MF0487_3 UD1-UD2 Auditoría de seguridad informática

Módulo 2

UNIDAD DIDÁCTICA 1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

Código deontológico de la función de auditoría.

Imagina al auditor informático como un detective de la seguridad. Su trabajo es encontrar vulnerabilidades y riesgos en los sistemas, pero siempre con ética y profesionalismo. El código deontológico es su guía para actuar correctamente.

¿Qué es un código deontológico?

Es un conjunto de normas y principios éticos que regulan la conducta de los profesionales de una determinada área. En el caso de la auditoría informática, establece cómo debe comportarse un auditor para garantizar la integridad, objetividad y confidencialidad en su trabajo.

Principios clave del código deontológico:

- **Integridad**: El auditor debe ser honesto, transparente y actuar con rectitud en todo momento.
- **Objetividad**: Debe realizar su trabajo de forma imparcial, sin dejarse influir por intereses personales o prejuicios.
- **Confidencialidad**: Debe proteger la información que maneja durante la auditoría, evitando su divulgación no autorizada.
- **Competencia profesional**: Debe mantener sus conocimientos actualizados y realizar su trabajo con diligencia y rigor.
- **Independencia**: Debe evitar cualquier situación que pueda comprometer su independencia de juicio.
- **Responsabilidad**: Debe asumir las consecuencias de sus acciones y decisiones.
- **Legalidad**: El auditor debe cumplir con todas las leyes y regulaciones aplicables.

¿Por qué es importante?

- **Genera confianza**: Un código deontológico sólido genera confianza en los clientes y en la sociedad en general.
- **Garantiza la calidad**: Asegura que las auditorías se realicen con profesionalismo y rigor.
- **Protege la información**: Salvaguarda la confidencialidad de los datos sensibles.
- **Evita conflictos de interés**: Previene situaciones que puedan comprometer la objetividad del auditor.
- **Promueve la ética**: Fomenta una cultura de integridad y responsabilidad en la profesión.

Ejemplos prácticos:

- Un auditor no debe aceptar sobornos o regalos que puedan influir en su juicio.
- Debe informar de forma clara y precisa sobre los hallazgos de la auditoría, sin ocultar información relevante.
- No debe utilizar la información confidencial a la que tiene acceso para beneficio propio o de terceros.
- Debe informar a las autoridades pertinentes en caso de detectar alguna actividad ilegal.

¿Dónde encontrar códigos deontológicos?

Existen diversas organizaciones profesionales que establecen códigos deontológicos para auditores informáticos, como:

- Instituto de Auditores Internos de España (IAI).
- Asociación de Técnicos de Informática (ATI).

En resumen:

El código deontológico es la brújula que guía al auditor informático en su trabajo. Le ayuda a tomar decisiones éticas y responsables, garantizando la calidad y la integridad de las auditorías.

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

Imagina que los sistemas de información de una empresa son como el cuerpo humano. Para mantenerlos sanos y funcionando correctamente, necesitamos diferentes tipos de chequeos. En el mundo de la auditoría informática, estos chequeos son los distintos tipos de auditoría.

¿Qué son los tipos de auditoría informática?

Son evaluaciones especializadas que se centran en diferentes aspectos de los sistemas de información de una organización. Cada tipo de auditoría tiene un objetivo específico y utiliza diferentes técnicas y herramientas.

Tipos principales de auditoría informática:

1. **Auditoría de seguridad**:
    a. Es como un chequeo de seguridad para detectar posibles amenazas y vulnerabilidades en los sistemas.
    b. Evalúa la eficacia de los controles de seguridad, como firewalls, antivirus y sistemas de detección de intrusiones.
    c. Busca debilidades que podrían ser aprovechadas por atacantes para robar información o dañar los sistemas.
2. **Auditoría de cumplimiento**:
    a. Es como un chequeo de cumplimiento de las normas y leyes aplicables.
    b. Verifica que los sistemas de información cumplan con las regulaciones, como el Reglamento General de Protección de Datos (RGPD) o la norma ISO 27001.
    c. Asegura que la organización está protegiendo adecuadamente la información confidencial y cumpliendo con sus obligaciones legales.

3. **Auditoría de rendimiento**:
    a. Es como un chequeo de rendimiento para evaluar la eficiencia y eficacia de los sistemas.
    b. Analiza el rendimiento de los sistemas, como la velocidad de procesamiento, la capacidad de almacenamiento y la disponibilidad de los servicios.
    c. Busca cuellos de botella y áreas de mejora para optimizar el rendimiento de los sistemas.
4. **Auditoría de gestión de proyectos**:
    a. Es como un chequeo del estado del proyecto.
    b. Revisa la metodología usada, los tiempos de ejecución, y los costes.
    c. Su meta es encontrar posibles fallos en la gestión de proyectos informáticos.
5. **Auditoría de sistemas (o auditoría técnica)**:
    a. Se centra en la evaluación de los componentes técnicos de los sistemas de información.
    b. Incluye la revisión de la configuración de hardware y software, la gestión de bases de datos y la seguridad de las redes.
    c. Se asegura de que la infraestructura técnica esté funcionando correctamente y de forma segura.

Relación entre los tipos de auditoría:

- Aunque cada tipo de auditoría se centra en un aspecto específico, todos están interrelacionados.
- Por ejemplo, una auditoría de seguridad puede revelar problemas de cumplimiento o de rendimiento.
- Una auditoría de cumplimiento puede requerir la implementación de controles de seguridad adicionales.
- En resumen, todos los tipos de auditoría trabajan juntos para garantizar la salud y el buen funcionamiento de los sistemas de información de una organización.

Ejemplos prácticos:

- Una empresa de comercio electrónico realiza una auditoría de seguridad para proteger la información de sus clientes.
- Un hospital realiza una auditoría de cumplimiento para asegurarse de que está protegiendo adecuadamente los datos médicos de sus pacientes.

- Un banco realiza auditorías de rendimiento regularmente para asegurar la disponibilidad de sus servicios online.

Criterios a seguir para la composición del equipo auditor.

Imagina que el equipo auditor es como un equipo de superhéroes, cada uno con habilidades y conocimientos únicos que se complementan para lograr el objetivo común: evaluar la seguridad y el funcionamiento de los sistemas de información.

¿Qué es un equipo auditor?

Es un grupo de profesionales con experiencia y conocimientos en diferentes áreas de la auditoría informática, que se encargan de realizar la evaluación de los sistemas de información de una organización.

Criterios clave para la composición del equipo auditor:

1. **Conocimientos y habilidades**:
    a. El equipo debe contar con profesionales con conocimientos en diferentes áreas de la auditoría informática, como seguridad, cumplimiento, rendimiento y gestión de proyectos.
    b. Es importante que los miembros del equipo tengan experiencia en las tecnologías y sistemas que se van a auditar.
    c. Las habilidades de comunicación y trabajo en equipo son fundamentales para el éxito de la auditoría.
2. **Independencia y objetividad**:
    a. El equipo auditor debe ser independiente de las áreas que se van a auditar para garantizar la objetividad de la evaluación.
    b. Es importante evitar conflictos de interés y situaciones que puedan comprometer la imparcialidad del equipo.
3. **Tamaño del equipo**:
    a. El tamaño del equipo debe ser adecuado al alcance y complejidad de la auditoría.
    b. En auditorías grandes y complejas, se requerirá un equipo más numeroso y con mayor diversidad de habilidades.
4. **Liderazgo**:
    a. Es fundamental contar con un líder de equipo con experiencia en la gestión de auditorías y con habilidades de liderazgo.

b. El líder del equipo será el responsable de coordinar las actividades de la auditoría, asignar tareas y asegurar la calidad del trabajo.

5. **Especialización**:
    a. Dependiendo del tipo de auditoría, se requerirá la participación de especialistas en áreas específicas, como seguridad de redes, bases de datos o sistemas operativos.
    b. Por ejemplo, si se va a realizar una auditoría de seguridad, se necesitará un especialista en pruebas de penetración y análisis de vulnerabilidades.
6. **Formación continua**:
    a. Los miembros del equipo deben mantener sus conocimientos actualizados y estar al día con las últimas tendencias en seguridad informática y auditoría.
    b. La formación continua es esencial para garantizar la calidad y eficacia de las auditorías.

Roles dentro del equipo auditor:

- **Líder de equipo**: Responsable de la planificación, ejecución y seguimiento de la auditoría.
- **Auditores**: Realizan las pruebas y evaluaciones necesarias para cumplir con los objetivos de la auditoría.
- **Especialistas**: Aportan conocimientos técnicos especializados en áreas específicas.

Ejemplos prácticos:

- Para una auditoría de seguridad en una empresa de comercio electrónico, el equipo auditor podría incluir un experto en seguridad de aplicaciones web, un especialista en seguridad de redes y un auditor de cumplimiento de la normativa PCI DSS.
- En una auditoría de rendimiento de un centro de datos, el equipo podría incluir un especialista en sistemas operativos, un experto en bases de datos y un analista de rendimiento de redes.

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

En una auditoría informática, necesitamos diferentes tipos de pruebas para evaluar la salud y el funcionamiento de los sistemas de información. Podemos dividirlas en dos categorías principales: pruebas sustantivas y pruebas de cumplimiento.

1. Pruebas de cumplimiento:

- **¿Qué son?**
    - Son como un control de calidad para verificar que los sistemas de información cumplen con las normas, políticas y procedimientos establecidos.
    - Se centran en evaluar la eficacia de los controles internos, es decir, las medidas que la organización ha implementado para proteger sus activos y garantizar la integridad de la información.
- **¿Qué buscan?**
    - Asegurar que los controles internos están diseñados e implementados correctamente.
    - Verificar que los controles internos están funcionando de manera efectiva y consistente.
    - Identificar posibles debilidades en los controles internos que podrían ser aprovechadas por atacantes o causar errores.
- **Ejemplos:**
    - Verificar que los usuarios tienen los permisos de acceso adecuados a los sistemas.
    - Revisar los registros de auditoría para detectar actividades sospechosas.
    - Comprobar que se realizan copias de seguridad de la información de forma regular.
    - Verificar que los sistemas cumplen con la normativa vigente, como el RGPD.

2. Pruebas sustantivas:

- **¿Qué son?**
    - Son como un examen médico detallado para detectar errores o irregularidades en los datos y transacciones.
    - Se centran en evaluar la validez y exactitud de la información procesada por los sistemas de información.
- **¿Qué buscan?**
    - Detectar errores o fraudes en los datos y transacciones.
    - Evaluar la integridad y fiabilidad de la información financiera y operativa.
    - Obtener evidencia de que los sistemas de información están generando información precisa y confiable.

- **Ejemplos:**
  - Verificar la exactitud de los saldos de las cuentas bancarias.
  - Revisar las transacciones de venta para detectar posibles fraudes.
  - Analizar los registros de acceso a los sistemas para identificar posibles intrusiones.
  - Comprobar la integridad de las bases de datos.

Diferencias clave:

- Las pruebas de cumplimiento se centran en los controles internos, mientras que las pruebas sustantivas se centran en los datos y transacciones.
- Las pruebas de cumplimiento buscan asegurar que los controles están funcionando correctamente, mientras que las pruebas sustantivas buscan detectar errores o irregularidades en la información.

Relación entre las pruebas:

- Ambos tipos de pruebas son importantes para obtener una visión completa de la salud y el funcionamiento de los sistemas de información.
- Las pruebas de cumplimiento proporcionan evidencia de que los controles internos son adecuados, mientras que las pruebas sustantivas proporcionan evidencia de que la información generada por los sistemas es precisa y confiable.
- En muchos casos una prueba de cumplimiento fallida, lleva a la realización de pruebas sustantivas, para comprobar si ese fallo de cumplimiento ha tenido consecuencias reales.

Tipos de muestreo a aplicar durante el proceso de auditoría.

En una auditoría informática, a menudo es imposible revisar todos los datos y transacciones. El muestreo nos permite seleccionar una parte representativa de la población para evaluar la totalidad.

¿Qué es el muestreo en auditoría?

Es el proceso de seleccionar una muestra de elementos de una población para obtener evidencia que permita al auditor formarse una opinión sobre la totalidad de la población.

Tipos principales de muestreo:

1. **Muestreo aleatorio**:

   a. Es como sacar números de un sombrero. Cada elemento de la población tiene la misma probabilidad de ser seleccionado.
   b. Garantiza que la muestra sea representativa de la población.
   c. Se utiliza cuando la población es homogénea y no se conocen patrones o tendencias.

2. **Muestreo estratificado**:
   a. Es como dividir la sopa en diferentes ollas y probar un poco de cada una.
   b. La población se divide en subgrupos o estratos con características similares.
   c. Se selecciona una muestra aleatoria de cada estrato.
   d. Se utiliza cuando la población es heterogénea y se quieren asegurar que todos los subgrupos estén representados en la muestra.

3. **Muestreo sistemático**:
   a. Es como probar cada décima cucharada de la sopa.
   b. Se selecciona un elemento inicial al azar y luego se seleccionan elementos a intervalos regulares.
   c. Es fácil de aplicar y puede ser efectivo si la población está ordenada aleatoriamente.
   d. Se debe tener cuidado de no seleccionar elementos que sigan un patrón cíclico.

4. **Muestreo por unidades monetarias (MUM)**:
   a. Se centra en los elementos de mayor valor monetario.
   b. Cada unidad monetaria tiene la misma probabilidad de ser seleccionada.
   c. Se utiliza cuando se quieren detectar errores o fraudes en transacciones de alto valor.

5. **Muestreo de descubrimiento**:
   a. Es como buscar una aguja en un pajar.
   b. Se utiliza cuando se quiere detectar un tipo específico de error o fraude.
   c. Se selecciona una muestra lo suficientemente grande para tener una alta probabilidad de encontrar el error o fraude si existe.

6. **Muestreo no estadístico (o de juicio)**:

a. El auditor selecciona la muestra basándose en su juicio y experiencia.

b. Se utiliza cuando no es posible o práctico utilizar métodos de muestreo estadístico.

c. Es importante que el auditor documente claramente los criterios utilizados para seleccionar la muestra.

Factores a considerar al elegir el tipo de muestreo:

- **Objetivo de la auditoría**: ¿Qué se quiere lograr con la auditoría?
- **Tamaño de la población**: ¿Cuántos elementos hay en la población?
- **Heterogeneidad de la población**: ¿La población es homogénea o heterogénea?
- **Riesgo de auditoría**: ¿Cuál es el riesgo de que la muestra no sea representativa?
- **Recursos disponibles**: ¿Cuánto tiempo y dinero se tiene disponible para la auditoría?

Utilización de herramientas tipo CAAT (Computer Assisted Audit Tools)

Imagina que tienes que revisar millones de registros de transacciones para detectar posibles errores o fraudes. Sería una tarea interminable y tediosa. ¡Ahí es donde entran las herramientas CAAT!

¿Qué son las herramientas CAAT?

Son programas informáticos que ayudan a los auditores a realizar tareas de auditoría de forma más eficiente y efectiva. Permiten automatizar tareas repetitivas, analizar grandes volúmenes de datos y obtener información valiosa de forma rápida y precisa.

¿Para qué se utilizan?

- **Análisis de datos**:
  - Permiten analizar grandes volúmenes de datos para identificar patrones, tendencias y anomalías.
  - Ayudan a detectar posibles errores, fraudes o irregularidades en los datos.
- **Pruebas de cumplimiento**:
  - Permiten verificar que los sistemas de información cumplen con las normas, políticas y procedimientos establecidos.
  - Ayudan a automatizar la revisión de los controles internos.
- **Muestreo**:

- Permiten seleccionar muestras representativas de la población para realizar pruebas de auditoría.
- Ayudan a garantizar que la muestra sea aleatoria y objetiva.

- **Detección de fraudes**:
  - Permiten identificar patrones de comportamiento sospechosos que podrían indicar fraude.
  - Ayudan a analizar transacciones y registros para detectar posibles irregularidades.
- **Evaluación de riesgos**:
  - Ayudan a evaluar los riesgos asociados a los sistemas de información.
  - Facilitan la identificación de áreas de alto riesgo que requieren una mayor atención.

Tipos de herramientas CAAT:

- **Software de auditoría generalizado (GAS)**:
  - Son herramientas de propósito general que permiten realizar una amplia gama de tareas de auditoría, como análisis de datos, muestreo y pruebas de cumplimiento.
  - Ejemplos: ACL Analytics, IDEA.
- **Herramientas de extracción y análisis de datos (ETL)**:
  - Permiten extraer datos de diferentes fuentes, transformarlos y cargarlos en una base de datos para su análisis.
  - Ayudan a integrar datos de diferentes sistemas para obtener una visión completa de la información.
- **Herramientas de visualización de datos**:
  - Permiten presentar los datos de forma gráfica y visual para facilitar su comprensión.
  - Ayudan a identificar patrones y tendencias que podrían no ser evidentes en los datos brutos.
- **Herramientas de pruebas de penetración**:
  - Permiten simular ataques informáticos para evaluar la seguridad de los sistemas de información.

- Ayudan a identificar vulnerabilidades y debilidades en los sistemas.

Beneficios de utilizar herramientas CAAT:

- **Mayor eficiencia**: Permiten automatizar tareas repetitivas y analizar grandes volúmenes de datos de forma rápida.
- **Mayor eficacia**: Ayudan a detectar errores, fraudes y riesgos que podrían pasar desapercibidos con métodos manuales.
- **Mayor objetividad**: Ayudan a garantizar que las pruebas de auditoría sean objetivas y basadas en datos.
- **Mayor cobertura**: Permiten analizar una mayor cantidad de datos y transacciones, lo que aumenta la cobertura de la auditoría.

Explicación de los requerimientos que deben cumplir los hallazgos de auditoría.

Los hallazgos de auditoría son el corazón del informe de auditoría. Son las pruebas que respaldan las conclusiones y recomendaciones del auditor. Para que sean útiles y creíbles, deben cumplir con ciertos requisitos.

¿Qué son los hallazgos de auditoría?

Son las observaciones y conclusiones del auditor sobre las debilidades, riesgos o incumplimientos detectados durante la auditoría.

Requisitos clave para los hallazgos de auditoría:

1. **Evidencia suficiente y apropiada**:
    a. Cada hallazgo debe estar respaldado por evidencia sólida y verificable.
    b. La evidencia puede ser documental, testimonial, física o analítica.
    c. La evidencia debe ser suficiente para respaldar las conclusiones del auditor y apropiada para el tipo de hallazgo.
2. **Claridad y concisión**:
    a. Los hallazgos deben ser redactados de forma clara, concisa y fácil de entender.
    b. Deben evitarse los tecnicismos innecesarios y el lenguaje ambiguo.
    c. El lector debe poder comprender fácilmente la naturaleza del hallazgo y sus implicaciones.
3. **Objetividad e imparcialidad**:

a. Los hallazgos deben ser objetivos y basados en hechos, no en opiniones o juicios personales.

b. El auditor debe evitar cualquier sesgo o prejuicio que pueda influir en sus conclusiones.

c. Se debe presentar tanto la evidencia positiva como la negativa.

4. **Relevancia y materialidad**:

    a. Los hallazgos deben ser relevantes para los objetivos de la auditoría y materiales para la organización.

    b. Deben centrarse en las debilidades y riesgos que tienen un impacto significativo en la organización.

    c. Se deben evitar los hallazgos triviales o irrelevantes.

5. **Oportunidad**:

    a. Los hallazgos deben ser comunicados a la dirección de la organización de forma oportuna.

    b. La comunicación oportuna permite a la dirección tomar medidas correctivas de forma rápida y eficaz.

    c. Los hallazgos deben ser comunicados tan pronto como sea posible después de su detección.

6. **Atributos de un hallazgo**:

    a. **Condición**: Que es lo que se encontro.

    b. **Criterio**: Contra que se comparo.

    c. **Causa**: Por que ocurrio.

    d. **Efecto**: Cuales fueron las consecuencias.

    e. **Recomendación**: Que se puede hacer para corregirlo.

Ejemplos prácticos:

- **Hallazgo**: "Se detectó que el 30% de los usuarios no tienen contraseñas seguras."
    - **Evidencia**: Análisis de las contraseñas de los usuarios.
    - **Condición**: Contraseñas no seguras.
    - **Criterio**: Política de contraseñas de la organización.
    - **Causa**: Falta de concienciación y formación de los usuarios.

- **Efecto**: Mayor riesgo de acceso no autorizado a los sistemas.
- **Recomendación**: Implementar una política de contraseñas más estricta y realizar campañas de concienciación.

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

Durante una auditoría, el auditor identifica diversas situaciones que requieren atención. Para clasificarlas correctamente, es fundamental distinguir entre observaciones y no conformidades.

¿Qué son las observaciones?

- Son áreas de mejora o recomendaciones que el auditor identifica durante la auditoría.
- Indican posibles debilidades o riesgos que podrían afectar a la organización en el futuro.
- No implican necesariamente un incumplimiento de normas o políticas.
- Es como una advertencia: "Esto podría causar problemas en el futuro, sería bueno revisarlo".

¿Qué son las no conformidades?

- Son incumplimientos de normas, políticas o procedimientos establecidos.
- Indican que la organización no está cumpliendo con los requisitos aplicables.
- Pueden tener un impacto negativo significativo en la organización.
- Es como una multa: "Esto incumple las normas, y tiene consecuencias".

Criterios para la categorización:

1. **Impacto**:
    a. **Observación**: Impacto potencial leve o moderado.
    b. **No conformidad**: Impacto real o potencial significativo.
2. **Cumplimiento**:
    a. **Observación**: No hay incumplimiento directo de normas o políticas.
    b. **No conformidad**: Incumplimiento claro y verificable de normas o políticas.
3. **Riesgo**:
    a. **Observación**: Riesgo potencial o bajo.

    b. **No conformidad**: Riesgo real o alto.

4. **Frecuencia**:
    a. **Observación**: Situación aislada o esporádica.
    b. **No conformidad**: Situación recurrente o sistemática.
5. **Evidencia**:
    a. **Observación**: Evidencia limitada o indicativa.
    b. **No conformidad**: Evidencia sólida y verificable.

Ejemplos prácticos:

- **Observación**: "Se detectó que algunos usuarios utilizan contraseñas débiles."
    - No incumple directamente la política, pero aumenta el riesgo.
- **No conformidad**: "Se detectó que el sistema de copias de seguridad no se está ejecutando correctamente."
    - Incumple la política de copias de seguridad y pone en riesgo la información.

Importancia de la categorización:

- Permite a la dirección priorizar las acciones correctivas.
- Ayuda a enfocar los recursos en las áreas de mayor riesgo.
- Facilita el seguimiento y la evaluación de las acciones correctivas.

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

En el mundo de la auditoría de sistemas de información, existen diversas normativas y metodologías que establecen los estándares y las mejores prácticas para realizar auditorías de forma rigurosa y profesional.

¿Por qué son importantes las normativas y metodologías?

- **Establecen un marco de referencia**: Proporcionan un conjunto de reglas y directrices que los auditores deben seguir.
- **Garantizan la calidad**: Aseguran que las auditorías se realicen de forma consistente y objetiva.
- **Facilitan la comparación**: Permiten comparar los resultados de diferentes auditorías.

- **Generan confianza**: Aumentan la confianza de los clientes y la sociedad en general en el trabajo de los auditores.

Normativas y metodologías clave:

1. **COBIT (Control Objectives for Information and Related Technology)**:
    a. Es un marco de referencia para la gobernanza y gestión de TI.
    b. Proporciona un conjunto de objetivos de control y métricas para evaluar la eficacia de los procesos de TI.
    c. Ayuda a alinear los objetivos de TI con los objetivos de negocio.
2. **ISO 27001**:
    a. Es una norma internacional para la gestión de la seguridad de la información.
    b. Establece los requisitos para implementar un sistema de gestión de seguridad de la información1 (SGSI).
    c. Ayuda a las organizaciones a proteger su información confidencial.
3. **ISO 27002**:
    a. Es una norma internacional que proporciona directrices para la implementación de controles de seguridad de la información.
    b. Complementa a la ISO 27001 y ofrece recomendaciones prácticas para proteger los activos de información.
4. **NIST (National Institute of Standards and Technology)**:
    a. Es una agencia del gobierno de EE. UU. que desarrolla estándares y guías para la seguridad de la información.
    b. El marco de ciberseguridad del NIST es ampliamente utilizado por organizaciones de todo el mundo.
5. **ITIL (Information Technology Infrastructure Library)**:
    a. Es un conjunto de buenas prácticas para la gestión de servicios de2 TI.
    b. Proporciona directrices para la planificación, entrega y soporte de servicios de TI.
    c. Ayuda a las organizaciones a mejorar la eficiencia y eficacia de sus servicios de TI.
6. **ISACA (Information Systems Audit and Control Association)**:

    a. Es una asociación profesional que desarrolla estándares y certificaciones para auditores de sistemas de información.
    b. Sus normas y guías son ampliamente reconocidas en la industria.

7. **PCI DSS (Payment Card Industry Data Security Standard)**:
    a. Es una norma de seguridad para organizaciones que procesan pagos con tarjeta de crédito.
    b. Establece los requisitos para proteger la información de los titulares de tarjetas.
8. **RGPD (Reglamento General de Protección de Datos)**:
    a. Es una normativa europea que regula la protección de datos personales.
    b. Establece los requisitos para la recopilación, almacenamiento y procesamiento de datos personales.

Relación entre las normativas y metodologías:

- Aunque cada normativa y metodología tiene un enfoque específico, todas están interrelacionadas.
- Por ejemplo, COBIT puede utilizarse para evaluar el cumplimiento de la ISO 27001.
- ITIL puede utilizarse para mejorar la gestión de servicios de TI y, por lo tanto, la seguridad de la información.

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

Principios generales de protección de datos de carácter personal.

Imagina que los datos personales son como la información privada de una persona, y la protección de datos es como un escudo que los protege de usos indebidos. Los principios de protección de datos son las reglas que rigen cómo se debe utilizar ese escudo.

¿Qué son los datos personales?

Cualquier información que identifique o pueda identificar a una persona física, como su nombre, dirección, número de teléfono, correo electrónico, etc.

¿Cuáles son los principios generales?

El Reglamento General de Protección de Datos (RGPD) establece los siguientes principios:

1. **Licitud, lealtad y transparencia**:
    a. Los datos deben ser tratados de forma legal, justa y transparente.
    b. Los interesados deben estar informados sobre cómo se utilizan sus datos.
    c. Es como jugar limpio: no se pueden usar los datos de forma engañosa o sin permiso.
2. **Limitación de la finalidad**:
    a. Los datos deben ser recogidos con fines específicos, explícitos y legítimos.
    b. No se pueden utilizar para fines incompatibles con los iniciales.
    c. Es como tener un propósito claro: no se pueden usar los datos para algo diferente a lo que se dijo.
3. **Minimización de datos**:
    a. Solo se deben recoger los datos necesarios para los fines del tratamiento.
    b. Se deben evitar los datos excesivos o innecesarios.
    c. Es como ser eficiente: solo se pide la información que realmente se necesita.
4. **Exactitud**:
    a. Los datos deben ser exactos y estar actualizados.
    b. Se deben tomar medidas para rectificar los datos inexactos.
    c. Es como mantener la información correcta: no se pueden usar datos erróneos o desactualizados.
5. **Limitación del plazo de conservación**:
    a. Los datos deben conservarse durante el tiempo necesario para los fines del tratamiento.
    b. Se deben eliminar o anonimizar los datos cuando ya no sean necesarios.
    c. Es como no acumular basura: no se pueden guardar los datos indefinidamente.
6. **Integridad y confidencialidad**:
    a. Los datos deben ser tratados de forma segura, protegiéndolos de accesos no autorizados, pérdidas o destrucciones.
    b. Se deben implementar medidas técnicas y organizativas adecuadas.

    c. Es como tener una caja fuerte: los datos deben estar protegidos de robos o daños.

7. **Responsabilidad proactiva**:
    a. El responsable del tratamiento debe ser capaz de demostrar el cumplimiento de los principios.
    b. Se deben implementar medidas para garantizar el cumplimiento.
    c. Es como ser un buen gestor: se deben tomar medidas para asegurar que se cumplen las normas.

¿Por qué son importantes estos principios?

- **Protegen los derechos de los interesados**: Garantizan que sus datos se utilizan de forma adecuada y segura.
- **Generan confianza**: Aumentan la confianza de los ciudadanos en las organizaciones que tratan sus datos.
- **Evitan sanciones**: El incumplimiento de los principios puede conllevar sanciones económicas y reputacionales.

Ejemplos prácticos:

- Una tienda online solo debe recoger los datos necesarios para procesar el pedido y enviar el producto.
- Un hospital debe proteger la información médica de sus pacientes de accesos no autorizados.
- Una empresa debe informar a sus empleados sobre cómo utiliza sus datos personales.

Actividad para los alumnos:

- Analizar casos prácticos de tratamiento de datos personales y evaluar si se cumplen los principios del RGPD.
- Debatir sobre la importancia de la transparencia y la responsabilidad proactiva en la protección de datos.
- Investigar sobre las sanciones que se pueden imponer por incumplimiento del RGPD.

Normativa europea recogida en la directiva 95/46/CE.

La Directiva 95/46/CE, adoptada en 1995, fue la primera normativa europea integral sobre protección de datos personales. Sentó las bases para la legislación posterior, incluido el RGPD.

Objetivos principales:

- **Armonizar la protección de datos**: Establecer un nivel mínimo de protección de datos en todos los Estados miembros de la UE.
- **Garantizar la libre circulación de datos**: Permitir el flujo de datos personales entre los Estados miembros, facilitando el comercio y la cooperación.
- **Proteger los derechos fundamentales**: Garantizar el respeto de los derechos y libertades de las personas físicas en relación con el tratamiento de sus datos personales.

Principios clave:

- **Licitud del tratamiento**: Los datos solo podían tratarse si existía una base legal, como el consentimiento del interesado o una obligación legal.
- **Calidad de los datos**: Los datos debían ser exactos, pertinentes y no excesivos en relación con la finalidad del tratamiento.
- **Transparencia**: Los interesados debían ser informados sobre el tratamiento de sus datos.
- **Seguridad**: Los responsables del tratamiento debían implementar medidas de seguridad adecuadas para proteger los datos.
- **Derechos de los interesados**: Se reconocían derechos como el acceso, la rectificación y la oposición al tratamiento.

Aspectos importantes:

- Estableció la figura de las autoridades de control nacionales, encargadas de supervisar el cumplimiento de la normativa.
- Introdujo el concepto de "datos sensibles", que requerían una protección especial.
- Reguló las transferencias internacionales de datos, exigiendo un nivel de protección adecuado en los países destinatarios.

Limitaciones y evolución:

- La Directiva 95/46/CE era una directiva, lo que significaba que los Estados miembros debían transponerla a su legislación nacional. Esto dio lugar a diferencias en la aplicación de la normativa.

- Con el avance de la tecnología y la globalización, la directiva se quedó obsoleta.
- Por estos motivos, el RGPD la derogó, con la finalidad de unificar la norma en todos los países miembros, y de actualizar la norma a los nuevos tiempos.

Importancia histórica:

- A pesar de sus limitaciones, la Directiva 95/46/CE fue un hito importante en la protección de datos en Europa.
- Sentó las bases para la legislación posterior, incluido el RGPD.
- Contribuyó a concienciar sobre la importancia de la protección de datos.

Actividad para los alumnos:

- Comparar los principios de la Directiva 95/46/CE con los del RGPD.
- Investigar cómo se transpuso la Directiva 95/46/CE en España.
- Debatir sobre la evolución de la protección de datos en Europa

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 (RD 1720/2007)

Normativa nacional

España ha tenido una trayectoria normativa en protección de datos, evolucionando para adaptarse a los cambios tecnológicos y a las exigencias europeas.

1. Código Penal:

- El Código Penal español incluye delitos relacionados con la protección de datos, como el acceso no autorizado a datos personales, la revelación de secretos y la alteración de datos.
- Estos delitos buscan proteger la confidencialidad y la integridad de los datos personales, estableciendo sanciones para quienes los vulneren.

2. Ley Orgánica para el Tratamiento Automatizado de Datos (LORTAD) (1992):

- Fue la primera ley española específica sobre protección de datos.
- Regulaba el tratamiento automatizado de datos personales, estableciendo principios como el consentimiento informado, la calidad de los datos y los derechos de acceso, rectificación y cancelación.

- Fue un paso importante hacia la protección de datos en España, pero quedó obsoleta con el avance de la tecnología.

3. Ley Orgánica de Protección de Datos (LOPD) (1999):

- Adaptó la legislación española a la Directiva 95/46/CE europea.
- Amplió la protección de datos a todo tipo de tratamiento, no solo al automatizado.
- Estableció la Agencia Española de Protección de Datos (AEPD) como autoridad de control.
- Desarrolló los derechos de los interesados y las obligaciones de los responsables del tratamiento.
- En la actualidad esta ley se ha visto modificada por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

4. Reglamento1 de Desarrollo de la Ley Orgánica de Protección de Datos (RD 1720/2007):

- Desarrolló y concretó las disposiciones de la LOPD.
- Estableció medidas de seguridad para proteger los datos personales, clasificándolas en tres niveles (básico, medio y alto).
- Reguló los ficheros de datos personales y los procedimientos para ejercer los derechos de los interesados.
- Este reglamento ha quedado derogado en gran medida, por la aplicación directa del RGPD, y por la ya citada Ley Orgánica 3/2018.

5. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

- Adapta el ordenamiento jurídico español al Reglamento (UE) 2016/6792 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos3 (RGPD).
- Garantiza los derechos digitales de los ciudadanos, como el derecho a la intimidad en el uso de dispositivos digitales y el derecho a la desconexión laboral.

Transición al RGPD:

- Con la entrada en vigor del RGPD en 2018, la normativa española ha debido adaptarse a la legislación europea.
- La LOPD ha sido modificada para complementar y especificar aspectos del RGPD.
- La Ley Orgánica 3/2018 es la que adapta la normativa española al RGPD.

Importancia:

- Esta evolución normativa refleja el creciente reconocimiento de la importancia de la protección de datos en la sociedad digital.
- Es fundamental conocer la legislación vigente para garantizar el cumplimiento de las obligaciones en materia de protección de datos.

Identificación y registro de los ficheros con datos de carácter personal utilizados por la organización.

En el contexto de la protección de datos, un "fichero" se refiere a cualquier conjunto estructurado de datos personales, accesible conforme a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

¿Por qué es importante la identificación y registro?

- **Cumplimiento normativo**: El RGPD y la Ley Orgánica 3/2018 exigen que las organizaciones lleven un registro de sus actividades de tratamiento, que incluye la identificación de los ficheros.
- **Transparencia**: Permite a los interesados conocer qué datos se tratan, con qué finalidad y quién es el responsable.
- **Gestión de riesgos**: Facilita la identificación de riesgos para la protección de datos y la implementación de medidas de seguridad adecuadas.
- **Rendición de cuentas**: Demuestra el compromiso de la organización con la protección de datos.

Pasos para la identificación y registro:

1. **Inventario de datos**:
    a. Identificar todos los datos personales que la organización recoge, almacena y utiliza.
    b. Clasificar los datos por categorías (por ejemplo, datos de clientes, empleados, proveedores).
    c. Determinar la finalidad de cada tratamiento.
2. **Identificación de ficheros**:
    a. Agrupar los datos en ficheros, teniendo en cuenta la estructura y la finalidad del tratamiento.
    b. Asignar un nombre y una descripción a cada fichero.

    c. Especificar el tipo de soporte (electrónico, papel).

3. **Registro de actividades de tratamiento**:
    a. Documentar la información relevante de cada fichero, incluyendo:
        i. Nombre y datos de contacto del responsable del tratamiento.
        ii. Categorías de datos personales tratados.
        iii. Finalidades del tratamiento.
        iv. Destinatarios de los datos.
        v. Plazos de conservación.
        vi. Medidas de seguridad implementadas.
        vii. Transferencias internacionales de datos.
4. **Actualización del registro**:
    a. Revisar y actualizar el registro periódicamente para reflejar los cambios en los tratamientos de datos.
    b. Documentar cualquier incidencia o brecha de seguridad relacionada con los ficheros.

Herramientas y recursos:

- **Guías y plantillas de la AEPD**: La Agencia Española de Protección de Datos ofrece recursos para facilitar el cumplimiento del RGPD.
- **Software de gestión de privacidad**: Existen herramientas que automatizan el registro de actividades de tratamiento y la gestión de ficheros.
- **Consultores especializados**: Profesionales que pueden asesorar a la organización en la identificación y registro de ficheros.

Consideraciones adicionales:

- **Datos sensibles**: Los ficheros que contienen datos sensibles (por ejemplo, datos de salud, religión, orientación sexual) requieren medidas de seguridad adicionales.
- **Evaluación de impacto**: En algunos casos, puede ser necesario realizar una evaluación de impacto de protección de datos (EIPD) antes de iniciar un nuevo tratamiento.

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

El Real Decreto 1720/2007, que desarrollaba la antigua LOPD, establecía tres niveles de seguridad para los ficheros con datos personales: básico, medio y alto. Cada nivel requería la implementación de medidas de seguridad específicas, proporcionales al riesgo que suponía el tratamiento de los datos.

Niveles de seguridad:

1. **Nivel básico**:
    a. Aplicable a ficheros con datos personales generales, como nombres, direcciones o números de teléfono.
    b. Medidas de seguridad:
        i. Documento de seguridad que describa las medidas implementadas.
        ii. Control de acceso a los locales donde se encuentran los ficheros.
        iii. Registro de incidencias.
        iv. Copias de seguridad periódicas.
2. **Nivel medio**:
    a. Aplicable a ficheros con datos personales relativos a infracciones administrativas o penales, solvencia patrimonial o servicios financieros.
    b. Medidas de seguridad:
        i. Todas las del nivel básico, más:
        ii. Control de acceso a los datos mediante identificadores y contraseñas.
        iii. Registro de accesos a los datos.
        iv. Auditorías periódicas.
3. **Nivel alto**:
    a. Aplicable a ficheros con datos especialmente protegidos, como datos de salud, ideología, afiliación sindical, religión, creencias, origen racial o vida sexual.
    b. Medidas de seguridad:
        i. Todas las de los niveles básico y medio, más:
        ii. Cifrado de los datos.
        iii. Control de acceso físico y lógico reforzado.

iv. Registro de todas las operaciones realizadas con los datos.

v. Auditorías periódicas más frecuentes.

Medidas de seguridad específicas:

- **Documento de seguridad**: Un documento que recoge las políticas, normas y procedimientos de seguridad adoptados por la organización.
- **Control de acceso**: Medidas para limitar el acceso a los datos personales solo a las personas autorizadas.
- **Registro de incidencias**: Un registro de cualquier evento que pueda afectar a la seguridad de los datos.
- **Copias de seguridad**: Copias de los datos para garantizar su recuperación en caso de pérdida o daño.
- **Auditorías**: Revisiones periódicas para verificar el cumplimiento de las medidas de seguridad.

Importancia:

- El Real Decreto 1720/2007 estableció un marco de referencia para la seguridad de los datos personales en España.
- Sus medidas de seguridad, aunque en parte superadas por el RGPD, siguen siendo relevantes para garantizar la protección de los datos.

Guía para la realización de la auditoría bienal obligatoria de ley orgánica 15-1999 de protección de datos de carácter personal

Es crucial aclarar que la Ley Orgánica 15/1999 ha sido derogada y reemplazada por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018. Por lo tanto, la auditoría bienal obligatoria ya no se rige por la LOPD, sino por el RGPD y la LOPDGDD.

A pesar de esto, vamos a crear una guía que se base en los principios y requisitos del RGPD y la LOPDGDD, para que sea útil en el contexto actual.

Aunque la auditoría bienal obligatoria como tal ya no existe, es recomendable realizar auditorías periódicas para garantizar el cumplimiento del RGPD y la LOPDGDD.

Objetivos de la auditoría:

- Evaluar el cumplimiento del RGPD y la LOPDGDD.
- Identificar riesgos y debilidades en el tratamiento de datos personales.
- Proponer medidas correctivas y preventivas.

- Demostrar la responsabilidad proactiva de la organización.

Pasos para la realización de la auditoría:

1. **Planificación**:
    a. Definir el alcance de la auditoría (qué procesos y sistemas se van a auditar).
    b. Establecer los objetivos y criterios de la auditoría.
    c. Designar al equipo auditor (interno o externo).
    d. Elaborar un plan de auditoría con el cronograma y los recursos necesarios.
2. **Recopilación de información**:
    a. Revisar la documentación relevante (políticas de privacidad, registros de actividades de tratamiento, evaluaciones de impacto, etc.).
    b. Realizar entrevistas con el personal involucrado en el tratamiento de datos.
    c. Analizar los sistemas y aplicaciones que tratan datos personales.
3. **Evaluación de cumplimiento**:
    a. Verificar el cumplimiento de los principios del RGPD (licitud, finalidad, minimización, exactitud, conservación, integridad y confidencialidad).
    b. Evaluar la eficacia de las medidas de seguridad implementadas.
    c. Comprobar el cumplimiento de los derechos de los interesados (acceso, rectificación, supresión, oposición, etc.).
    d. Revisar el cumplimiento de la LOPDGDD, especialmente en aspectos como los derechos digitales y las garantías adicionales.
4. **Identificación de hallazgos**:
    a. Documentar las observaciones y no conformidades encontradas durante la auditoría.
    b. Clasificar los hallazgos según su gravedad e impacto.
    c. Recopilar evidencia suficiente y apropiada para respaldar los hallazgos.
5. **Elaboración del informe de auditoría**:
    a. Incluir un resumen ejecutivo, el alcance y los objetivos de la auditoría, los hallazgos y las recomendaciones.
    b. Presentar los hallazgos de forma clara, concisa y objetiva.
    c. Proponer medidas correctivas y preventivas para abordar los hallazgos.

6. **Seguimiento y acciones correctivas**:
    a. Establecer un plan de acción para implementar las recomendaciones del informe.
    b. Asignar responsabilidades y plazos para la implementación de las acciones correctivas.
    c. Realizar un seguimiento periódico para verificar la eficacia de las acciones correctivas.

Aspectos clave a auditar:

- **Registro de actividades de tratamiento**: Verificar que esté completo y actualizado.
- **Evaluaciones de impacto de protección de datos (EIPD)**: Comprobar que se han realizado cuando es necesario.
- **Medidas de seguridad**: Evaluar su eficacia y adecuación a los riesgos.
- **Gestión de brechas de seguridad**: Revisar los procedimientos y registros.
- **Cumplimiento de los derechos de los interesados**: Verificar la eficacia de los procedimientos para atender las solicitudes.
- **Transferencias internacionales de datos**: Comprobar que se realizan con garantías adecuadas.
- **Delegado de protección de datos (DPD)**: Verificar su designación y funciones.