Auditar redes de comunicación y sistemas informáticos

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

Auditoria Informatica

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

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

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 **ISACA** (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. profesionales a unos principios éticos y morales adecuados.

Normas profesionales de la ISACA

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.

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.

Normas profesionales de la ISACA

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.

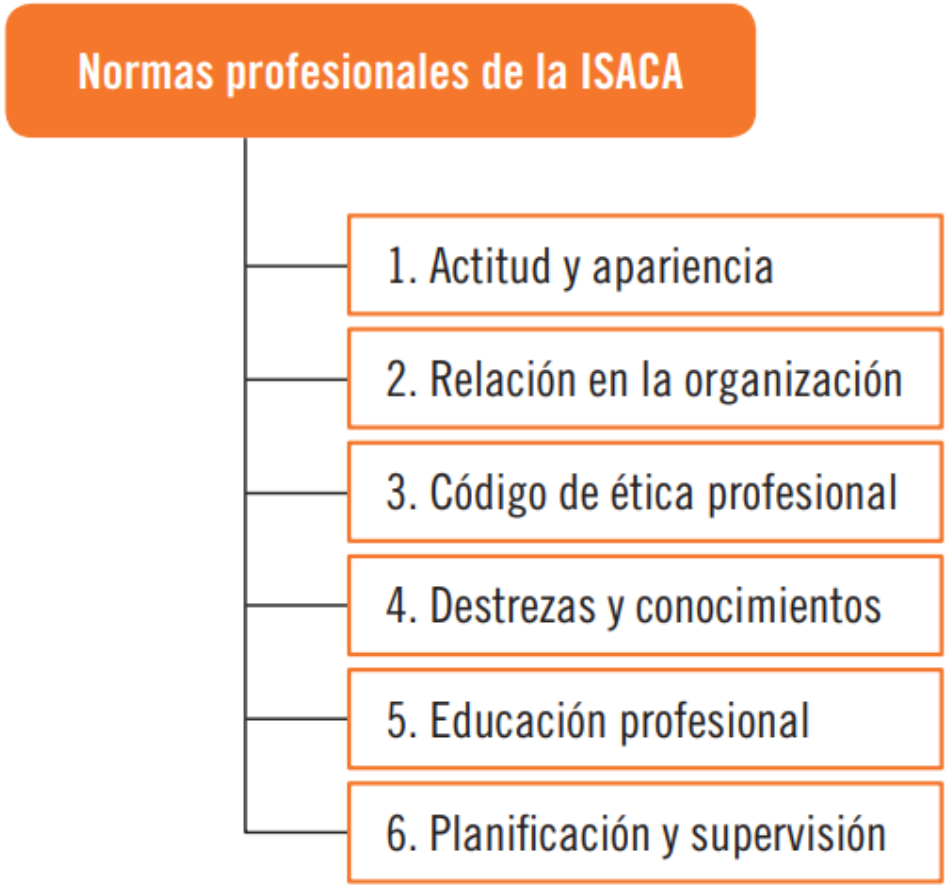
7. En el proceso de auditoría, el auditor debe respaldarse necesariamente con evidencias que confirmen sus hallazgos, resultados y conclusiones.

8. Las tareas de auditoría deben llevarse a cabo son sumo cuidado profesional, cumpliendo las normativas de auditoría aplicables.

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.

Normas profesionales de la ISACA



El Código de Ética de ISACA

Establece una serie de preceptos con el fin de guiar la conducta profesional de los miembros de la organización y de los poseedores de su certificación. Más concretamente, este código de ética se define en siete lineamientos:

1. Apoyar la implementación y el cumplimiento de los estándares, procedimientos, normas y controles de los sistemas de información y de la tecnología de la empresa.
2. Ejecutar las tareas con objetividad, diligencia y rigor profesional, siguiendo los estándares marcados en la profesión.
3. Actuar en interés de las partes interesadas (empleadores, clientes, público en general, etc.) de un modo diligente, leal y honesto, sin contribuir en actividades ilícitas o incorrectas que puedan desacreditar la profesión o a la asociación.
4. Mantener la confidencialidad de la información que se obtenga en el desarrollo de la auditoría, salvo que sea exigida por una autoridad legal. La información no se podrá utilizar en beneficio propio ni cederla a terceros inapropiados.
5. Mantener la aptitud y capacidad en los campos relacionados con la auditoría y los sistemas de información mediante la realización de actividades que permitan actualizar y mejorar las habilidades, competencias y conocimientos necesarios.
6. Informar a las partes involucradas de los resultados obtenidos en el proceso de auditoría.
7. Apoyar la educación profesional de las partes interesadas (gerencia, clientes, etc.) para una mejor comprensión de las tareas de auditoría, de la gestión de los sistemas de información y de la tecnología de la organización.

Código deontológico de la función de 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.

Código deontológico de la función de auditoría

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.

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.

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.

Código deontológico de la función de auditoría

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.

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.

Código deontológico de la función de auditoría

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.

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.

Código deontológico de la función de auditoría

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.

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.

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.

Código deontológico de la función de auditoría

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.

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.

Principio de veracidad

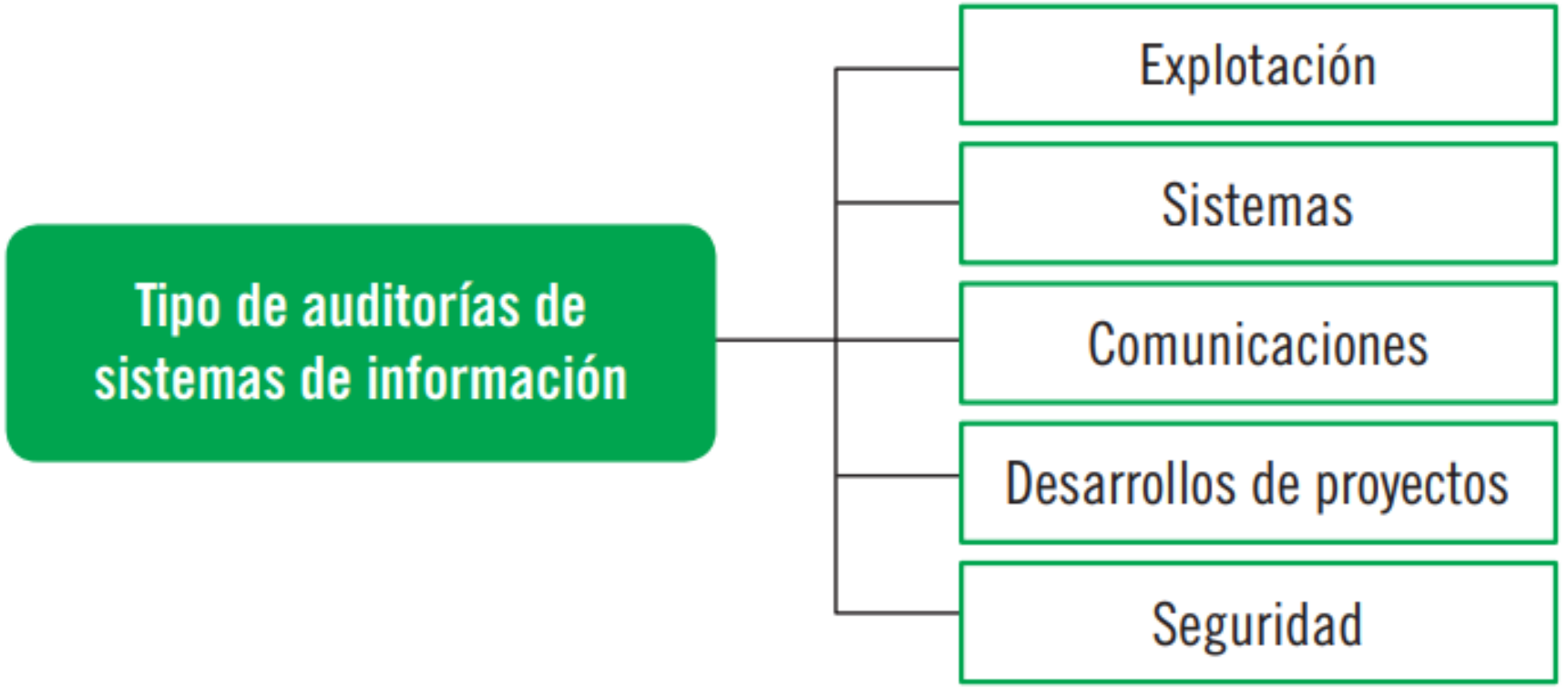
- El auditor, en el ejercicio de su profesión, deberá asegurar en todo momento la veracidad de sus manifestaciones y opiniones, sin incumplir el secreto profesional y el respeto al auditado.

Relación de los distintos tipos de auditoría en el marco de los sistemas de información

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

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

Relación de los distintos tipos de auditoría en el marco de los sistemas de información



Relación de los distintos tipos de auditoría en el marco de los sistemas de información

Auditoría informática de explotación

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.

- Sistemas operativos
- Software básico
- Tunning
- Optimización de los sistemas y subsistemas
- Administración de las bases de datos
- Investigación y desarrollo

Relación de los distintos tipos de auditoría en el marco de los sistemas de información

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.

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.

Auditoría de seguridad informática

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

Auditorías de buenas prácticas en Seguridad de la Información

En la realización de este tipo de auditorías es habitual es uso de **marcos de referencia o frameworks** (a nivel nacional o internacional)

Algunos de los marcos de referencia más reconocidos en este ámbito son los siguientes:

- International Organization for Standardization (ISO 27000)
- National Institute of Standards and Technology (NIST)
- Esquema Nacional de Seguridad (ENS)

Auditorías de cumplimiento legal y regulatorio

En la realización de este tipo de auditorías, **se evalúa el cumplimiento de leyes y reglamentos relacionados con la seguridad**. Algunas de las más importantes son las nombradas a continuación:

- Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)
- Reglamento General de Protección de Datos (RGPD)
- Ley de Servicios de la Seguridad de la Información (LSSICE)
- Ley de Propiedad Intelectual (LPI)
- Esquema Nacional de Seguridad (ENS)
- Ley de Protección de Infraestructuras Críticas (PIC)
- Ley de Prevención de Riesgos Laborales (LPRL)

Hacking ético

Dentro de las auditorías de hacking etico, podemos diferenciar entre; **auditorías de vulnerabilidades**, **test de intrusión** y ejercicios de **Red Team**. Cada uno de estos tipos de auditoría tiene unas especificaciones y unas restricciones características, como lo son el alcance o el tipo de medios técnicos a utilizar. Sin embargo, el objetivo de estos no es otro que el de encontrar posibles vulnerabilidades o agujeros de seguridad en la infraestructura tecnológica de la organización.

En este tipo de auditorías, se cuenta con metodologías y estándares para asegurar resultados efectivos. Algunas de las metodologías más utilizadas son:

Open Source Security Methodology Manual (OSSTMM)

Center for Internet Security (CIS)

Open Web Application Security Project (OWASP)

MITRE ATT&CK.

Criterios a seguir para la composición del equipo auditor

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.

Criterios a seguir para la composición del equipo auditor

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.

Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

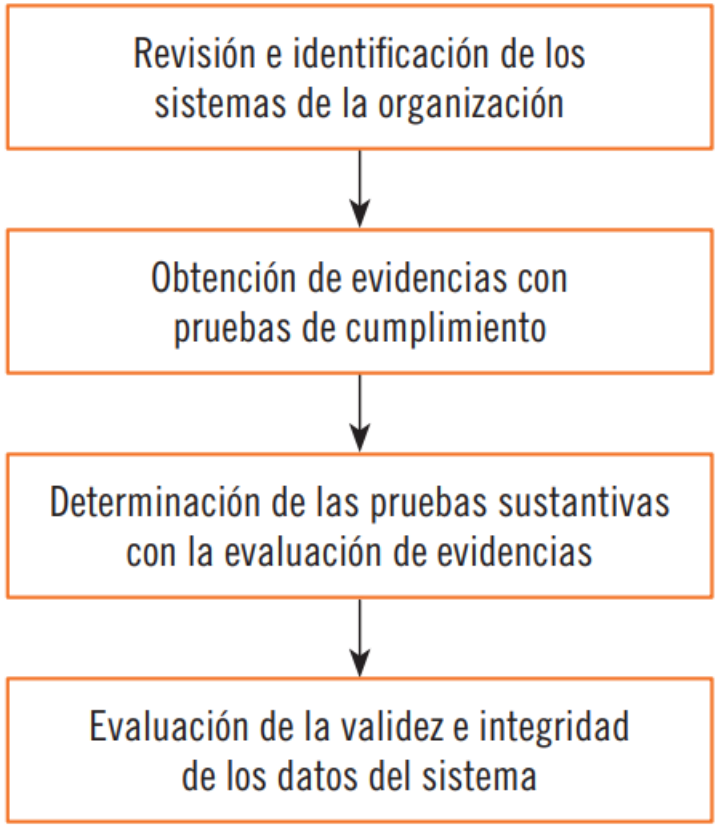
- **Pruebas sustantivas**: Verifican el grado de confiabilidad del SO del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.
- **Pruebas de cumplimiento**: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas sustantivas**: Verifican el grado de confiabilidad del SO del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.
- **Pruebas de cumplimiento**: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento



Tipos de pruebas a realizar en el marco de la auditoría, pruebas sustantivas y pruebas de cumplimiento

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.

Tipos de muestreo a aplicar durante el proceso de auditoría

Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

Denominada por sus siglas en inglés (**Computer Assisted Audit Techniques**) o **Técnicas de Auditoría Asistidas por Computador**. Son herramientas y técnicas de auditoría que permiten al auditor aumentar el alcance y la eficiencia de la auditoría con procedimientos automatizados. Pueden generar una gran parte de la evidencia de la auditoría de los sistemas de información.

Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

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.

Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

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

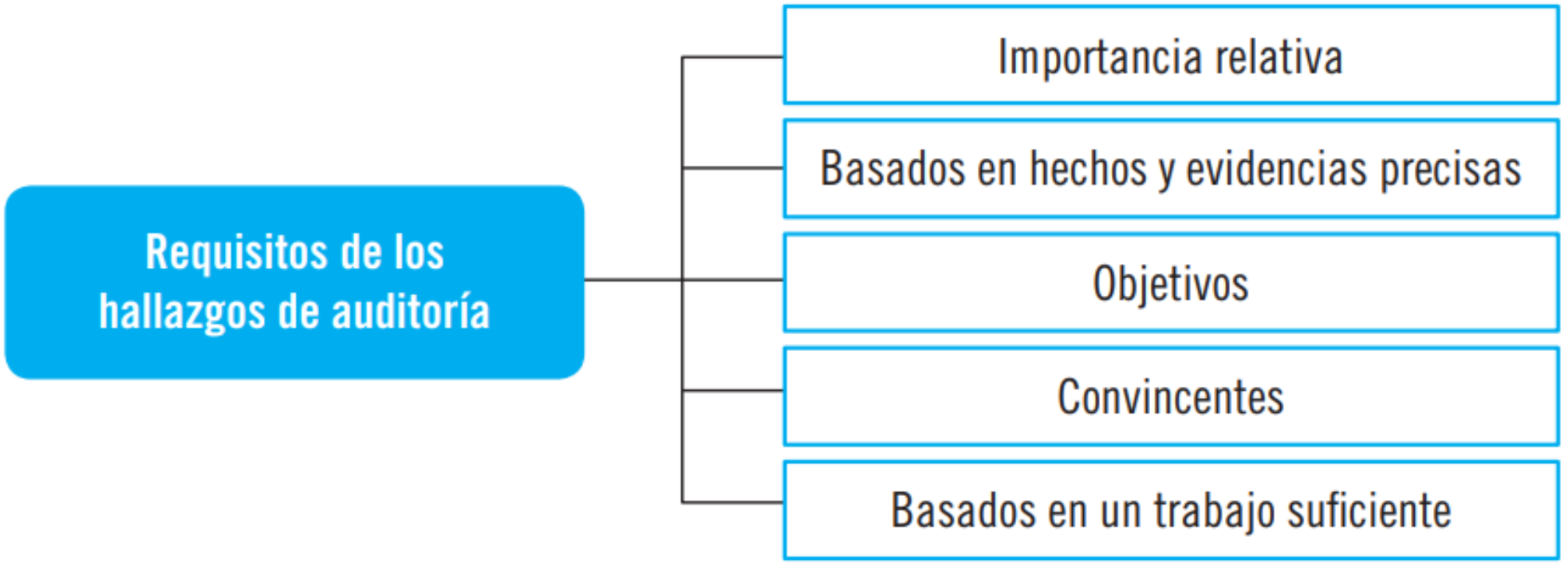
- Capacidad de muestreo.
- Utilización de algoritmos de búsqueda de patrones de fraude.
- Acceso a datos de varios formatos.
- Filtrado de datos.
- Recurrencia de pruebas.
- Relación de información procedente de varios archivos distintos.
- Generación de informes y reportes, tanto de texto como con gráficos.

Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

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.

Explicación de los requerimientos que deben cumplir los hallazgos de auditoría

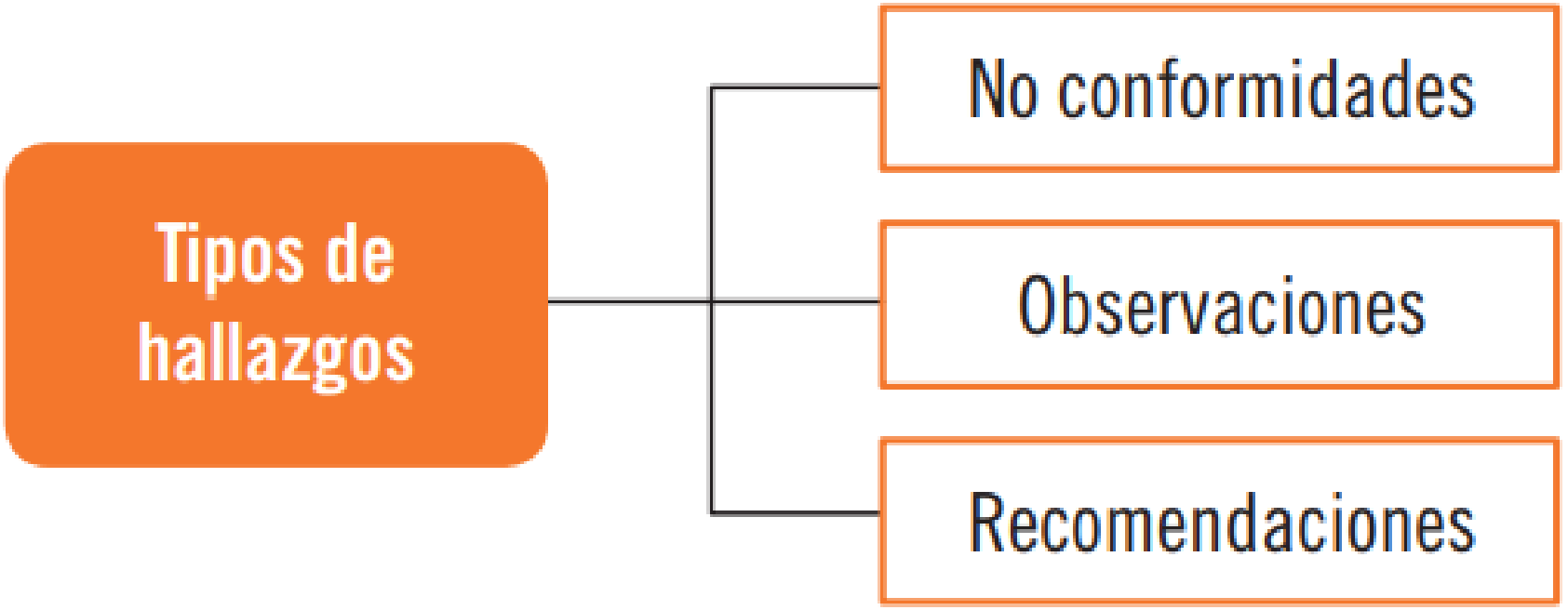


Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades

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.

Aplicación de criterios comunes para categorizar los hallazgos como observaciones o no conformidades

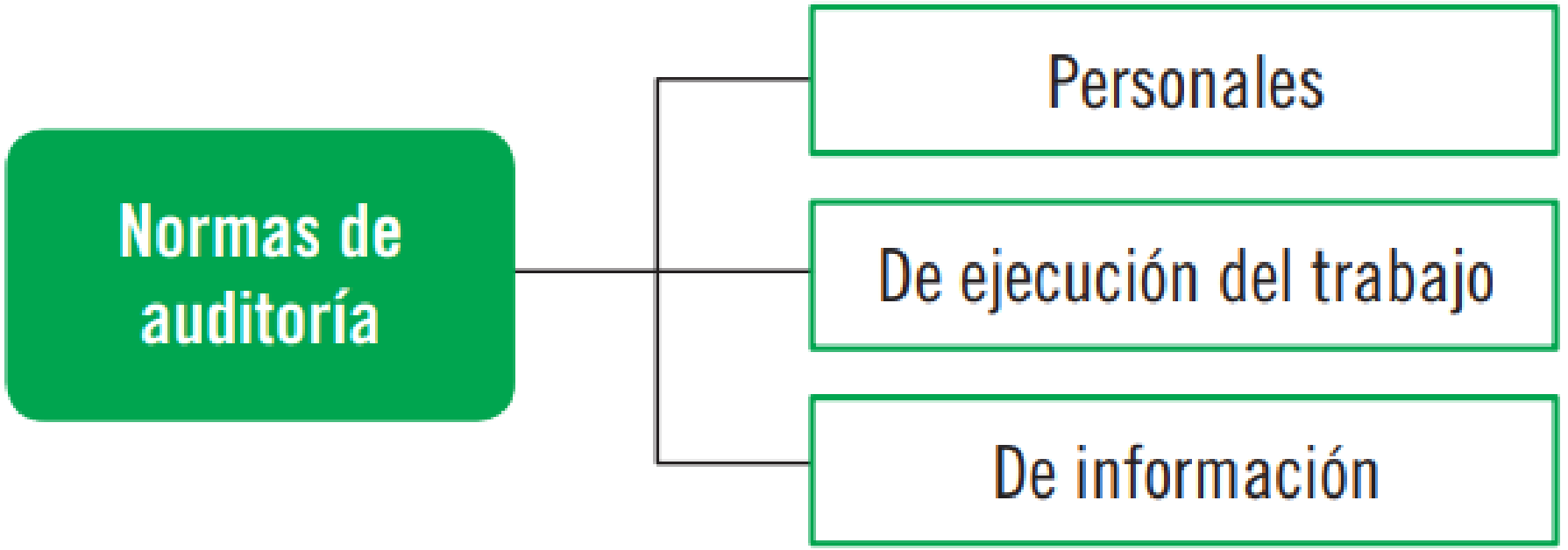


Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas

- **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.

Relación de las normativas y metodologías relacionadas con la auditoría de sistemas de información comúnmente aceptadas



Auditar redes de comunicación y sistemas informáticos

2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

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.

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.

Conceptos principales de la protección de datos

- **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.

Conceptos principales de la protección de datos

■ **Procedimiento de disociación**: tratamiento de datos de carácter personal con el fin de aislar la información del interesado que se obtenga de ellos.

■ **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

Principios de protección de datos de carácter personal

Principios de la protección de datos de carácter personal	
Principio de calidad	Datos adecuados, pertinentes y no excesivos según su finalidad.
Principio de consentimiento del afectado	Deber información y de consentimiento previo e inequívoco del interesado para poder tratar los datos.
Datos especialmente protegidos	Datos que requieren medidas más estrictas por hacer referencia a la ideología, religión o creencias del interesado.
Datos relativos a la salud	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.
Principio de seguridad de los datos	El responsable del fichero deberá establecer medidas de seguridad suficientes para mantener la integridad de los datos y no sufrir modificaciones no autorizadas.
Principio de deber de secreto	El responsable del fichero y todos los partícipes de su tratamiento deberán someterse obligatoriamente al secreto profesional aunque ya se haya terminado la relación contractual.
Principio de comunicación de datos	Condiciones específicas para la cesión de datos personales a terceros.
Principio de acceso a los datos por cuenta de terceros	Relación contractual entre el responsable del tratamiento del fichero y el tercero, convirtiéndose este desde ese momento en encargado del fichero.

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).

Principios de protección de datos personales de la Directiva 95/46/CE

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

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

Principios de protección de datos personales de la Directiva 95/46/CE

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

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.

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)

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.

- 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

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 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

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 95/46/CEE, mencionada anteriormente, y derogó a la antigua Ley Orgánica de Tratamiento Automatizado de Datos (LORTAD).

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.

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.

Contenido de la LOPD

Título	Descripción
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.

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

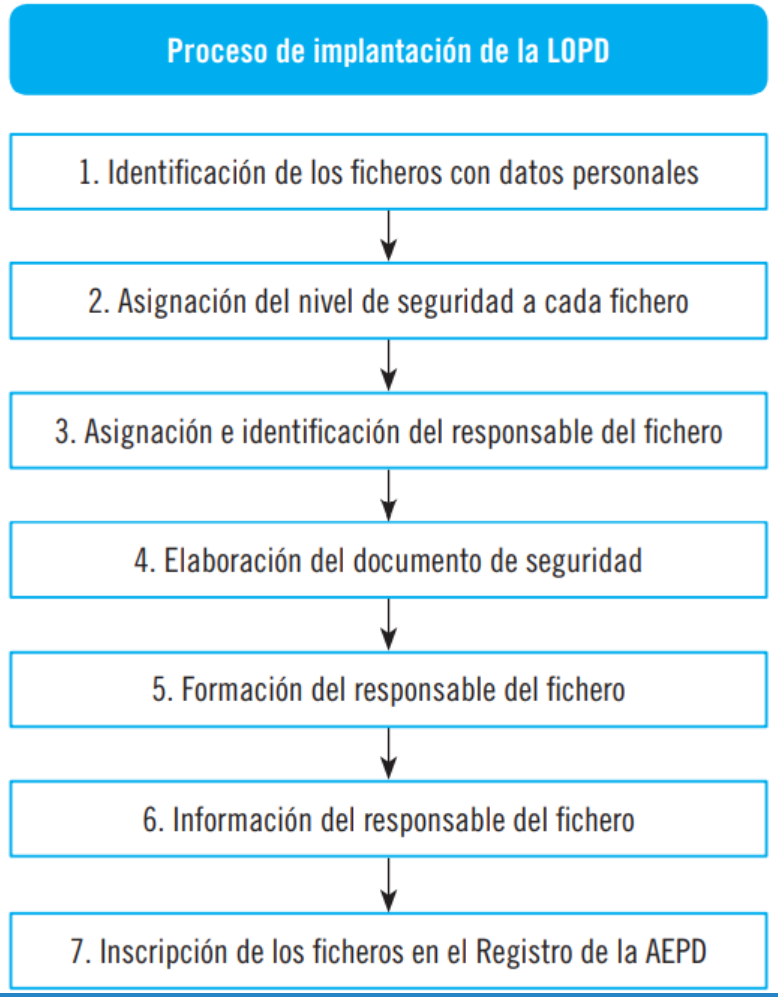
En 2008 entró en vigor el Reglamento de desarrollo de la LOPD (Real Decreto 1720/2007) con la finalidad de establecer medidas de protección de datos personales referentes al derecho de la intimidad.

Contenido de la LOPD	
Título	**Descripción**
Título VIII: De las medidas de seguridad en el tratamiento de datos de carácter personal	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.

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.

Proceso de implantación de la LOPD



Explicación de las medidas de seguridad para la protección de los datos de carácter personal recogidas en el Real Decreto 1720/2007

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
Medidas de nivel básico
Se aplican a cualquier fichero o tratamiento de datos de carácter personal.
Niveles de seguridad de los datos de carácter personal
Medidas de nivel medio
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.
Medidas de nivel alto
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.

Medidas de seguridad generales para todo tipo de ficheros

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.

Medidas de seguridad generales para todo tipo de ficheros

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.

Medidas de seguridad para el tratamiento de datos automatizado

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.

Medidas de seguridad para el tratamiento de datos automatizado

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.

Medidas de seguridad para el tratamiento de datos automatizado

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.

Medidas de seguridad para el tratamiento de datos automatizado

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.

Medidas de seguridad para el tratamiento de datos no automatizado

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.

Medidas de seguridad para el tratamiento de datos no automatizado

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.

Guía para la realización de la auditoría bienal obligatoria de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal

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

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.