Gestión de la seguridad y normativas

La gestión de la seguridad y el cumplimiento de normativas son pilares fundamentales para proteger los activos de información en cualquier organización. En esta sección, exploraremos las principales normas y estándares como la ISO/IEC 27002 y la metodología ITIL, así como leyes relevantes como la LOPDGDD. Comprenderemos cómo estas directrices y regulaciones establecen las bases para garantizar la confidencialidad, integridad y disponibilidad de la información, y cómo implementarlas eficazmente en el entorno empresarial.

1. Norma ISO/IEC 27002:2022 Código de buenas prácticas para la gestión de la seguridad de la información.

La norma ISO/IEC 27002:2022 es un estándar internacional desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC). Este estándar ofrece un conjunto de controles de referencia para la seguridad de la información, ciberseguridad y protección de la privacidad, incluyendo una guía de implementación basada en las mejores prácticas reconocidas a nivel mundial. En términos generales, proporciona orientación para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) según la norma ISO 27001.

Aunque ISO 27002 no es un estándar certificable por sí mismo, cumplir con sus directrices en seguridad de la información, seguridad física, ciberseguridad y gestión de la privacidad acerca a las organizaciones al cumplimiento de los requisitos necesarios para obtener la certificación ISO 27001.

La ISO/IEC 27002 fue revisada y actualizada el 15 de febrero de 2022 para reflejar los avances y prácticas actuales en seguridad de la información en distintos sectores empresariales y gubernamentales. Esta revisión afecta a numerosos estándares y marcos de seguridad que están relacionados o utilizan los controles de ISO 27002:2013.

La Norma ISO/IEC 27002:2022 proporciona recomendaciones para establecer, implementar y mantener controles de seguridad de la información. Esta versión actualizada refleja las necesidades cambiantes en materia de seguridad, adaptándose a las tecnologías emergentes y a las nuevas amenazas digitales.

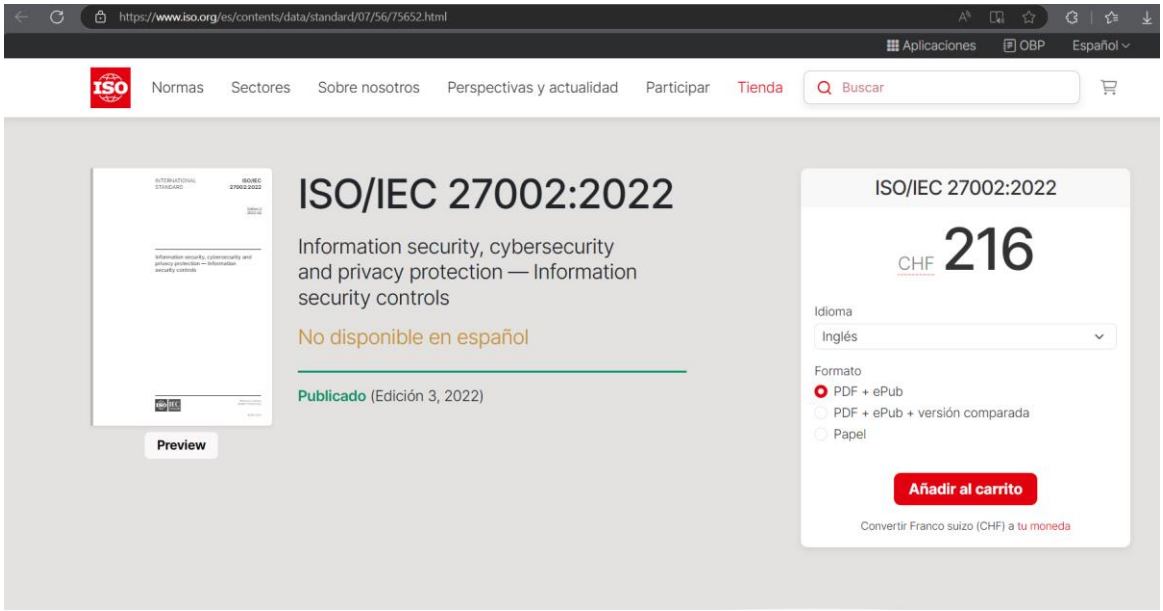
Una de las novedades más destacadas es la reorganización de los controles de seguridad. Ahora se agrupan en cuatro temas principales: Controles Organizacionales, Controles de Personas, Controles Físicos y Controles Tecnológicos. Esta estructura facilita la identificación y aplicación de medidas de seguridad específicas en cada área:

Por ejemplo, dentro de los Controles Tecnológicos, se incluye la implementación de autenticación multifactor para acceder a sistemas críticos. Esto es similar a agregar varias cerraduras a una puerta, aumentando la dificultad para que un intruso acceda sin autorización.

Además, se han incorporado nuevos controles para abordar riesgos asociados con tecnologías modernas. Se incluyen medidas para la seguridad en la nube, inteligencia artificial y trabajo remoto, reflejando la creciente dependencia de estas tecnologías en las operaciones empresariales.

Algunos controles de versiones anteriores han sido eliminados o fusionados debido a su obsolescencia o redundancia. Esto ayuda a las organizaciones a enfocarse en prácticas relevantes y efectivas, evitando invertir recursos en medidas que ya no aportan valor significativo:

La norma también enfatiza un enfoque basado en el riesgo, donde las organizaciones deben evaluar y priorizar los riesgos específicos que enfrentan. Esto es como un médico que personaliza un tratamiento según la condición específica de cada paciente, en lugar de aplicar el mismo remedio para todos.



Pie de imagen: Acceso a la ISO/IEC 27002:2022 https://www.iso.org/es/contents/data/standard/07/56/75652.html

El desafío principal para las organizaciones que inician en la gestión de la seguridad de la información es el amplio alcance que implica. La implementación y mantenimiento de un SGSI abarca un espectro tan extenso que puede ser abrumador determinar por dónde comenzar. En este contexto, adoptar los controles sugeridos en ISO/IEC 27002 es un excelente punto de partida para fortalecer la seguridad de la información de su organización.

Al aplicar los controles de seguridad de la información establecidos en ISO 27002, las organizaciones pueden obtener múltiples ventajas:

- Proporciona una base sólida para abordar cuestiones relacionadas con la seguridad de la información, ciberseguridad, seguridad física y privacidad de datos.
- Incrementa la confianza y percepción positiva de clientes y socios comerciales al demostrar el compromiso con estándares reconocidos internacionalmente.
- Al alinearse con requisitos de seguridad globales, se simplifica la colaboración con socios y clientes internacionales.
- El cumplimiento del estándar ayuda a desarrollar prácticas óptimas que pueden aumentar la eficiencia y productividad de la organización.
- Ofrece directrices claras para la implementación, gestión, mantenimiento y evaluación de sistemas de gestión de seguridad de la información.
- Las organizaciones que cumplen con ISO 27002 tienen una posición favorable en negociaciones contractuales y en la participación en oportunidades de negocio globales.
- : Posibilidad de obtener primas de seguro más bajas debido a la adopción de controles reconocidos.
- Los controles de ISO 27002 pueden mapearse con otros estándares como NIST, SOC2, CIS, TISAX®, facilitando la integración con diversos marcos de seguridad.

Actividad 1

Relaciona cada descripción con el término o concepto correspondiente-

1. Este estándar ofrece un conjunto actualizado de controles para la seguridad de la información, ciberseguridad y protección de la privacidad.
2. La nueva versión ha reorganizado los controles en cuatro temas principales para facilitar su aplicación.
3. La norma enfatiza que las organizaciones deben evaluar y priorizar los riesgos específicos que enfrentan.
4. Se han añadido controles para abordar riesgos asociados con tecnologías modernas como la nube y el trabajo remoto.
5. Aplicar los controles de esta norma incrementa la confianza de clientes y socios al demostrar compromiso con estándares internacionales.

A. Enfoque basado en el riesgo
B. Reorganización en cuatro temas principales
C. Ventajas de aplicar los controles de ISO 27002
D. Incorporación de nuevos controles para tecnologías modernas
E. ISO/IEC 27002:2022

2. Metodología ITIL 4 Biblioteca de Infraestructuras de Tecnologías de la Información.

La Metodología ITIL 4 es la última evolución del marco de mejores prácticas para la gestión de servicios de TI. Esta versión introduce conceptos modernos y flexibles que permiten a las organizaciones adaptarse rápidamente a los cambios tecnológicos y de negocio. No es una norma estricta, sino un enfoque flexible y pragmático que se adapta a las necesidades específicas de cada organización. Su objetivo es ayudar a proporcionar servicios tecnológicos que generen valor para clientes, usuarios y la empresa en general.

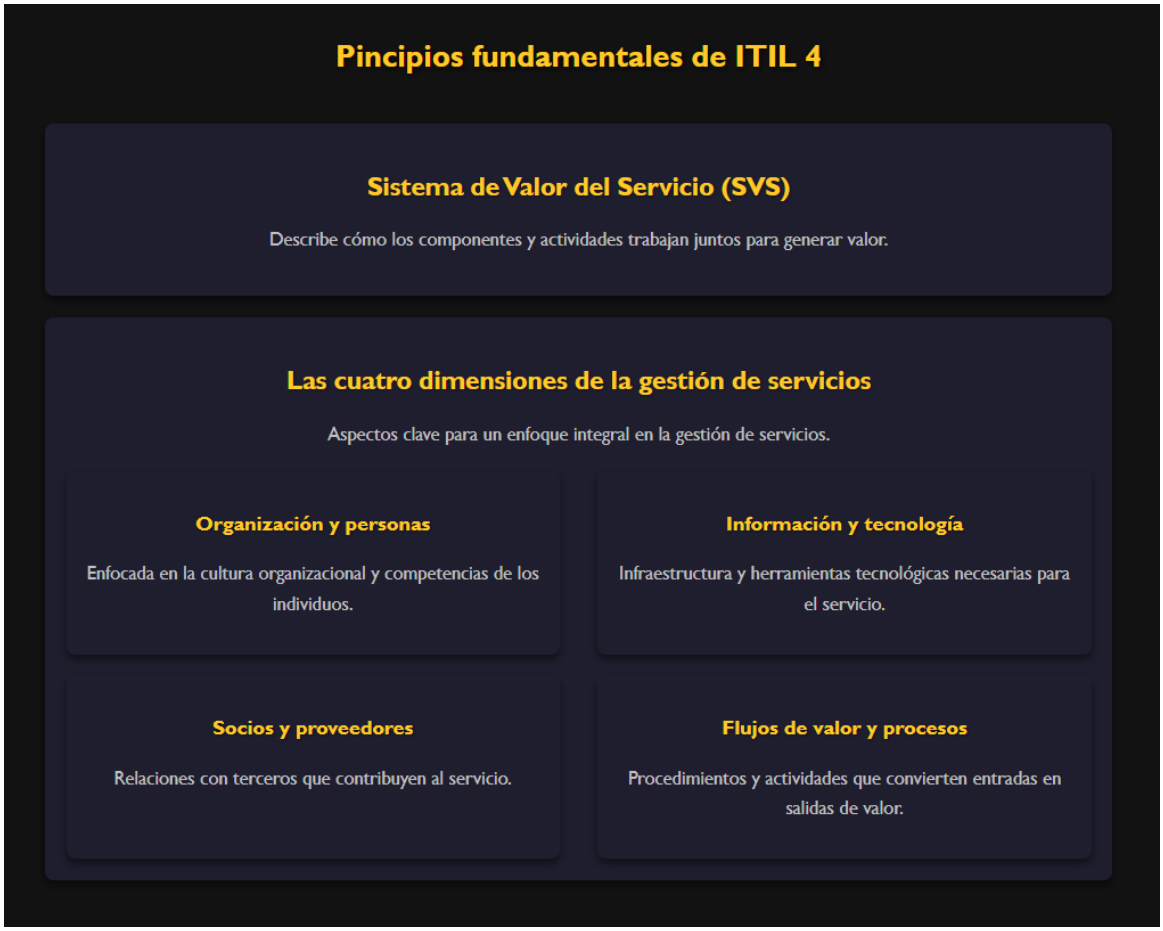
El valor aportado se percibe a través de dos conceptos fundamentales: utilidad y garantía. La utilidad se refiere a las características funcionales que satisfacen las necesidades del cliente, mientras que la garantía asegura que el servicio cumple con los niveles de calidad y disponibilidad esperados.

Para ofrecer estos servicios eficientemente, es esencial contar con recursos y competencias. Los recursos son los medios y fondos disponibles, y las competencias son las habilidades y conocimientos para utilizarlos adecuadamente. ITIL describe estas habilidades de gestión de servicios, proporcionando una guía para mejorar continuamente los procesos y prácticas dentro de una organización.

En la metodología ITIL 4, es importante comprender los diferentes roles y actores involucrados:

- Usuarios: Personas que utilizan los servicios diariamente y experimentan directamente su calidad y eficacia.
- Clientes: Representan a los usuarios ante los equipos de TI, especificando las necesidades y expectativas en términos de servicios.
- Proveedores de servicios: Equipos de TI y sus colaboradores internos o externos que desarrollan y mantienen los servicios.
- Patrocinadores: Aportan y autorizan el presupuesto necesario para construir, implementar y dar soporte a los servicios.

Estos roles interactúan dentro de un marco definido por modelos de responsabilidad, como el RACI (Responsable, Aprobador, Consultado e Informado), que asegura una clara asignación de tareas y responsabilidades.



Una de las características principales de ITIL 4 es el Sistema de Valor del Servicio (SVS), que proporciona un modelo integral para la creación, entrega y mejora continua de servicios. Este enfoque promueve la colaboración y la integración entre diferentes departamentos y procesos, similar a cómo los músicos de una orquesta trabajan juntos para interpretar una sinfonía armoniosa. La cadena de valor del servicio es el núcleo del SVS y representa el modelo operativo que transforma las oportunidades y demandas en valor. Se compone de seis actividades interconectadas:

Establecer una visión compartida y definir objetivos estratégicos.
Implementar ajustes y optimizaciones continuas en servicios y procesos.
Participación: Interactuar con partes interesadas para comprender sus necesidades y expectativas.
Crear y modificar servicios o productos de manera efectiva.
Adquirir y desarrollar los componentes necesarios para los servicios.
Proveer servicios de calidad y brindar soporte continuo a los usuarios.

ITIL 4 también introduce las Prácticas de Gestión en lugar de los procesos rígidos de versiones anteriores. Son conjuntos de recursos y actividades estructuradas para lograr un objetivo específico. ITIL 4 define 34 prácticas divididas en tres categorías:

1. Prácticas de Gestión General: Aplicables a toda la organización, como gestión de estrategia, gestión del riesgo o mejora continua.
2. Prácticas de Gestión de Servicios: Específicas para la gestión de servicios de TI, como gestión de incidentes, gestión de nivel de servicio o gestión de problemas.
3. Prácticas de Gestión Técnica: Relacionadas con aspectos tecnológicos, como gestión de despliegue, gestión e infraestructura y plataformas o desarrollo y gestión de software.

ITIL 4 establece siete principios fundamentales que orientan las decisiones y acciones dentro de una organización. El primero es “Enfocarse en el Valor”, lo que implica que todas las actividades deben aportar valor tanto al cliente como a la organización. A continuación, “Comenzar Donde se Está” sugiere aprovechar las prácticas y recursos existentes antes de introducir cambios, evitando así desperdiciar esfuerzos previos.

El principio de “Progresar Iterativamente con Retroalimentación” recomienda implementar mejoras en pequeños pasos, permitiendo aprender y ajustar continuamente. “Colaborar y Promover la Visibilidad” enfatiza la importancia de la comunicación y transparencia entre equipos y departamentos para lograr objetivos comunes. Por su parte, “Pensar y Trabajar de Forma Holística” invita a considerar el sistema completo y sus interrelaciones al tomar decisiones, asegurando una comprensión integral de las consecuencias.

El principio de “Mantenerlo Simple y Práctico” aconseja evitar complejidades innecesarias, enfocándose en lo esencial para lograr eficiencia. Por último, “Optimizar y Automatizar” busca mejorar procesos mediante la optimización y la automatización cuando sea posible, liberando recursos y aumentando la productividad.

La integración de metodologías ágiles como Agile, DevOps y Lean es otra innovación de ITIL 4. Esto permite a las organizaciones adoptar enfoques más eficientes y centrados en el valor para el cliente. Es como cambiar de un método de producción en masa a uno personalizado que satisface mejor las necesidades específicas de los usuarios.

Algunas prácticas anteriores han sido actualizadas o eliminadas para reflejar las tendencias actuales. Por ejemplo, la Gestión de Activos de Software ahora se incluye dentro de la Gestión de Activos de TI, reconociendo la convergencia de hardware y software en el entorno tecnológico moderno.

ITIL 4 reconoce que no existe un enfoque único para todos y alienta a las organizaciones a adaptar las prácticas según sus necesidades particulares. Esto evita la implementación de procesos innecesarios y fomenta la eficiencia. Es similar a un sastre que ajusta un traje a medida en lugar de vender uno de talla estándar.

Entre las prácticas esenciales de ITIL 4 se encuentra:

- La gestión de incidentes, cuyo objetivo es restaurar el servicio normal lo más pronto posible y minimizar el impacto en el negocio. Un incidente se define como cualquier interrupción no planificada o reducción en la calidad de un servicio. Algunos incidentes, debido a su gravedad, requieren procedimientos específicos de gestión de crisis;
- La mejora continua, que se enfoca en alinear diariamente los servicios y prácticas con las necesidades cambiantes, afectando a productos, servicios y todos los elementos relacionados. Esto garantiza que la organización evolucione junto con su entorno;
- La gestión de problemas, por su parte, busca identificar y resolver las causas raíz de los incidentes para prevenir su recurrencia. Mientras que la gestión de incidentes se centra en solucionar interrupciones inmediatas, la gestión de problemas aborda las razones subyacentes que las provocan, permitiendo implementar soluciones permanentes.

Para implementar ITIL de manera efectiva, es importante comprender sus objetivos y alinearlos con los de la empresa, comunicando su valor en todos los niveles de la organización. Esto asegura que todos entiendan que el propósito es agregar valor real mediante una gestión eficiente de servicios de TI.

Es necesario analizar el proceso actual para identificar áreas de mejora y reconocer qué prácticas de ITIL ya se aplican. A partir de ahí, se pueden definir procesos y responsables, asignando claramente roles y enfatizando la importancia del personal en el éxito de ITIL. La actitud y habilidades del equipo son fundamentales.

Al comenzar la implementación, no es obligatorio adoptar todos los procesos simultáneamente. Es recomendable iniciar con aquellos que aporten mayor valor inmediato, como la gestión de incidencias y la gestión del conocimiento, y avanzar gradualmente.

Por último, es esencial revisar y mejorar continuamente, aplicando la mejora continua para ajustar y optimizar los procesos a lo largo del tiempo. Esto garantiza que la organización se mantenga alineada con sus objetivos y pueda adaptarse a las necesidades cambiantes.

Anotación

La adopción de ITIL ofrece múltiples ventajas. Mejora la calidad del servicio, aumentando la consistencia y eficiencia en la entrega, lo que se traduce en una mayor satisfacción del cliente. Optimiza los costos al priorizar y utilizar eficientemente los recursos, alineándolos con las necesidades del negocio y reduciendo gastos innecesarios. Además, permite una mayor satisfacción del cliente al comprender y atender mejor sus necesidades, fortaleciendo la relación y fidelidad. Por último, facilita una mejor gestión del riesgo, permitiendo una gestión proactiva que evita incidentes graves y mantiene los riesgos bajo control, garantizando la continuidad del negocio.

3. Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).

La Ley Orgánica 3/2018, conocida como LOPDGDD, es la norma española que adapta el Reglamento General de Protección de Datos (RGPD) de la Unión Europea al ordenamiento jurídico nacional. Esta ley regula el tratamiento de datos personales e introduce garantías para los derechos digitales de los ciudadanos.

Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales.

La LOPDGDD establece obligaciones específicas para las organizaciones que manejan datos personales. Por ejemplo, exige la realización de evaluaciones de impacto cuando el tratamiento pueda implicar un alto riesgo para los derechos y libertades de las personas. Esto es similar a revisar minuciosamente un plan antes de construir un edificio para asegurar que todo sea seguro y cumpla con las regulaciones.

Uno de los aspectos prácticos más relevantes es la necesidad de obtener el consentimiento expreso de los individuos para el tratamiento de sus datos. Ya no es suficiente con casillas premarcadas o textos confusos; el consentimiento debe ser claro y específico. Imaginemos que antes bastaba con un asentimiento ambiguo para entrar a un club exclusivo, pero ahora se requiere una invitación personalizada y firmada.

La ley también refuerza el derecho al olvido, permitiendo a las personas solicitar la eliminación de sus datos cuando ya no sean necesarios para el fin con el que fueron recogidos. Esto es

especialmente importante en el contexto digital, donde la información puede difundirse rápidamente.

En cuanto a las sanciones, la LOPDGDD establece multas significativas para las organizaciones que incumplan sus disposiciones. Estas pueden alcanzar hasta 20 millones de euros o el 4% de la facturación anual global de la empresa, lo que sea mayor. Es como si una tienda enfrentara multas tan altas que podrían poner en riesgo su continuidad, incentivando así el cumplimiento de la ley.

La ley también introduce nuevas figuras, como el Delegado de Protección de Datos (DPD), que es el responsable de supervisar el cumplimiento de la normativa en la organización. Este rol es obligatorio en ciertos casos, como en entidades públicas o empresas que manejan grandes volúmenes de datos sensibles.

Además, la LOPDGDD aborda los derechos digitales en el entorno laboral. Por ejemplo, regula el uso de dispositivos digitales y la videovigilancia en el trabajo, estableciendo que los empleados deben ser informados de manera clara sobre estas prácticas. Es como si en una fábrica se colocaran letreros visibles indicando que hay cámaras de seguridad, garantizando así la transparencia.

Como ya sabemos, el tratamiento de datos de carácter personal ha cobrado una relevancia especial en los últimos años, sobre todo desde la implementación del Reglamento General de Protección de Datos (RGPD) en Europa. Este reglamento tiene como objetivo garantizar que la información personal de los ciudadanos sea gestionada de manera segura y responsable, con derechos claros para los individuos y obligaciones definidas para las organizaciones que tratan sus datos.

Los principios generales de la protección de datos se basan en el respeto a la privacidad y los derechos fundamentales de las personas, y cualquier empresa u organización que maneje datos personales debe seguirlos rigurosamente. Veamos estos principios con detalle:

Principio de licitud, lealtad y transparencia.

- Este principio implica que los datos personales deben ser tratados de manera legal, justa y transparente para el titular de estos. En otras palabras, cualquier recogida o uso de datos personales debe ser informado de manera clara y comprensible para el usuario, y debe contar con una base legal, como el consentimiento explícito del individuo.

Principio de limitación de la finalidad

- Los datos personales solo pueden recogerse con fines específicos, explícitos y legítimos, y no pueden ser tratados para otros fines distintos a los que se informaron inicialmente.

Principio de minimización de datos

- Este principio establece que solo deben recogerse los datos personales que sean estrictamente necesarios para cumplir con el propósito previsto. Es decir, no se deben recoger más datos de los que realmente se necesitan.

Principio de exactitud

- Los datos personales deben ser precisos y estar actualizados. Si los datos que maneja una organización son inexactos o están desactualizados, deben corregirse o eliminarse.

Principio de limitación del plazo de conservación

- Los datos personales solo deben conservarse durante el tiempo que sea necesario para cumplir con el propósito para el que fueron recogidos. Una vez cumplido ese plazo, deben ser eliminados o anonimizados.

Principio de integridad y confidencialidad

- Los datos personales deben tratarse de manera que se garantice su seguridad, protegiéndolos contra accesos no autorizados, pérdida o destrucción. Para cumplir con este principio, las organizaciones deben implementar medidas técnicas y organizativas adecuadas.

La legislación vigente en materia de protección de datos en España, basada en el RGPD y la LOPDGDD, establece sanciones muy estrictas para las organizaciones que no cumplan con los requisitos establecidos. Las infracciones pueden ir desde el incumplimiento de obligaciones básicas hasta la violación grave de los derechos de los interesados.

Tipos de infracciones:

- Infracciones leves: Estas infracciones suelen estar relacionadas con errores administrativos o de procedimiento que, aunque no sean graves, vulneran ciertos aspectos de la normativa. Un ejemplo sería no informar adecuadamente a los usuarios sobre la finalidad del tratamiento de sus datos.
- Infracciones graves: Incluyen casos en los que la organización no ha obtenido el consentimiento adecuado para el tratamiento de datos, o cuando no se cumplen con las obligaciones básicas de seguridad, como la implementación de medidas de protección suficientes.
- Infracciones muy graves: Son las violaciones que afectan gravemente los derechos de los interesados, como una brecha de seguridad que exponga información sensible, o el tratamiento de datos sin base legal. Estas infracciones pueden tener consecuencias serias para las empresas, tanto en términos financieros como reputacionales.

Situación	Tipo de infracción
No informar a los usuarios sobre el uso de sus datos en un formulario de contacto.	Leve
No obtener el consentimiento explícito antes de enviar publicidad a clientes por correo electrónico.	Grave
Exponer información médica sensible de los pacientes debido a una brecha de seguridad.	Muy grave
Guardar datos de empleados más allá del tiempo necesario sin justificación.	Grave
Un error administrativo al procesar una solicitud de rectificación de datos de un usuario.	Leve
Tratar datos sin base legal adecuada, como procesar datos sin consentimiento válido.	Muy grave

Pie de imagen: Ejemplos de infracciones en protección de datos.

Actividad 2

Lee las siguientes situaciones y clasifícalas como infracción leve, infracción grave o infracción muy grave:

1. Una empresa olvida incluir una cláusula informativa en el formulario de su página web, donde se explica el uso de los datos de los usuarios.

2. Una clínica médica sufre un ciberataque y expone historiales clínicos de sus pacientes.

3. Una tienda online no obtiene el consentimiento explícito de los clientes antes de enviar correos promocionales.

4. Una empresa almacena datos personales de clientes más tiempo del necesario, sin una justificación legal.

Las sanciones por incumplimiento de la normativa pueden ser muy elevadas, especialmente desde la entrada en vigor del RGPD. Las multas pueden alcanzar hasta 20 millones de euros o el 4% del volumen de negocio global anual de la empresa, lo que sea mayor. Este tipo de sanciones tiene un efecto disuasorio, ya que las empresas saben que una infracción no solo afecta económicamente, sino también a su reputación. Las sanciones del RGPD y LOPDGDD se dividen en varios niveles:

RGPD

Las multas pueden ser de hasta 10 o 20 millones de euros, o el 2-4% del volumen de negocio anual, dependiendo de la gravedad. Incluyen incumplimiento de obligaciones, consentimiento, y protección de datos.

- Multas hasta 10 millones de euros o 2% del volumen de negocio:
  - Obligaciones del responsable y encargado (Art. 8, 11, 25-39).
  - Organismos de certificación (Art. 42, 43).
  - Autoridades de control (Art. 41, 4).

- Multas hasta 20 millones de euros o 4% del volumen de negocio:
    - Principios básicos del tratamiento (Art. 5-9).
    - Derechos de los interesados (Art. 12-22).
    - Transferencias internacionales (Art. 44-49).
    - Incumplimiento de resoluciones (Art. 58).

LOPDGDD

Clasifica las infracciones en leves (hasta 40.000€), graves (hasta 300.000€), y muy graves (hasta 20 millones de euros), y castiga desde errores administrativos hasta violaciones graves como brechas de seguridad.

- Leves: Hasta 40.000€ (prescriben en 1 año).
    - Ej: No informar sobre el tratamiento de datos.
- Graves: 40.001€-300.000€ (prescriben en 2 años).
    - Ej: Obtener datos de menores sin consentimiento.
- Muy graves: 300.000€-20 millones de euros (prescriben en 3 años).
    - Ej: Transferir datos sin garantías.

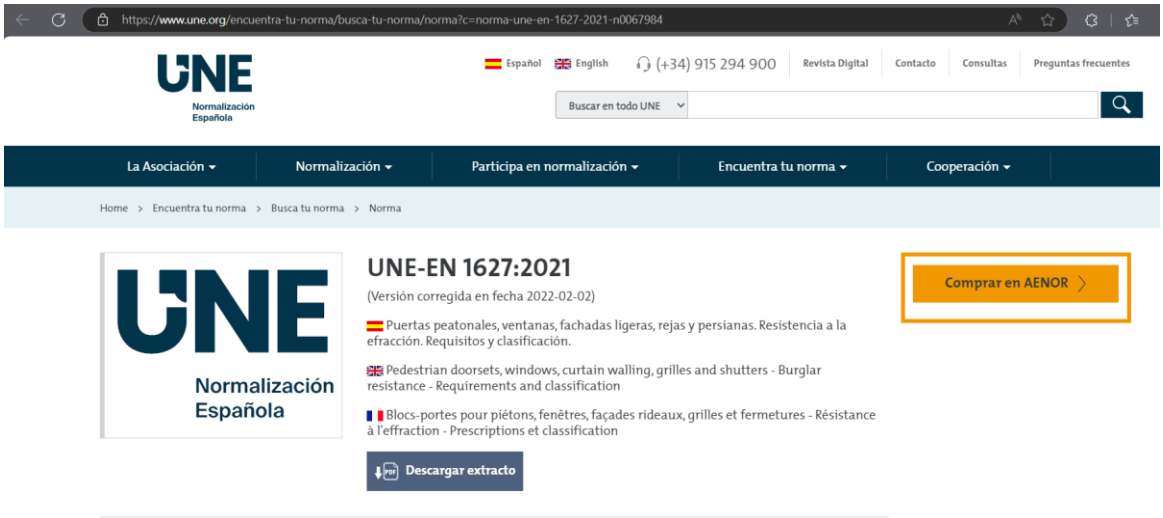
Factores para sancionar:

- Naturaleza y duración de la infracción.
- Personas afectadas.
- Daños y cooperación con la autoridad.

4. Normativas más frecuentemente utilizadas para la gestión de la seguridad física.

La gestión de la seguridad física es esencial para proteger los activos tangibles de una organización, como edificios, equipos y personas. Existen varias normativas y estándares que se utilizan comúnmente para guiar estas prácticas.

Una de las normativas más destacadas es la Norma UNE-EN 1627, que establece requisitos para la resistencia a la efracción de puertas, ventanas y otros elementos de construcción. Esta norma clasifica los productos en diferentes niveles de seguridad, similar a cómo los candados tienen clasificaciones según su resistencia:



Otra referencia importante es la Ley 5/2014 de Seguridad Privada en España, que regula los servicios y actividades de seguridad privada. Esta ley establece los requisitos para las empresas de seguridad, los vigilantes y el uso de sistemas de seguridad, asegurando que las prácticas se realicen de manera profesional y bajo estándares adecuados:

El estándar ISO 22301 sobre Sistemas de Gestión de la Continuidad del Negocio también es relevante, ya que incluye aspectos de seguridad física para garantizar que una organización pueda operar ante interrupciones. Por ejemplo, tener planes de contingencia para desastres naturales o cortes de energía es como tener un kit de emergencia en casa para situaciones inesperadas.

La Norma ISO/IEC 27001, aunque enfocada en la seguridad de la información, incluye controles relacionados con la seguridad física en su Anexo A. Estos controles abarcan desde el control de acceso a instalaciones hasta la protección contra desastres ambientales.

En el ámbito de la protección contra incendios, la Norma UNE 23007-14 es fundamental. Establece los requisitos para los sistemas de detección y alarma de incendios, asegurando una respuesta rápida ante emergencias.

La Reglamentación de Instalaciones de Protección Contra Incendios (RIPCI) es otra normativa esencial en España. Define las condiciones y requisitos que deben cumplir las instalaciones y equipos de protección contra incendios, garantizando su eficacia y mantenimiento adecuado:

En cuanto a la seguridad en infraestructuras críticas, la Ley 8/2011 y el Real Decreto 704/2011 establecen medidas para la protección de servicios esenciales, como energía, transporte y agua. Estas normativas requieren que las empresas identifiquen sus activos críticos y establezcan planes de protección específicos.

Por último, destaca la Norma UNE-EN 50132, que se centra en los sistemas de videovigilancia para uso en seguridad. Establece directrices para el diseño, instalación y mantenimiento de estos sistemas, asegurando su eficacia y cumplimiento legal.

Es relevante mencionar que algunas prácticas antiguas, como el uso de sistemas de seguridad sin protocolos de cifrado o control de acceso básico, ya no son adecuadas ante las amenazas actuales. Las organizaciones deben actualizar sus sistemas y procedimientos para incorporar tecnologías modernas, como controles biométricos o sistemas de vigilancia inteligentes.

Anotación

Las normativas de seguridad física suelen complementarse con políticas internas de la organización, que deben estar alineadas con los estándares legales y las mejores prácticas del sector. Esto garantiza una protección integral y coherente de todos los activos físicos, similar a cómo un escudo y una armadura trabajan juntos para proteger a un caballero en batalla.

Actividad 3

Reflexiona sobre cómo las organizaciones pueden adaptar y aplicar las normativas de seguridad física para proteger eficazmente sus activos tangibles frente a las amenazas actuales y futuras.

5. Prueba de autoevaluación.

¿Cuál es una de las principales novedades de la norma ISO/IEC 27002:2022?

a. La eliminación de todos los controles de seguridad anteriores.

b. La reorganización de los controles en cuatro temas principales.

c. La introducción de medidas únicamente para la seguridad física.

¿Qué concepto clave introduce ITIL 4 para gestionar servicios de TI de manera integral?

a. Modelos de control jerárquico.

b. Sistema de Valor del Servicio (SVS).

c. Automatización de todos los procesos.

Según la LOPDGDD, ¿qué requisito es necesario para el tratamiento de datos personales?

a. Consentimiento claro y específico.

b. Casillas premarcadas.

c. Una declaración general de conformidad.

¿Qué ley regula las medidas para la protección de infraestructuras críticas en España?

a. Ley 5/2014 de Seguridad Privada.

b. Ley 8/2011 y Real Decreto 704/2011.

c. Reglamento de Protección Contra Incendios.

¿Cuál es el principio que indica que los datos personales solo deben tratarse mientras sean necesarios?

a. Principio de integridad y confidencialidad.

b. Principio de limitación de la finalidad.

c. Principio de limitación del plazo de conservación.

La norma ISO/IEC 27002:2022 incluye medidas de seguridad para tecnologías como la nube, _____ y trabajo remoto.

La LOPDGDD refuerza el derecho al _____, permitiendo la eliminación de datos personales cuando ya no sean necesarios.

ITIL 4 introduce un enfoque flexible y práctico que se adapta a las necesidades de cada _____.

La Ley _____ regula los servicios y actividades de seguridad privada en España.

Una infracción muy grave en protección de datos podría acarrear una multa de hasta _____ millones de euros.

Análisis de los procesos de sistemas