectar posibles vías de entrada de intrusos y tráfico de red inusual que ofrezca indicios de amenaza. Ejemplos de estas herramientas son Netcat, Nmap y NBTScan. También sirven para evaluar la seguridad de una red los analizadores de protocolos, que analizan paquetes de datos que se transmiten en la red para detectar errores de configuración, de conexión, etc.

Otra herramienta fundamental y de gran utilidad para el auditor es Nessus, un analizador de vulnerabilidades capaz de identificarlas, emitir informes con los resultados obtenidos y formular propuestas de solución.

Por otra parte y a nivel externo, existen los analizadores de páginas web, cuya función principal es conocer la estructura de los sitios web y detectar sus vulnerabilidades para evitar que sufran ataques de seguridad.

Estas herramientas, junto con las herramientas de ataques de diccionario y fuerza bruta, sirven para que el auditor detecte vías de ataque e intrusiones, que deberán ser solucionadas para disminuir el riesgo del sistema de información y de la organización en general.

## CAPÍTULO 5 DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

### 1. INTRODUCCIÓN

Uno de los aspectos fundamentales de las auditorías de los sistemas de información es la evaluación de su nivel de seguridad.

Este grado de seguridad no solo debe ser a nivel de las vulnerabilidades de las aplicaciones instaladas en los equipos, sino que debe contener una serie de medidas que intenten bloquear la entrada de ataques que puedan afectar a la información.

Tanto si los ataques afectan levemente a la información como si tienen efectos devastadores sobre el sistema, debe implantarse un sistema de protección que detecte los posibles atacantes y que evite y prevenga su entrada.

Una de las medidas más eficientes y utilizadas es la implantación de cortafuegos de red. En este capítulo, se describen los distintos tipos de cortafuegos junto con sus componentes, utilidades y arquitecturas principales.

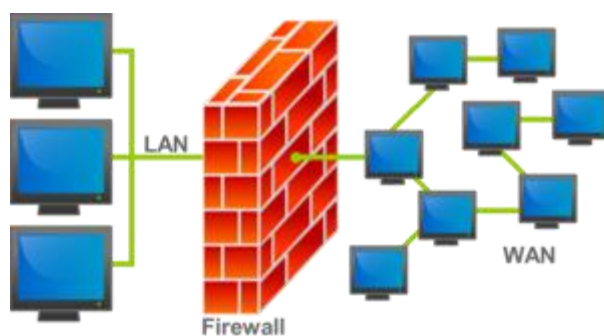
### 2. PRINCIPIOS GENERALES DE CORTAFUEGOS

La evolución de los sistemas de información permite un aumento de su conectividad, pasando de ser utilizados en redes locales a poder transmitir cualquier tipo de información a través de Internet.

Este hecho ha provocado que crezcan también las amenazas que pueden afectar a los sistemas vulnerando los mecanismos de seguridad y afectando gravemente a los datos que contienen.

Además, cuando se trata de estaciones de trabajo y servidores, no hay medidas de seguridad sólidas que mantengan un nivel de seguridad adecuado. Por este motivo, se diseñaron los cortafuegos o .firewalls.

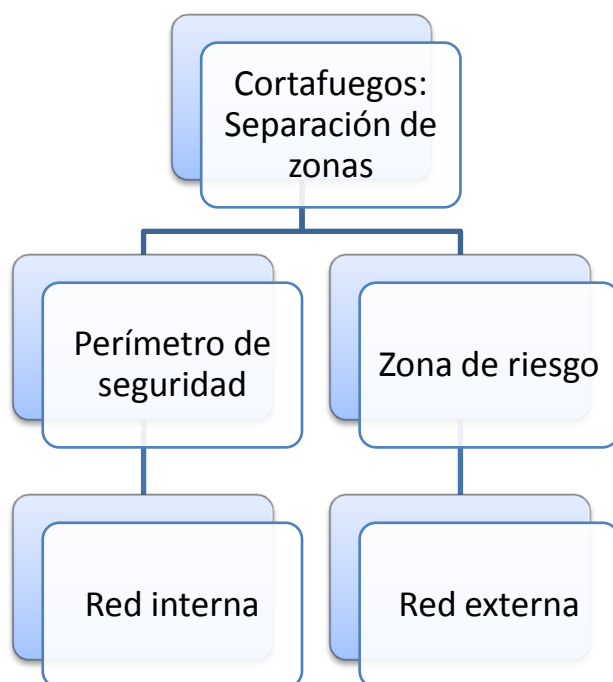
Un cortafuegos o firewall es un sistema compuesto por uno o varios dispositivos cuya función principal es la separación entre la red local de un sistema de información y la red exterior para impedir la entrada de ataques y aumentar el nivel de seguridad de la organización.



En otras palabras, es un sistema cuya funcionalidad principal es efectuar un control de accesos entre dos redes: la red interna y la red externa o Internet.

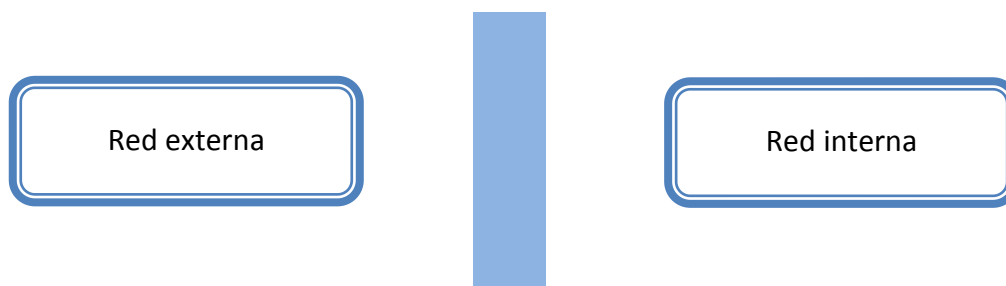
El cortafuegos utiliza los conceptos de perímetro de seguridad y zona de riesgo para determinar las redes interna y externa de un sistema de información:

- **Perímetro de seguridad:** espacio protegido por el cortafuegos, suele ser propiedad de la organización y se corresponde con su red interna.
- **Zona de riesgo:** es la red frente a la que se protege el perímetro de seguridad con el cortafuegos.



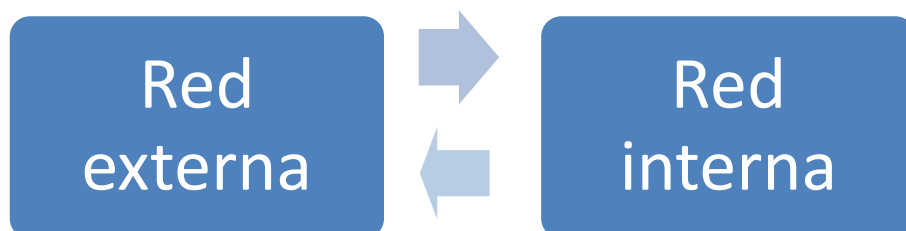
Los cortafuegos son la medida más efectiva de seguridad si se pretende tener conectado el sistema de información de la organización.

Está claro que la protección completa y más efectiva sería el aislamiento total de la red interna de la red externa con la no conexión de los dispositivos a Internet.



Este formato de protección es muy eficaz, ya que impide que entre cualquier intruso no autorizado a la red interna, pero conlleva pérdidas de conectividad importantes debidas al aislamiento total.

Otra opción es mantener el sistema de información de la organización conectado con la red externa sin protección.



Esta configuración ya evita el problema de la falta de conectividad, pero deja al sistema completamente vulnerable ante posibles incidentes de seguridad e intrusiones.

La mejor alternativa, después de ver las ventajas e inconvenientes de los formatos anteriores, es la utilización de un cortafuegos. Con esta configuración se mantiene la conectividad del sistema con el exterior, pero se resuelven problemas de seguridad con la implantación del cortafuegos, que impide accesos no autorizados.



La protección que ofrece un cortafuegos se define en tres objetivos básicos:

- Establecer un enlace controlado entre la red interna y la red externa de un sistema de información.
- Proteger a la red interna de posibles ataques e intrusiones procedentes de la red externa (Internet).
- Establecer un punto único de defensa con una ubicación estratégica (aumentando lo máximo posible tanto la conectividad como la seguridad del sistema) .

### 2.1.- Características de diseño de un cortafuegos

Para maximizar la fiabilidad y eficiencia de un cortafuegos, es fundamental que su diseño e implantación se tomen de un modo razonado, debiéndose estudiar todos los aspectos de la organización que puedan ser influyentes.

El diseño de la estructura de un cortafuegos debe realizarse teniendo en cuenta tres objetivos fundamentales:

- Todo el tráfico de datos desde la red interna hacia el exterior debe pasar por el cortafuegos.
- Solo se permitirá pasar a la red local el tráfico autorizado específicamente por la política de seguridad de la organización.
- El cortafuegos debe ser inmune a posibles penetraciones de intrusos, mediante la utilización de sistemas confiables acordes y de sistemas operativos seguros.

Además de los objetivos a considerar en el diseño del cortafuegos, deben tenerse en cuenta los siguientes servicios de control de accesos que deben poder cubrirse:

- Control de servicios: establece a qué tipo de servicios de la organización se puede acceder desde las redes internas y externas.
- Control de dirección: establece las direcciones de entrada y salida en las que se permitirá el tráfico de datos desde/hacia la red externa.
- Control de usuarios: establece controles de acceso para determinar a qué servicios puede acceder cada usuario.
- Control de comportamiento: establece el uso concreto de ciertos servicios particulares.

#### Técnicas para el control de accesos del cortafuegos

- Control de servicios
- Control de dirección
- Control de usuarios
- Control de compartimiento

#### Importante

Los cortafuegos no protegen de los ataques originados desde dentro la red interna, por lo que es necesario implantar medidas de seguridad adicionales que impidan la expansión de intrusiones internas.

### **Características de configuración de un cortafuegos**

Cuando se va a implantar y configurar un cortafuegos en un sistema de información, hay que tomar tres decisiones fundamentales: políticas de seguridad, monitorización y economía.

#### **Política de seguridad**

La primera decisión trata sobre la política de seguridad del cortafuegos y del nivel de protección que se pretende implantar. Cada organización debe establecer la protección del cortafuegos, atendiendo a la utilización de la red y a las características de los usuarios. No es lo mismo que la empresa desee bloquear todo el tráfico de una red que pretenda bloquear solo sitios web potencialmente peligrosos.

#### **Monitorización**

La segunda decisión hace referencia al grado de monitorización y control que pretende establecer la organización. En el momento de definir la política de seguridad a establecer, la empresa tendrá que definir el grado de seguridad del cortafuegos, decidiendo qué tipo de información se va a permitir y cuál se va a denegar. Se distinguen dos posturas opuestas para decidir la monitorización del firewall:

- Política restrictiva: en la que se deniega todo lo que no se permite.
- Política permisiva: en la que se permite todo lo que no se deniega.

Una política restrictiva siempre es más aconsejable en materia de seguridad, pero con su aplicación es posible que las limitaciones de acceso a ciertos sitios sean excesivas e impidan el desarrollo de las tareas habituales de la organización.

#### **Economía**

El último punto a tener en cuenta para tomar la decisión de qué cortafuegos implantar en la organización es puramente económico. Según la valoración de los activos y de la información objetivo que se desee proteger, los costes a asumir por la implantación serán menores o superiores.

Es evidente que, cuanto mayor sea el valor de los activos a proteger, mayor será el gasto que deberá soportar la organización para la implantación del cortafuegos y mayor calidad deberá tener el sistema a implantar.

Sin embargo, si el valor de los activos que se pretenden proteger es limitado, no merecerá la pena realizar una alta inversión: es posible que la inversión supere los costes que podría ocasionar algún tipo de ataque.

**Nota**

Para tomar decisiones económicas relativas al diseño del firewall, no solo se deben considerar los gastos de implantación, sino que también deben tenerse en cuenta los gastos de mantenimiento, que deberán ser cubiertos a lo largo de su vida útil.

**3. COMPONENTES DE UN CORTAFUEGOS DE RED**

Cuando ya se han decidido las características principales del cortafuegos a implantar, el siguiente paso es decidir qué mecanismos se van a incorporar a dicho cortafuegos para cumplir con las políticas de seguridad definidas por la organización.

Todos los cortafuegos están compuestos por tres componentes sobre los que se deberán implantar los mecanismos de protección:

- Filtrado de paquetes.
- Proxy de aplicación.
- Monitorización de la actividad.

**Componentes de los cortafuegos de red**

- Filtrado de paquetes
- Proxy de aplicación
- Monitorización de la actividad

**3.1.- Filtrado de paquetes**

Generalmente, los cortafuegos utilizan reglas de filtrado de paquetes con el objetivo de disminuir la carga de la red. El filtrado de paquetes se utiliza para cumplir con los objetivos de seguridad de una red establecidos por la organización, evitando los accesos no autorizados, pero permitiendo en todo momento los accesos autorizados.

El funcionamiento del componente de filtrado de paquetes es bastante sencillo:

- En un primer momento se analiza la cabecera de cada paquete de datos que pretende entrar en la red local de la organización.
- Según las reglas preestablecidas por la organización y atendiendo al análisis del paquete, se le permitirá el acceso o será bloqueada. Los aspectos más habituales por analizar son:
  - Protocolo utilizado.
  - Dirección de origen y dirección de destino.
  - Puerto de destino.



Las reglas de permisión y bloqueo de acceso a paquetes de acceso se establecen en una tabla de condiciones y acciones relacionadas que se van consultando ordenadamente hasta detectar una condición que indique el bloqueo o el reenvío del paquete.

La tabla siguiente es un ejemplo de reglas de filtrado por la IP de origen y/o destino de la trama de datos.

Origen	Destino	Tipo	Puerto	Acción
158.34.0.0	-	-	-	Denegar
-	195.45.15.0	-	-	Permitir
158.35.0.0	-	-	-	Denegar
-	193.23.32.9	-	-	Denegar

Según las reglas establecidas en la tabla de condiciones, si llega un paquete procedente de la IP 158.34.0.0 será denegado, independientemente de la IP de destino.

Lo mismo sucedería con los paquetes de red procedentes de la IP 158.35.0.0.

En cuanto a las IP de destino, cualquier paquete de datos que pretenda acceder a la IP 193.23.32.9 será bloqueado. Sin embargo, se permitirán los datos que quieran acceder a la IP 195.45.15.0, siempre que no provengan de la IP definida en la regla anterior (158.34.0.0).

### Importante

La correcta definición de las reglas de filtrado de tramas es fundamental. Si se definen reglas incorrectamente, se puede incurrir en graves fallos de seguridad por permitir accesos potencialmente peligrosos.

Origen	Destino	Tipo	Puerto	Acción
198.34.0.0	-	-	-	Denegar
-	135.23.40.0	-	-	Denegar
198.35.0.0	-	-	-	Denegar
-	135.23.53.0	-	-	Permitir

### 3.2.- Proxy de aplicación

Aparte de las reglas de filtrado de paquetes de datos, los cortafuegos suelen incorporar paquetes de aplicaciones software que reenvíen o bloqueen conexiones a unos servicios concretos.

Estas aplicaciones software se denominan servicios proxy y las máquinas en las que son ejecutadas son las pasarelas de aplicación.

Los servicios proxy permiten aumentar el nivel de seguridad de la red, aunque es importante mencionar tanto sus ventajas como sus inconvenientes.

Sus principales ventajas son:

- Permisi3n exclusiva de ser vicios con proxy: los servicios proxy solo permiten usar aquellos servicios para los que existe un proxy. Si la pasarela de aplicaci3n solo tiene proxies para protocolos HTTP y FTP, el servicio proxy solo permitir3 el uso de los servicios con estos protocolos, denegando el resto de servicios.
- Filtrado de protocolos: los servicios proxy ofrecen opciones de filtrado de datos yendo m3s all3 del filtrado por las caracter3sticas de la cabecera del paquete (como es el caso del componente filtrado de paquetes).
- Simplificaci3n de reglas de filtrado: los servicios proxy facilitan la tarea de establecer y definir las reglas de filtrado por su mayor simplicidad ante el componente de filtrado de paquetes. Simplemente hay que permitir el tr3fico de datos hacia la pasarela y bloquear el resto de datos.

Sin embargo, tambi3n deben remarcarse sus desventajas:

- Cada servicio requiere un servicio proxy propio.
- Es m3s costoso que los filtros de paquetes simples.
- Tambi3n tienen menor rendimiento que los filtros de paquetes.

Los servicios proxy pueden convertirse en un cuello de botella de redes, ya que deben pasar por ellos todas las solicitudes y paquetes de datos.

Proxy de aplicaci3n	
Ventajas	Desventajas
Permis3n exclusiva de servicios con proxy.	Necesidad de proxy propio para cada servicio.
Filtrado de protocolos.	Mayor coste.
Simplificaci3n de reglas de filtrado.	Menor rendimiento.
	Cuellos de botella.

**Nota**

Un cuello de botella se produce cuando la capacidad de procesamiento de un dispositivo determinando es superior que la capacidad del bus por el que está conectado, produciendo bajadas de rendimiento y saturación del servicio.

**3.3.- Monitorización de la actividad**

La monitorización de la actividad del cortafuegos es imprescindible para la seguridad de los elementos que protege, ya que permite obtener información sobre:

- Todos los ataques que se han producido (o se están produciendo).
- La presencia de paquetes de datos sospechosos (independientemente de si finalmente son ataques reales o no).

¿Qué información debe registrar y almacenar el cortafuegos? Se recomienda la recopilación de información referente a: Información general en la que se incluyan estadísticas de los tipos de paquetes de datos recibidos, las direcciones de origen y destino más frecuentes, etc.

- Información adicional de las conexiones al sistema, como el origen y destino de la conexión, el nombre del usuario, etc.
- Intentos denegados de utilización de protocolos.
- Intentos de acceso de paquetes de datos externos con direcciones de equipos internos (a través de falsificación de direcciones).
- Paquetes de datos cuyo origen es desconocido y/o sospechoso.

Este tipo de información es de gran utilidad para el administrador del sistema y para el responsable de seguridad, ya que permiten un análisis exhaustivo de los comportamientos sospechosos y la implantación de medidas preventivas que impidan ataques que deriven de dichos comportamientos.

**Nota**

Para los casos en los que la cantidad de registros de la monitorización del cortafuegos sea muy elevada, existen herramientas en el mercado que permiten el filtrado de los registros según criterios predefinidos.

**4. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD**

Se destacan tres tipos de cortafuegos atendiendo a su ubicación y funcionalidad:

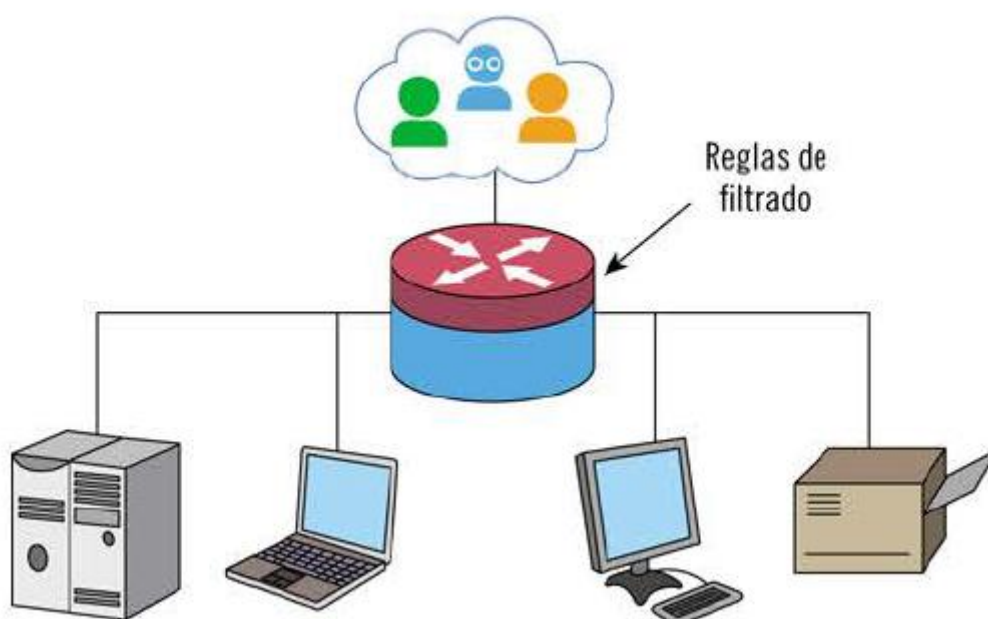
### Tipos de cortafuegos de red

- Router con filtrado de paquetes
- Gateway a nivel de aplicación
- Gateway a nivel de circuitos

#### 4.1.- Routers con filtrado de paquetes

Los routers con filtrado de paquetes son un tipo de cortafuegos que filtran los paquetes IP entrantes, atendiendo a una serie de reglas predefinidas: según la definición de estas reglas, estos routers descartan el paquete o lo reenvían.

#### Estructura con filtrado de paquetes



Como se ha mencionado en el componente de filtrado de paquetes, el filtro se configura a través de una serie de reglas basadas en los encabezados de los paquetes de datos.

Las principales ventajas e inconvenientes se describen en la siguiente tabla.

<b>Routers de filtrado de paquetes</b>	
<b>Ventajas</b>	<b>Desventajas</b>
Simplicidad.	Dificultad para la correcta definición de las reglas de acceso a los paquetes de información.
No son visibles para los usuarios.	No requieren autenticación de los usuarios.
Destacan por su elevada velocidad.	

Este tipo de cortafuegos son especialmente susceptibles a unos ataques determinados:

- Suplantación de direcciones IP por direcciones internas: se aconseja borrar los paquetes de datos que contengan direcciones internas que provienen del exterior.
- Ataques de encaminamiento de fuente: al bloquear ciertas direcciones IP, los *routers* de filtrado no pueden impedir los ataques de encaminamiento de fuente. Para solucionar este problema, se aconseja eliminar los paquetes de datos que utilizan esta opción.
- Fragmentos de reducido tamaño: este tipo de cortafuegos falla bastante con paquetes de datos con encabezados TCP por su fragmentación.

Nota

#### **Nota**

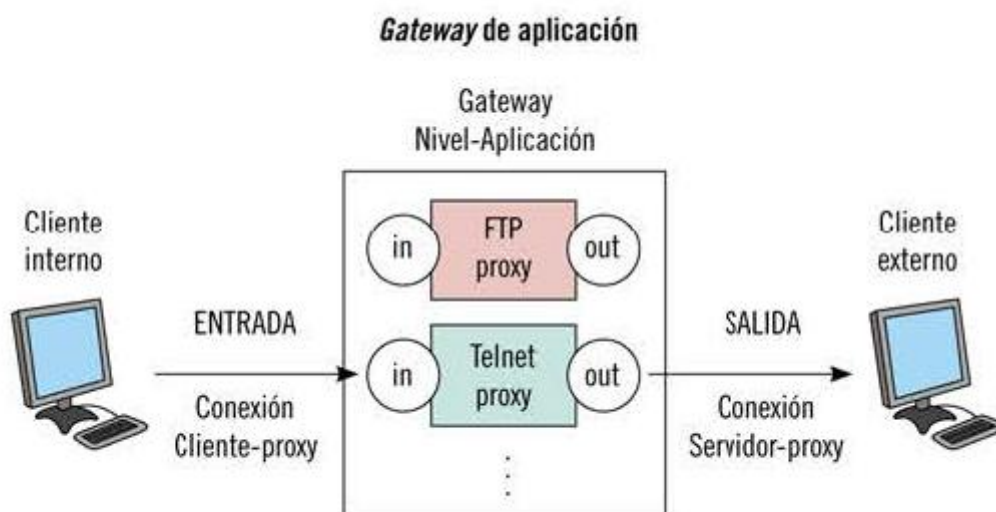
El ataque de encaminamiento de fuente es el envío de paquetes de datos que analizan todos los posibles destinos y deciden cuál es la mejor ruta. Al filtrar solo ciertas direcciones IP, los routers de filtrado no pueden controlar la entrada de este tipo de ataques.

#### **4.2.- Gateways a nivel de aplicación**

Los gateways a nivel de aplicación se asocian al componente de servidores proxy de los cortafuegos.

Son repetidores de tráfico a nivel de aplicación: cuando un usuario solicita un servicio, lo realiza a través del proxy. Una vez recibida la petición, el proxy realiza el pedido al servidor real y devuelve la información solicitada al usuario.

Su finalidad principal es el análisis de los paquetes de datos para detectar contenidos que puedan violar la seguridad de la red.



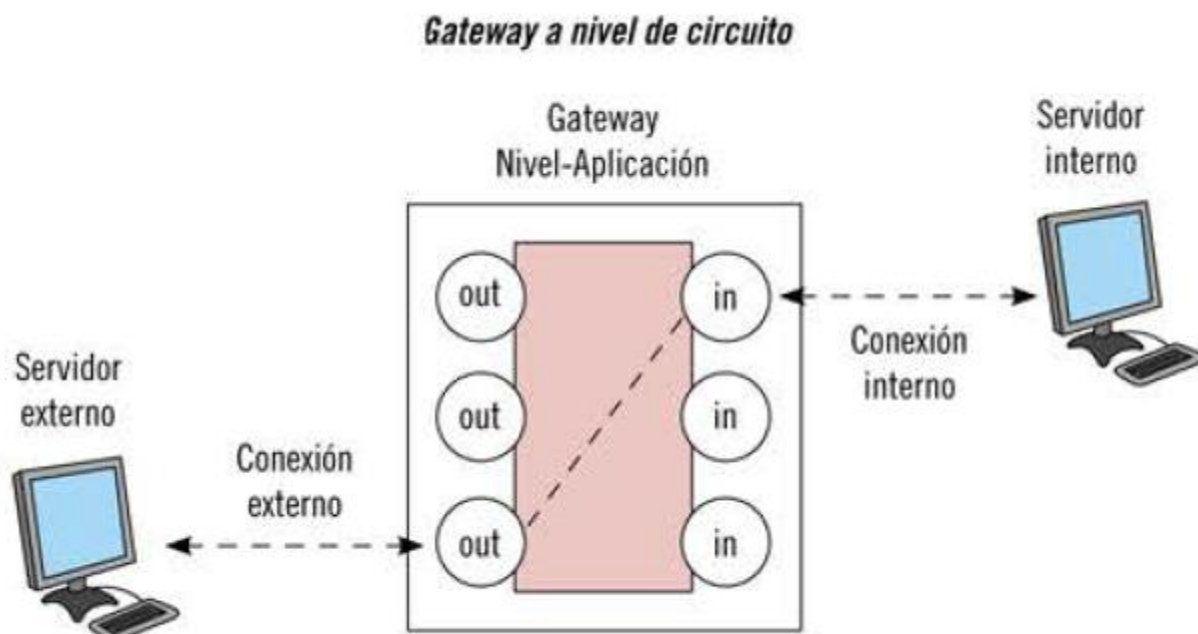
Las principales ventajas y desventajas se describen en la tabla siguiente.

<i>Gateway (pasarela) a nivel de aplicación</i>	
Ventajas	Desventajas
Ofrece mayor seguridad que los routers de filtrado de paquetes.	Puede provocar cuellos de botella por sobrecarga de procesamiento en cada conexión.
Revisa solo las aplicaciones permitidas, aumentando su eficacia.	
Revisa todo el tráfico de red entrante.	
Evita el tráfico directo entre redes.	

### 4.3.- Gateways a nivel de circuito

Los gateways o pasarelas a nivel de circuito son sistemas que redirigen los paquetes de datos cuando se ha comprobado que se ha establecido la conexión.

Para establecer la conexión, estos gateways validan el inicio de la comunicación para verificar si se realiza correctamente según el protocolo de transportes. Cuando ya se ha validado la comunicación, todos los paquetes que se reenvían a continuación no son verificados (solo se revisan las cabeceras de los paquetes). En términos generales, los gateways a nivel de circuito establecen funciones que determinan qué conexiones serán permitidas para la transmisión de datos.



Este tipo de .firewall ofrece la posibilidad de determinar una política restrictiva que permita cerrar y abrir puertos solo cuando sea estrictamente necesario .

#### 4.4.- Host bastion

Host bastion es un punto crítico del sistema en la seguridad de la red identificado por el administrador del cortafuegos. No es un tipo de cortafuegos en sí, pero es interesante mencionarlo porque sirve como plataformas para:

- Gateways a nivel de aplicación.
- Gateways a nivel de circuito.

Se trata de una aplicación ubicada en un punto crítico de un servidor para proteger a la red interna de la organización. Este punto crítico ha sido configurado previamente para que atraiga los posibles ataques que intenten acceder al sistema.

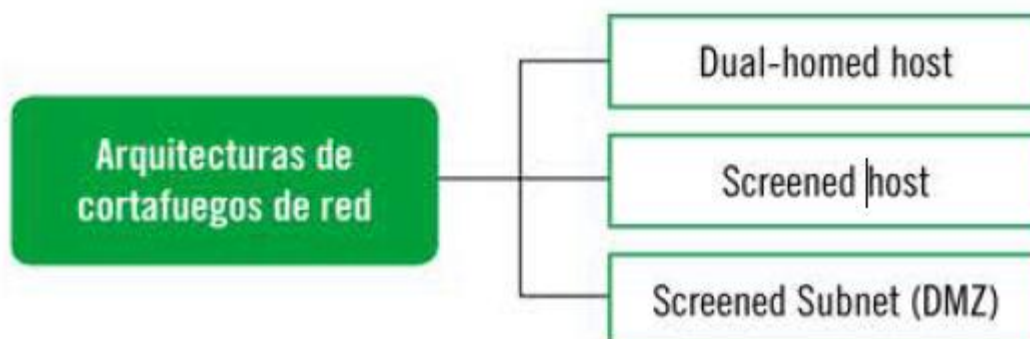


## 5. ARQUITECTURAS DE CORTAFUEGOS DE RED

Además de la utilización de los cortafuegos simples como los *routers* con filtrado de datos o los sistemas de pasarela única, hay varias posibilidades de firewalls más complejos que permiten el aumento de la seguridad del perímetro de seguridad.

Las arquitecturas complejas más comunes son las siguientes:

- *Dual-homed host*.
- *Screened host*.
- *Screened Subnet (DMZ)*.





Estas tres arquitecturas, además de utilizar un sistema como el *router* de filtrado o el *gateway*, combinan estos elementos con bastiones para un bloqueo de datos potencialmente peligroso más eficaz que permita una mayor protección del sistema de información.

### 5.1.- Arquitecturas de cortafuegos dual-homed host

Las arquitecturas de cortafuegos dual-homed host ofrecen una mayor protección que los cortafuegos simples y están compuestas por dos placas de red:

- Una de las tarjetas suele conectarse a la red interna.
- La otra tarjeta se conecta a la red externa de la organización.

Con esta arquitectura se evita que, si el router con filtrado de tramas se ve comprometido, se permita el acceso del tráfico de red a la red interna, ya que toda la información entre Internet y la red interna debe pasar previamente por el host bastion.

Estos sistemas deben ejecutar por lo menos un servidor proxy para cada servicio que se desee pasar por el firewall.

#### Recuerde

Los servidores proxy filtran el tráfico de red, permitiéndose el acceso a una serie de servicios predefinidos.

En la siguiente imagen, se puede observar una configuración clásica de las arquitecturas dual-homed host.

Como se puede observar, *el firewall* actúa como intermediario entre las redes interna y externa: los sistemas conectados en cada bando del *host bastion* se comunican a través de este, sin haber posibilidad de comunicarse directamente.

Los servicios del *host bastion* pueden realizarse de dos formas distintas:

Los usuarios en la red interna con cuentas en el *host bastion* permiten que estos puedan iniciar sesión y utilizar los servicios de la red externa.

Esta alternativa es bastante vulnerable, ya que depende de la contraseña establecida por el usuario: si la contraseña es fácil de descubrir, hay más peligro de intrusión.

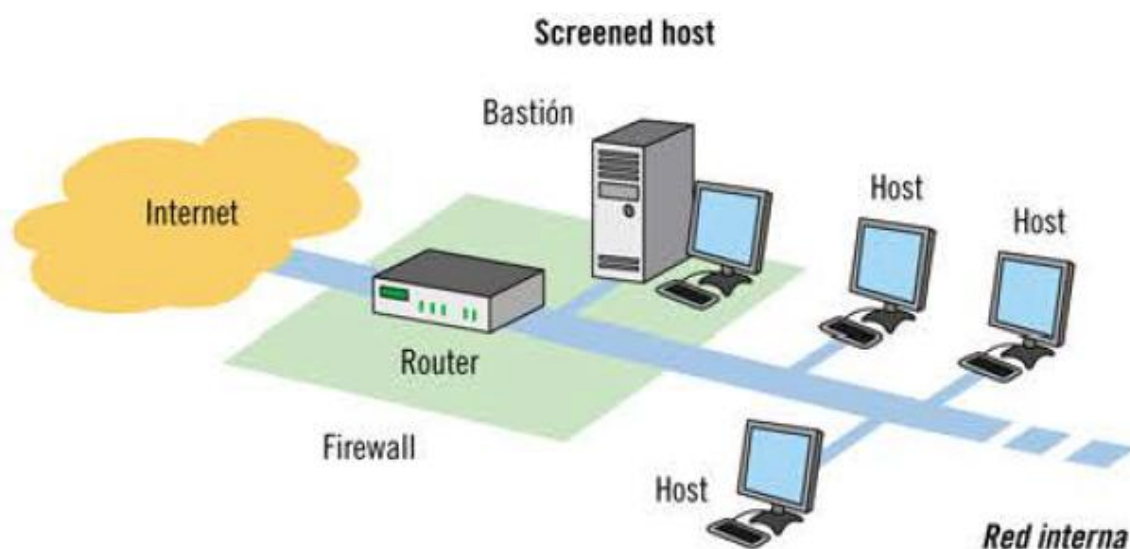
Mediante la ejecución de servicios *proxy* para cada uno de los servicios que se quieran permitir. Aquí se aumenta la seguridad de la red interna, ya que es completamente independiente de la actividad de los usuarios en el establecimiento de contraseñas.

## 5.2.- Arquitecturas de cortafuegos con screened host (single-homed host)

Los cortafuegos single-homed host están formados por dos sistemas de protección que filtran conexiones a nivel de circuito y a nivel de aplicación:

- Un router con filtrado de paquetes.
- Un host bastion.

En estas arquitecturas, el router se configura específicamente para que todos los paquetes de datos que provienen de la red externa deban pasar obligatoriamente por el host bastion, lo que obliga a la organización al establecimiento de elevados sistemas de protección a dicho bastión.



El host bastion, ubicado entre la red interna y el router, es el único que puede establecer conexiones entre la red interna y la red externa, permitiendo solamente algunos tipos concretos de conexiones y protocolos.

En estas arquitecturas, hay varias alternativas de configuración del router de filtrado de paquetes:

- Establecer permisos para que solo hosts determinados puedan abrir conexiones a la red externa para servicios concretos y preestablecidos.
- Deshabilitar todas las conexiones de los hosts a la red externa, de modo que solo sea el host bastion el que pueda establecer estas conexiones.
- Dirigir ciertos paquetes de datos del exterior a los hosts internos directamente a través del router.

La elección de una alternativa u otra dependerá de la política de seguridad establecida por la organización:

- Si la organización establece una política muy restrictiva se elegirá la opción de deshabilitar las conexiones externas.
- Sin embargo, si la organización tiene definida una política de seguridad menos restrictiva, se permitirá la conexión directa de ciertos paquetes de datos.

Los cortafuegos screened host más flexibles que las arquitecturas simples, ya que permiten que ciertos servicios que no estarían permitidos por la estructura con servicios proxy puedan redirigirse a la red interna a través del router de un modo directo.

#### **Recuerde**

En esta arquitectura, la red local permanece oculta al exterior gracias al bloqueo del tráfico de red ejecutado por el host bastion.

En comparación con las arquitecturas dual-homed host, las screened host son más seguras, al añadir una nueva capa de seguridad: mientras que las dual-homed host solo filtran la información por el host bastion, las screened host, además de filtrar la información por el host bastion, añaden un router extra de filtrado.

Sin embargo, como desventaja principal existe la posibilidad de que, si un intruso vulnera al host bastion, este tendrá acceso completo a la red interna de la organización.

### **5.3.- Arquitecturas de cortafuegos screened subnet (DMZ)**

Estas arquitecturas se ofrecen como solución al problema de seguridad del establecimiento de host bastion: en las arquitecturas anteriores, si un atacante puede acceder al host bastion, podrá también acceder a toda la red interna.

Las arquitecturas de cortafuegos screened subnet añaden un elemento más de seguridad que evite el acceso a la red por vulneración del host bastion.

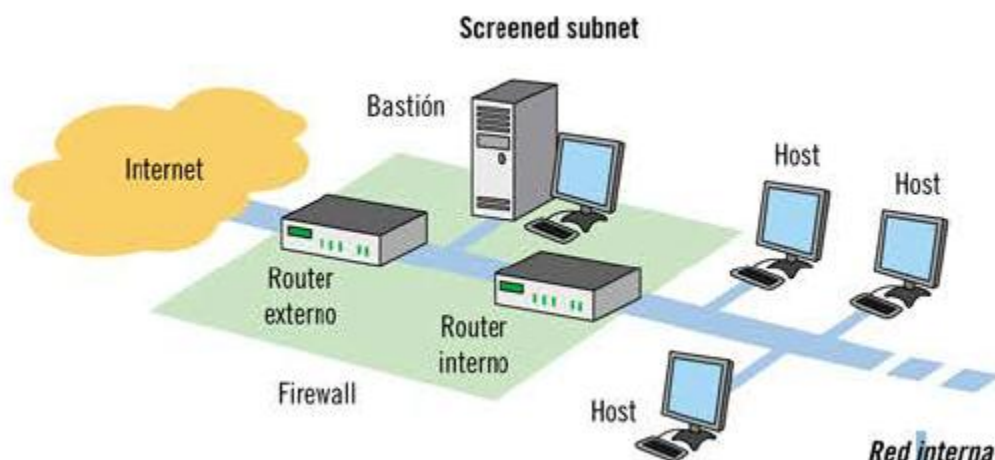
Este elemento de seguridad se establece con una red de perímetro en la que se conecta el host bastion, la red llamada "zona desmilitarizadaDMZ".

Para establecer esta arquitectura de cortafuegos se añade otro router entre el host bastion y la red interna, de modo que el host bastion se ubica entre:

- Un router interno situado entre la red interna y la red perimetral.
- Un router externo ubicado entre la red perimetral y la red externa.

Con esta configuración, se limita el peligro de la existencia de un punto único de acceso (vulnerable a ataques) con la implantación de una capa de seguridad adicional que aísla la red

interna de la red externa. De este modo, con el aislamiento del host bastion en la red perimetral, se disminuye el impacto de cualquier posible ataque a dicho host.



Para establecer esta arquitectura de cortafuegos se añade otro router entre el host bastion y la red interna, de modo que el host bastion se ubica entre:

- Un router interno situado entre la red interna y la red perimetral.
- Un router externo ubicado entre la red perimetral y la red externa.

Con esta configuración, se limita el peligro de la existencia de un punto único de acceso (vulnerable a ataques) con la implantación de una capa de seguridad adicional que aísla la red interna de la red externa. De este modo, con el aislamiento del host bastion en la red perimetral, se disminuye el impacto de cualquier posible ataque a dicho host.

Si un intruso pretende acceder a la red interna del sistema de información, solo tendrá acceso hasta la red perimetral, ya que el router interno le impedirá el acceso a la red local.

En esta arquitectura también se oculta el tráfico de paquetes de datos en la red local y se establece como una de las arquitecturas más seguras de las descritas hasta el momento.

Este nivel de protección adicional está fundamentado en las funciones de los routers internos y externos y del host bastion:

- El router externo administra el acceso del tráfico de datos de la red externa a la red perimetral. Su función principal es proteger a la red interna y a la red perimetral de ataques externos.
- El router interno, sin embargo, administra el acceso de la red perimetral a la red interna con el objetivo de proteger a la red interna de las redes externa y perimetral. Con este router se implanta un nivel adicional de seguridad que sigue protegiendo a la red interna en caso de vulnerarse el router externo.
- El host bastion se establece como punto de contacto para las conexiones de datos procedentes de la red externa.

**Nota**

La decisión de implantar una arquitectura de cortafuegos u otra dependerá de la protección que se quiera establecer y de los costes que se pretendan asumir. Si los activos a proteger no tienen valor, no tiene sentido establecer arquitecturas con zonas desmilitarizadas.

**6. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED**

A lo largo del capítulo, se han ido describiendo las principales arquitecturas de los cortafuegos de red, tanto básicas como más complejas. A partir de estas arquitecturas, se pueden establecer distintas configuraciones según las necesidades de protección de cada organización.

**6.1.- Utilización de varios host bastions**

Una de las posibles configuraciones alternativas es la utilización de varios host bastions con algunos de los siguientes objetivos:

- Aumentar el rendimiento de los servicios de red.
- Obtener servicios de apoyo con la introducción de redundancia.
- Separar servicios determinados por necesitar niveles distintos de seguridad.

**6.2.- Red perimetral con un solo router**

Otra opción sería utilizar un solo router para la implantación de una red perimetral: este router haría las funciones de router interno y externo a la vez.

El requisito fundamental para el establecimiento de esta arquitectura es que el router sea capaz de procesar todo el tráfico de datos que reciba, ya que debe filtrar tanto los datos de la red interna como los de la red externa.

**Nota**

La utilización de solo un router para el establecimiento de la red perimetral conlleva el mismo peligro que las arquitecturas screened host: si el ataque consigue vulnerar el router, tendrá acceso a toda la red interna.

### **6.3.- Utilización del host bastion como router externo**

Cuando se quieren conectar dos redes con interfaces de red distintas, se puede utilizar el host bastion como router externo.

Con esta arquitectura, el host bastion ejecuta a la vez el filtrado de paquetes de datos y los servicios proxy.

El principal inconveniente de esta configuración es su elevado coste para el desempeño de los servicios proxy. Además, aunque no se expone a vulnerabilidades, sí es cierto que el host bastion está más expuesto a posibles ataques, al no haber ninguna barrera entre la red local y este.

Por ello, se recomienda el establecimiento de medidas adicionales de seguridad que añadan protección extra al host bastion y minoren su vulnerabilidad ante intrusiones y ataques .

## **7. RESUMEN**

Un cortafuegos es un sistema compuesto por uno o varios dispositivos cuya función principal es la separación entre la red local de un sistema de información y la red exterior, de modo que se impida la entrada de ataques y se incremente la seguridad del sistema de información.

El perímetro de seguridad es el espacio protegido por el cortafuegos, mientras que la zona de riesgo es la red frente a la que se protege dicho perímetro de seguridad.

Para determinar la configuración de un cortafuegos, deben tenerse en cuenta tres características fundamentales: la política de seguridad de la organización, la monitorización del cortafuegos y la economía y presupuesto que se está dispuesto a asumir.

Atendiendo a estas características, se pueden implantar distintos tipos de cortafuegos según su ubicación y funcionalidad.

Los routers con filtrado de paquetes son cortafuegos que filtran los paquetes de datos entrantes atendiendo a una serie de reglas predefinidas.

Los gateways o pasarelas a nivel de aplicación analizan el tráfico atendiendo a los servicios solicitados (permitiendo el acceso solo a determinadas aplicaciones) y los gateways o pasarelas a nivel de circuito redirigen los paquetes de datos una vez validada la conexión.

La elección de implantar un tipo de cortafuegos u otro dependerá de las preferencias de seguridad de la organización, además del valor de los activos y de la información que se desea proteger.

Si entre estos tipos de cortafuegos no hay ninguno que se adapte lo suficiente a los objetivos de la organización, se pueden implantar cortafuegos con arquitecturas más complejas, como los cortafuegos dual-homed host, los cortafuegos screened host y las arquitecturas screened subnet (que utilizan zona desmilitarizada como medida adicional de protección).

## **CAPÍTULO 6 GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMA DE INFORMACIÓN**

### **1. INTRODUCCIÓN**

El concepto de auditoría informática es muy amplio y conlleva multitud de tareas y conocimientos que deben llevar a cabo una serie de profesionales especializados que sean capaces de desarrollar sus tareas de un modo correcto, pertinente y eficiente.

En capítulos anteriores, ya se han comentado todas las fases y procedimientos de la auditoría informática por lo que, llegado este punto, es necesario juntarlos para tener una visión global del concepto general y ser capaz de esquematizar todo el proceso.

En este capítulo se ofrecen una serie de guías con las tareas recomendadas para cada una de las fases de la auditoría de sistemas informáticos.

Eso sí, debe tenerse en cuenta que este proceso no es homogéneo para todas las organizaciones y sistemas de información, sino que será necesario adaptar las tareas descritas a los resultados obtenidos en un estudio de cada sistema y entorno que permitan obtener unas evaluaciones personalizadas y correctas.

### **2. GUÍA PARA LA AUDITORÍA DE LA DOCUMENTACIÓN Y NORMATIVA DE SEGURIDAD EXISTENTE EN LA ORGANIZACIÓN AUDITADA**

A modo de recordatorio, la auditoría informática consiste en una serie de técnicas y procedimientos realizados con el objetivo de evaluar y controlar un sistema de información. El objeto de la evaluación es proteger los activos y recursos del sistema de información mediante una ejecución correcta, eficiente y productiva de las actividades que se llevan a cabo en todo el proceso del sistema. Todo ello debe estar relacionado con las políticas definidas previamente por cada organización de modo que se obtengan los niveles de calidad de servicio establecidos.

Este proceso de auditoría se divide en cuatro fases o procesos diferenciados:

- Documentación y normativa de seguridad.
- Elaboración del plan.
- Realización de las pruebas.
- Elaboración del informe.

#### **2.1.- Guía para la auditoría de la documentación**

La documentación para la auditoría de los sistemas de información es el registro continuo de todas las tareas realizadas por el auditor. De este modo, con los documentos aportados por el auditor, se da soporte a aspectos tan importantes como:

- Las evidencias encontradas.
- Las debilidades detectadas que requieren revisión.
- Las conclusiones del auditor obtenidas a raíz de los resultados de la auditoría.

Estos documentos son denominados también "papeles de trabajo" y deben ser cumplimentados no solo en la redacción del informe de auditoría, sino que deben elaborarse a lo largo de todas las fases de la auditoría informática.

Son varios los motivos que justifican la elaboración de la documentación a lo largo de todo el proceso de auditoría, como se ve en la siguiente tabla.

Utilidades de la documentación
Recogen las evidencias detectadas durante todo el trabajo de auditoría.
Ayudan al auditor a realizar su trabajo.
Sirven como soporte del trabajo del auditor para poder ser utilizado en posteriores auditorías.
Permiten la revisión externa de la auditoría realizada por el auditor contratado.
Aportan un enfoque metodológico y protocolizado de las tareas auditoras.

Los papeles de trabajo deben diseñarse según los criterios y necesidades del auditor, teniendo en cuenta la revisión previa que este ha realizado de la organización, del sistema de información a evaluar y de los aspectos más críticos.

### Consejo

La elaboración de los papeles de trabajo debe realizarse con profesionalidad y objetividad, de modo que ayuden al auditor a realizar sus tareas con mayor facilidad.

Es de vital importancia que los papeles de trabajo posean las siguientes características:

- Completos: deben abarcar todas las tareas ejecutadas y los principales resultados detectados.
- Claros: deben redactarse de una forma clara para que sean comprensibles para todos los destinatarios de la auditoría.
- Concisos: solo incluirán aquella información que se considere relevante para una mejor comprensión de las tareas de auditoría realizadas. No se deben incluir detalles innecesarios que solo dificultarán su lectura y comprensión.

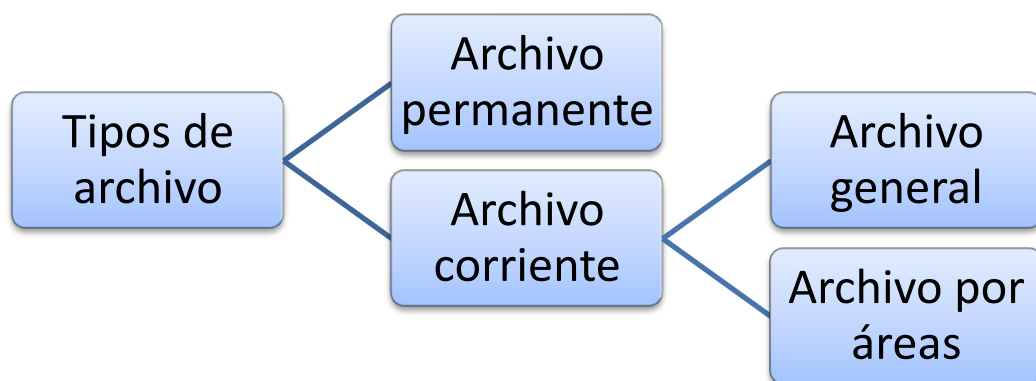


### Importante

Hay que tener en cuenta que los que van a leer los informes de auditoría y los papeles de trabajo no tienen el mismo conocimiento técnico que el auditor. Este deberá adecuar el vocabulario a un lenguaje simple y de fácil comprensión para cualquier tipo de destinatario.

#### 2.1.1.- Guía para la documentación: la utilización de los archivos

Para una correcta documentación del proceso de auditoría, se recomienda la organización de los papeles de trabajo en dos tipos de archivos distintos:



#### Archivo permanente

El archivo permanente deberá contener todos los papeles de trabajo que tengan interés continuo; es decir, que también sean de utilidad no solo en la auditoría que se realiza, sino que además sirvan como documento de consulta en futuras auditorías.

Se consideran papeles que deben incluirse en el archivo permanente:

- Aspectos generales y consideraciones sobre la organización.
- Aspectos generales y consideraciones sobre el sector de la organización.
- Composición de los directivos y miembros del consejo de administración.
- Organigrama de la organización.
- Características de los equipos que forman parte de los sistemas de información.
- Manuales de instrucciones y utilización de los equipos, dispositivos y aplicaciones del sistema.
- Esquema de la planificación plurianual de auditoría.
- Toda la información restante que se considere importante para futuras auditorías.

El archivo permanente también es denominado archivo continuo de auditoría.

### **Nota**

#### **Nota**

Una documentación adecuada y correcta servirá también como modo de prueba de todas las tareas y evaluaciones que realiza el auditor. Si hay alguna problemática con la organización por la calidad de la auditoría, el auditor podrá utilizar los papeles de trabajo para garantizar y demostrar la calidad de su trabajo.

### **Archivo corriente**

El archivo corriente, también llamado archivo de la auditoría en curso, deberá contener papeles que solo sean de utilidad para la auditoría que se está realizando. No se incluirán los documentos importantes para auditorías posteriores.

Este tipo de archivo se divide también en dos tipologías:

- Archivo general.
- Archivo por tareas.

Los documentos que se archivarán en el archivo general son los que no se pueden englobar en ninguna tarea ni área específica del trabajo de auditoría. Son sobre todo:

- El informe elaborado por el auditor.
- La carta con las recomendaciones del auditor.
- El esquema de planificación de la auditoría realizada.
- La información intercambiada con los directivos de la organización.
- El tiempo que cada miembro del equipo auditor ha utilizado para el desarrollo de cada tarea.
- Los acontecimientos posteriores a la finalización de la auditoría.

En cuanto al archivo por áreas, se recomienda elaborar y mantener un archivo de papeles de trabajo para cada área definida de la auditoría realizada. Es aconsejable recopilar todos los documentos que hacen referencia a cada área para tener una visión más global de las tareas llevadas a cabo en cada una de las áreas.

Más concretamente, se incluirán en el archivo por áreas:

- Programa de auditoría de cada área.
- Conclusiones específicas de cada área.
- Conclusiones de las tareas de auditoría y de los resultados obtenidos en cada área.

## 2.2.- Normativa de auditoría de sistemas de información

La mayoría de organismos encargados de diseñar normas estándar sobre los procesos y técnicas de auditoría clasifican dichas normas en tres grandes categorías:

- Personales.
- Para la ejecución de trabajo.
- Para la elaboración de los informes.

### Normas personales

Las normas personales del proceso de auditoría hacen referencia a características específicas del auditor o de los miembros del equipo auditor, tales como:

- Conocimientos.
- Aptitudes.
- Experiencia.
- Comportamiento ético.

Sobre todo, se destacan dos características fundamentales que debe tener todo auditor de sistemas de información en el ejercicio de sus actividades:

- **Independencia:** el auditor debe ser totalmente independiente de la organización o entidad que va a auditar.
- **Formación:** debe tener un alto nivel de conocimientos sobre la materia de los aspectos que va a auditar para desarrollar sus tareas con total profesionalidad. En caso de no tener suficiente conocimiento, deberá acudir a otros profesionales para recibir consejos y sugerencias.

#### Nota

Además de la independencia y de la formación del auditor, este deberá tener sumo cuidado profesional en el ejercicio de sus tareas, siendo cauto y ofreciendo recomendaciones y soluciones solo cuando disponga de información y documentación de apoyo suficiente.

### Normas técnicas de la ejecución del trabajo de auditoría

Cualquier tipo de trabajo con una cierta complejidad requiere una planificación y un diseño previo para su correcto desarrollo e implantación.

En la auditoría de los sistemas de información no debe ser menos: se requiere una planificación técnica y una estrategia global que sea acorde con los objetivos especificados por la organización.

Además, todo el proceso de planificación e implantación del trabajo de auditoría deberá estar sometido a un control interno para evaluar el correcto desarrollo de la misma y los puntos críticos del sistema, tanto a nivel general como en tareas específicas.

Por último, las normas técnicas de la ejecución del trabajo de auditoría también indican específicamente que las evidencias obtenidas deben tener dos características fundamentales para que sean válidas y pertinentes:

- Suficiencia.
- Competencia.

Para comprobar y demostrar que las evidencias son suficientes y competentes, se obtendrá una base razonable de apoyo a través de la inspección, observación y confirmación de la información obtenida para detectar dichas evidencias.

### **Normas de información y preparación del informe**

Los informes de auditoría también deberán ceñirse a las normas de auditoría informática generalmente aceptadas.

Estas normas, imprescindibles para una emisión del informe adecuada, hacen referencia a:

- Consistencia: en el informe deben constar las normas y principios de auditoría utilizados en la auditoría y las excepciones de incumplimientos, junto con su racionamiento.
- Revelación suficiente: la información plasmada en el informe debe ser relevante y aportar elementos nuevos. Un informe que no aporte información relevante carece por completo de calidad y utilidad.
- Opinión del auditor: una vez comentadas las técnicas utilizadas para la evaluación y los resultados obtenidos, el auditor deberá emitir una opinión sobre dichos resultados, junto con unas recomendaciones de mejora.

En resumen, la siguiente tabla ofrece una guía esquemática de la normativa de la auditoría de seguridad informática.

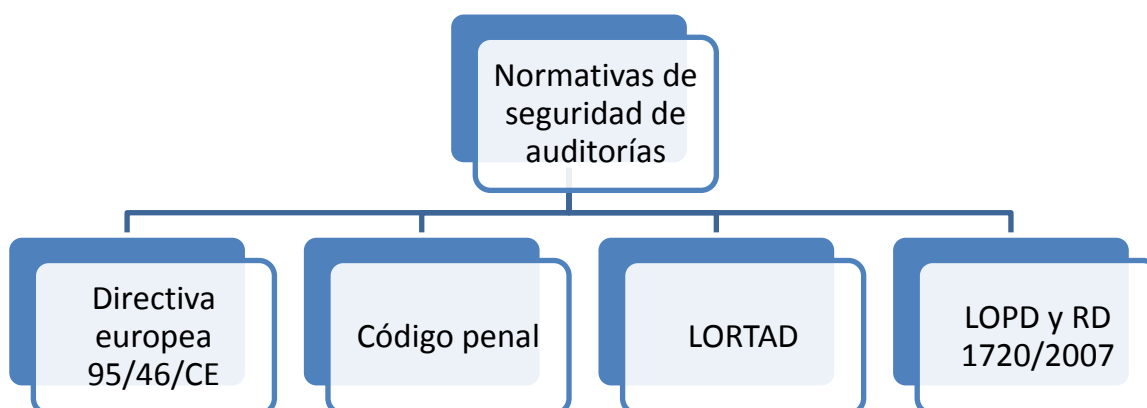
Normas de auditoría	
<b>Personales</b>	Independencia
	Formación
<b>Para la ejecución del trabajo</b>	Planificación
	Control interno
	Evidencia
<b>Informes</b>	Consistencia

Revelación suficiente
Opinión del auditor

### 2.3.- Normativa referente a la protección de datos de carácter personal

La auditoría de sistemas de información debe realizarse siempre respetando la normativa referente a la protección de datos de carácter personal, mencionada en capítulos anteriores.

A modo de guía y recordatorio, las principales normas que deberán tomarse en consideración y asegurar su cumplimiento son las del siguiente cuadro.



#### Directiva europea 95/46/CE

Esta directiva europea hace referencia a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de dichos datos.

Debe considerarse un complemento de la Ley Orgánica de Protección de Datos de Carácter Personal y establece una serie de principios de obligado cumplimiento.

#### Código penal

Aunque el Código penal recoge normativa legal de muchos otros aspectos, también hace referencia a la tipificación del delito informático y a la vulneración del derecho a proteger los datos personales, indicándose las penas y sanciones en que puede incurrirse.

**LORTAD (Ley Orgánica para el Tratamiento Automatizado de Datos)**

La LORTAD está ya derogada a favor de la actual Ley Orgánica de Protección de Datos de Carácter Personal. No obstante, se recomienda una lectura profunda para conocer los orígenes de la protección de los datos personales y su evolución.

**LOPD y R. D. 1720/2007**

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) y su reglamento de desarrollo (R. D. 1720/2007) deben ser la referencia fundamental para el desarrollo de las tareas de auditoría.

Se trata de las normas nacionales específicas referentes a la protección de datos personales y en ellas se describen las medidas de seguridad a tomar para su correcta obtención, tratamiento y conservación.

**Recuerde**

El incumplimiento de la normativa referente a la protección de datos personales en el desarrollo de la auditoría puede conllevar sanciones administrativas, por lo que no debe menospreciarse su importancia.

**3. GUÍA PARA LA ELABORACIÓN DEL PLAN DE AUDITORÍA**

Para que la auditoría de seguridad se desarrolle correctamente, será necesario elaborar un plan de auditoría.

El objetivo de esta planificación es la recopilación de información de la organización y de sus sistemas de información para obtener una información global del área a auditar.

La recopilación de información se deberá realizar a través de observaciones, entrevistas con los agentes que interactúan con el sistema y con la solicitud de documentos e información a los responsables de la organización.

Con esta información, el auditor ya será capaz de definir concretamente:

- El objetivo general del estudio.
- El alcance que la auditoría deberá tener.
- El programa desarrollado de las tareas de auditoría.

El plan de auditoría deberá señalar detalladamente el objetivo, el alcance y la dirección de la misma y deberá comprender también un plan de trabajo para que, cuando se produzca algún

cambio o modificación inesperada al plan general, estos se documenten debidamente en el plan de auditoría general.

### **3.1.- Recolección de información para el plan de auditoría**

De este modo, la elaboración del plan de auditoría deberá realizarse con una investigación previa en la que se solicitará y revisará la información de todas sus áreas.

La información a solicitar y revisar se distinguirá atendiendo a cuatro grupos diferenciados:

- A nivel organizacional.
- A nivel del área informática.
- Recursos materiales y técnicos.
- A nivel de sistemas.

#### **Información a nivel organizacional**

No solo hay que recopilar información sobre el sistema de información y sus elementos principales. Para elaborar el plan de auditoría, es imprescindible conocer el funcionamiento de la organización y el entorno que la rodea para detectar faltas de eficiencia y oportunidades de mejora.

La información que se deberá solicitar para determinar el alcance de la auditoría hace referencia a:

- Objetivos a corto y largo plazo.
- Manual, reglas y organigrama de la organización.
- Antecedentes de la organización.
- Políticas generales definidas por la organización.

#### **Información a nivel del área de informática**

Está claro que, además de conocer la información global de la organización, también habrá que tener un amplio conocimiento de los procedimientos, políticas y funcionamiento del área informática de la organización, ya que se trata del área en la que se enfoca la auditoría a realizar.

La principal información que a recolectar es:

- Objetivos a corto y largo plazo específicos del área de informática.
- Organigrama del área.
- Manual de políticas, reglamentos y normativas del área.
- Número de personas trabajando en el área y cantidad de puestos de trabajo.
- Procedimientos administrativos desarrollados.
- Presupuestos y gastos del área.

#### **Recursos materiales y técnicos**

Para determinar el alcance de la auditoría, también es necesario conocer los recursos de que dispone la organización, tanto a nivel técnico como a nivel material.

Para conocer dichos recursos, se recomienda obtener información sobre:

- Documentos, localización y características principales de los equipos del sistema (tanto los instalados como los almacenados sin instalar).
- Fechas de instalación de todos los equipos y previsiones de instalación de los equipos almacenados.
- Contratos de adquisición, alquiler y mantenimiento en vigor de los equipos y dispositivos de la organización.
- Contratos de seguros del sistema de información.
- Convenios establecidos con otras instalaciones y organizaciones.
- Configuraciones de los equipos.
- Capacidad actual y máxima de los equipos.
- Planes de expansión del sistema de información.
- Políticas de utilización de los equipos.
- Políticas de procedimientos y operaciones de la organización.

#### **Importante**

El conocimiento de los planes de expansión de la organización es muy relevante, ya que permitirá al auditor determinar si la capacidad del sistema de información actual será capaz de absorber la expansión o si, por el contrario, será necesaria una ampliación y/o renovación.

#### **Información a nivel de los sistemas de información**

En este apartado se engloba la información específica del sistema de información en cuanto a procedimientos, equipos específicos, políticas de entrada y salida, documentación, etc.

Más concretamente, se recomienda recopilar información sobre los siguientes aspectos:

- Manual de los formularios que rellenan los empleados en el desarrollo de sus tareas con el sistema.
- Manual de los procedimientos de los sistemas de información.
- Descripción genérica del sistema.
- Proceso de documentación y archivo de la información del sistema.
- Fechas de instalación de los equipos y dispositivos del sistema a auditar.
- Proyectos de instalación de ampliaciones y renovaciones de los sistemas.



### **3.2.- Elaboración del plan de auditoría y de los programas de trabajo**

Con toda la información necesaria para la comprensión de la organización y de sus sistemas de información, ya se puede proceder a establecer un plan de auditoría y unos programas de trabajo.

En otras palabras, se podrá diseñar y establecer la programación de las tareas de auditoría.

Este plan de auditoría deberá elaborarse teniendo en cuenta dos aspectos fundamentales:

- Auditoría general/específica.
- Auditoría global/parcial.

#### **Auditoría general/ específica**

Hay que tener en cuenta que no es lo mismo realizar una evaluación del sistema o de la organización en general que evaluar un área concreta de la organización.

En el caso de una auditoría general, la auditoría será más compleja y costosa y requerirá una mayor asignación de recursos.

Por el contrario, si solo se va a evaluar un área específica de la organización, los costes y recursos asignados serán bastante inferiores.

#### **Auditoría global/parcial**

Además, el plan de auditoría deberá considerar si la auditoría será a nivel global de todo el sistema de información o a nivel parcial (en el que se evaluarán solo una serie de equipos y procesos muy concretos y específicos).

El volumen de la auditoría será el que determinará la cantidad de auditores y recursos necesarios, además de las características y conocimientos especializados que deberán tener los auditores .

#### **Guía para la elaboración del plan de auditoría**

Si se tienen claros los objetivos, la metodología y el alcance de la auditoría del sistema a evaluar, ya se puede proceder a elaborar el plan de auditoría.

Los pasos a realizar en la elaboración del plan de auditoría son:

1. Identificación del origen de la auditoría.
2. Realización de una visita preliminar al área/organización que será auditada.
3. Establecimiento de los objetivos generales de la auditoría.
4. Determinación de los puntos y elementos a evaluar.
5. Elaboración de planes y presupuestos para la realización de las tareas de auditoría.

6. Identificación y selección de los métodos, herramientas, utilidades y procedimientos que van a ser necesarios a lo largo de la auditoría.
7. Asignación de los recursos materiales y técnicos necesarios para el desarrollo de las tareas.

Este plan se debe elaborar ateniéndose a las recomendaciones reflejadas en la siguiente tabla.

Guía para la elaboración del plan de auditoría
1. En el plan de auditoría no se establecen fechas ni calendarios, ya que solo figurarán los recursos genéricos (no específicos).
2. Se establece la necesidad de recursos y esfuerzos globales para la auditoría.
3. Se establecen las prioridades de las áreas o materias auditables, teniendo en cuenta las preferencias de la organización auditada.
4. Se establece la disponibilidad de los recursos durante el proceso de evaluación (es posible que algún recurso no pueda ser utilizado mientras se revisa).
5. Se asignan y estructuran las actividades y tareas que deberán ser realizadas por cada miembro del equipo auditor.
6. Por último, en el plan deben especificarse claramente todas las ayudas y facilidades que el auditor debe recibir por parte de la organización auditada.

### Contenido del plan de auditoría

El plan de auditoría debe ser establecido y comunicado debidamente a la organización auditada para que esta revise y apruebe dicho plan o para que proponga las modificaciones que sean necesarias.

El plan de auditoría deberá contener, como mínimo, los siguientes aspectos:

- Objetivos y alcance de la auditoría.
- Criterios utilizados.
- Identificación de las áreas que serán auditadas.
- Identificación del personal y de las funciones de las áreas auditadas.
- Identificación de los aspectos de calidad a los que se les debe asignar una prioridad alta.
- Identificación de la documentación de referencia.
- Tiempo y duración estimados para las entrevistas iniciales.
- Ubicación de la auditoría y fechas estimadas.
- Cronograma de las reuniones del responsable de seguridad de la organización o del sistema informático con el auditor.
- Requerimientos confidenciales.
- Contenido, formato y estructura básica del informe de auditoría.

Un ejemplo de formato para el plan de las auditorías podría ser el siguiente:

<b>Formato para el plan de auditoría</b>				
Área o sistema auditado:				
Responsable del área auditada:				
Auditor principal:				
Fechas de ejecución de la auditoría:				
Fecha de presentación del Informe:				
<b>1. OBJETO DE LA AUDITORÍA</b>				
<b>2. ALCANCE DE LA AUDITORÍA</b>				
<b>3. DOCUMENTACIÓN</b>				
<b>4. EQUIPO AUDITOR</b>				
<b>5. PERSONAL ENTREVISTADO</b>				
<b>6. ACTIVIDADES PREVISTAS Y REALIZADAS</b>				
FECHA:				
HORA	ÁREA	NÚMERO	AUDITOR	AUDITADO
<b>7. APROBACIÓN</b>				
<b>Auditor principal</b>			<b>Responsable del área auditada</b>	

#### 4. GUÍA PARA LAS PRUEBAS DE AUDITORÍA

Cuando ya se tiene bien definida la planificación de la auditoría de seguridad, el siguiente paso es implantarla. La implantación consistirá en la realización de una serie de pruebas cuyos resultados permitan detectar debilidades y fortalezas del sistema de información auditado y justifiquen la detección de las evidencias.

#### 4.1.- Tipos de pruebas

Para la obtención de las evidencias, se pueden utilizar varios tipos de pruebas, técnicas y procedimientos, que se describen a continuación.

### **Cuestionarios**

Para obtener información que justifique las evidencias detectadas, el auditor debe enviar una serie de cuestionarios a personas concretas y adecuadas, sin que estas sean de obligatorio cumplimiento.

### **Entrevistas**

Después de la primera toma de contacto, el auditor debe recabar información más detallada de tres formas:

- Con la petición de documentación específica.
- Con entrevistas abiertas sin guión preestablecido.
- Con entrevistas predeterminadas y guionizadas.

#### **Nota**

La fase de entrevistas es una de las más importantes de toda la auditoría, ya que permite conocer detalles y matices imposibles de detectar con herramientas y aplicaciones informáticas.

### **Checklist**

Aparte de comprobar el funcionamiento del sistema del auditado, el auditor debe someter al auditado a un cuestionario llamado *checklist*.

Esta *checklist* debe ser perfectamente comprensible para el auditado, de modo que las respuestas expresadas reflejen claramente la situación actual del sistema de información.

Se recomienda que las *checklists* sean respondidas oralmente, no por escrito.

Cabe destacar dos tipos de *checklist*:

- Rango.
- Binario.

Las *checklists* de rango están formadas por una serie de preguntas a las que el auditor debe responder dentro de un rango preestablecido. Según la puntuación del rango obtenida, ya se hacen más específicas sobre los motivos de la puntuación.

Sin embargo, la *checklist* binaria está formada por preguntas de respuesta única y excluyente: sí o no. Es necesario que las preguntas sean muy precisas para que los resultados obtenidos sean claros y exactos.

**Nota**

Aunque las *checklists* binarias exigen menos uniformidad al equipo auditor al ser de respuesta cerrada, ofrecen información menos rica que las *checklists* de rango, en las que se permite un abanico de puntuaciones.

**Comparación de programas**

La comparación de programas consiste en la comparación de una versión de una aplicación determinada en ejecución con otra versión de la misma aplicación modificada a propósito para detectar las diferencias.

**Mapeo y rastreo de programas**

Con aplicaciones especializadas, se analizan los programas que se están ejecutando en ese momento, indicando información específica sobre:

- Procesamiento de la información.
- Variables de memoria utilizadas.

**Datos de prueba**

Con la utilización de los datos de prueba se preparan una serie de transacciones y operaciones con datos correctos e incorrectos para comprobar si los controles internos funcionan debidamente.

**Simulación paralela**

La simulación paralela consiste fundamentalmente en el desarrollo de aplicaciones y programas que simulen programas específicos de un sistema en ejecución.

El objetivo es procesar ambos programas en dos entornos simulados distintos para detectar las diferencias en su funcionamiento y en sus resultados.

### Trazas o huellas

Las trazas o huellas se han comentado en capítulos anteriores. Para detectarlas se utilizan aplicaciones específicas encargadas de rastrear las rutas que siguen los datos a través de los programas.

De este modo, con el rastreo de los datos se pueden detectar todos los fallos y problemas de validación que pueden tener los datos hasta llegar a su destino.

#### Nota

El rastreo de trazas de datos se llevará a cabo teniendo en cuenta la distinta intensidad de tráfico de datos de un sistema a lo largo de un período determinado. No será lo mismo un rastreo en horas punta que en horas de baja actividad

### Logs o archivos de registros

Con el análisis de *logs* o archivos de registros se puede observar el historial de los datos y de las modificaciones que han ido sufriendo en un período determinado.

### Software de auditoría

En la actualidad, existen en el mercado programas y aplicaciones específicos para la realización de auditorías externas que ayudan al auditor a realizar la gran mayoría de pruebas descritas anteriormente.

En resumen, en la siguiente tabla se muestra una guía simplificada de las principales pruebas de auditoría recomendadas.

Pruebas de auditoría	
<b>Cuestionarios</b>	Obtención de información general.
<b>Entrevistas</b>	Obtención de información específica.
<b>Checklists</b>	Cuestionario concreto y específico.
<b>Comparación de programas</b>	Comparación de programas en versión de ejecución y en versión piloto.

<b>Mapeo y rastreo de programas</b>	Análisis de los programas en ejecución.
<b>Datos de prueba</b>	Verificación del correcto funcionamiento de los controles internos.
<b>Simulación paralela</b>	Simulación simultánea de un mismo programa.
<b>Trazas o huellas</b>	Rastreo de la ruta de los datos.
<b>Logs o archivos de registro</b>	Comprobación del historial de la información.
<b>Software de auditoría</b>	Utilización de programas especializados para la auditoría .

### Guía para la elaboración del informe de auditoría

El informe de auditoría es el documento escrito que refleja los resultados obtenidos a través de las pruebas de auditoría junto con sus conclusiones, observaciones, sugerencias y recomendaciones realizadas por el auditor.

La importancia de una correcta elaboración de este informe es fundamental, ya que es el reflejo de todo el trabajo del auditor a la organización que lo contrató para la auditoría.

#### 4.2.- Documentos específicos

El informe de auditoría debe contener específicamente tres documentos específicos:

- Carta de envío.
- Resumen ejecutivo.
- Informe de auditoría informática.

#### Carta de envío

La carta de envío debe ser la presentación del auditor y de la empresa a la que pertenece como trabajador.

Es imprescindible que se muestre la profesionalidad del auditor y que tiene un extenso conocimiento, tanto en la materia auditora como en la organización que se ha estado evaluando.

#### Resumen ejecutivo

El resumen ejecutivo incluirá los aspectos generales de la auditoría. Más específicamente, deberá contener:

1. Antecedentes.

2. Fundamento legal y normativa.
3. Objetivos y alcance de la auditoría.
4. Procedimientos relevantes utilizados y limitaciones encontradas.
5. Resumen breve de los resultados de la auditoría.
6. Identificación de los hechos que deben originar responsabilidades.
7. Comentarios de la organización sobre la aceptación del informe de auditoría.

**Importante**

En el informe ejecutivo no deben utilizarse términos o acrónimos informáticos. Hay que tener en cuenta que será leído por directivos y gerentes que no tienen los conocimientos técnicos de la auditoría informática.

**Informe de auditoría informática**

Esta parte del informe es la que debe contener la información importante sobre el desarrollo de las tareas de auditoría, los resultados obtenidos y las recomendaciones y sugerencias del auditor.

En este documento se deberá incluir, como mínimo:

1. Fecha de emisión del informe.
2. Alcance de la auditoría, limitaciones y objetivos establecidos.
3. Descripción de la metodología aplicada para la realización del proceso de auditoría.
4. Documentación revisada en la auditoría.

**Nota:** Además de la documentación revisada en la auditoría, también se incluirá toda la documentación elaborada por el auditor a lo largo de todo el proceso auditor.

5. Pruebas de auditoría realizadas.
6. Fechas en las que se ha llevado a cabo el proceso de auditoría (concretándose las fechas del trabajo de campo, de las entrevistas, reuniones y revisiones técnicas ejecutadas).
7. Limitaciones detectadas en la realización de las pruebas que impidan la emisión de un juicio del auditor sobre ciertos aspectos de la seguridad del sistema informático.
8. Informe ejecutivo en el que se incluya un resumen de los aspectos más destacables y del grado general de cumplimiento de los objetivos de auditoría.
9. Sección de recomendaciones. Estas deben cumplir dos requisitos:
  - a. Las recomendaciones deben ser abiertas, facilitando varias alternativas de solución posibles que permitan elegir al responsable de seguridad.
  - b. Las recomendaciones deben formularse indicando específicamente la existencia de riesgos e implicaciones.



10. Sección de anexos: donde se describirán los detalles y resultados de las pruebas de auditoría ejecutados que fundamentan las conclusiones del auditor mostradas en el informe ejecutivo.
11. Anexo opcional sobre las opiniones emitidas por el responsable de seguridad del sistema de información frente a los comentarios del informe y de las acciones que se tomarán para solucionar las posibles deficiencias.

**Nota:** El informe debe incluir las no conformidades del responsable de seguridad sobre las tareas y procedimientos realizados por el auditor, de modo que queden reflejadas en papel y justifiquen su actuación.

12. Firma del auditor (si solo hay un auditor) o del jefe del equipo de auditoría (en el caso de existir un equipo auditor) y listado de los miembros del equipo.

Un ejemplo del informe de auditoría se muestra a continuación.

Formato para el plan de auditoría
Área o sistema auditado: Responsable del área auditada: Auditor principal: Fechas de ejecución de la auditoría: Fecha de presentación del informe:
1. OBJETO DE LA AUDITORÍA
2. ALCANCE DE LA AUDITORÍA
3. DOCUMENTACIÓN
4. EQUIPO AUDITOR
5. PERSONAL ENTREVISTADO
6. ACTIVIDADES PREVISTAS Y REALIZADAS
7. ESTADO DE LA GESTIÓN DE LA AUDITORÍA
En el estado de gestión se incluirán las fortalezas y oportunidades de mejora, además de las no conformidades encontradas.
8. CONCLUSIONES
9. APROBACIÓN DEL INFORME

## 6. Resumen

La realización de las tareas de auditoría de un sistema de información se divide en varias fases.

En primer lugar, se auditan la documentación y la normativa de seguridad que puedan verse relacionados con el sistema a auditar. Lo más frecuente es la revisión y comprobación de las normas de auditoría y de las normas referentes a la protección de datos personales.

A continuación, una vez obtenida y revisada toda la documentación necesaria y la normativa implicada, se debe realizar un plan de auditoría, en el que se describen los objetivos, las partes implicadas y las tareas a desarrollar durante todo el proceso auditor.

En tercer lugar, cuando ya se tiene definida la planificación de las tareas auditoras, se puede proceder a la realización de las pruebas de auditoría.

La elección de las pruebas a ejecutar dependerá de las características de la organización, de las del sistema de organización y de los aspectos principales que se desean auditar, entre otros factores.

Por último, con los resultados obtenidos con las pruebas de auditoría se realiza uno de los documentos más relevantes de la auditoría: el informe de auditoría. Este estará formado por varios documentos y deberá ser redactado de modo que se reflejen a la perfección la situación real del sistema de un modo comprensible para la organización y las sugerencias y recomendaciones formuladas por el profesional auditor.