MINISTERIO DE TRABAJO Y ECONOMÍA SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL SEPE SERVEI PÚBLIC D'OCUPACIÓ ESTATAL
MINISTERIO DE EDUCACIÓN, FORMACIÓN PROFESIONAL Y DEPORTES
Generalitat de Catalunya
SOC Servei d'Ocupació de Catalunya
IRON HACK SPAIN

Gestión de servicios en el sistema informático.

IFCT0109 – Seguridad informática

MF0490_3 (90 horas)

Comunicaciones seguras

- Introducción
- Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información
- Metodología ITIL. Librería de infraestructuras de las tecnologías de la información
- Ley Orgánica de protección de datos de carácter personal/Ley Orgánica de protección de Datos personales y garantía de los derechos digitales
- Normativas más frecuentemente utilizadas para la gestión de la seguridad física

Introducción

En la actualidad, las tecnologías de la información son esenciales en cualquier organización, integrándose plenamente en sus procesos de gestión. Es crucial comprender las normativas relacionadas con estas tecnologías.

Este capítulo comienza con una visión general del código de buenas prácticas para la gestión de la seguridad de la información, la norma ISO/IEC 27002. Luego, se analiza la librería de infraestructuras de TI, que proporciona recomendaciones para una integración exitosa de las tecnologías con los servicios organizacionales.

Dado que los datos personales suelen estar presentes en las bases de datos organizacionales, se destaca la importancia de cumplir con la normativa sobre el tratamiento de datos personales para evitar infracciones por desconocimiento.

Finalmente, se enfatiza la necesidad de mantener un adecuado nivel de seguridad física para proteger contra intrusiones no autorizadas y el uso indebido de archivos manuales sensibles. El capítulo concluye con medidas y recomendaciones para garantizar un nivel óptimo de seguridad física.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Introducción

La Norma ISO/IEC 27002, desarrollada conjuntamente por la International Organization for Standardization (ISO) y la Comisión Electrotécnica Internacional (IEC), es una evolución de la normativa inicialmente conocida como ISO 17799. Esta norma se enmarca dentro de la serie ISO/IEC 2700X, dedicada a regular aspectos de seguridad en los entornos digitales y electrónicos, proporcionando un conjunto de buenas prácticas en la gestión de seguridad de la información.

Importante: La ISO 17799 se establece como un compendio de buenas prácticas para la efectiva gestión de la seguridad de la información, sentando las bases para la actual ISO/IEC 27002.

La serie ISO/IEC 2700X comprende:

- ISO 27000: Define el vocabulario empleado en toda la serie, facilitando la comprensión de las normas.
- ISO/IEC 27001: Ofrece un manual de buenas prácticas y establece los requisitos para los sistemas de gestión de seguridad de la información (SGSI).
- ISO/IEC 27002: Se presenta como una guía de buenas prácticas que incluye objetivos de control y controles recomendados para asegurar un nivel óptimo de seguridad de la información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Introducción

Estructura de la Norma ISO/IEC 27002

La norma se organiza en varias secciones detalladas a continuación:

- Introducción.
- Campo de aplicación.
- Términos y definiciones.
- Estructura del estándar.
- Evaluación y tratamiento del riesgo.
- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de archivos.
- Seguridad ligada a los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de seguridad de información.
- Gestión de continuidad del negocio.
- Cumplimientos legales.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Introducción.

La información constituye un activo de inestimable valor para las organizaciones en un entorno empresarial globalizado e interconectado. La globalización incrementa la vulnerabilidad de la información ante posibles ataques y amenazas, lo que hace esencial protegerla con los niveles más altos de seguridad.

La norma ISO 27002 establece una guía clara para asegurar sistemas de información robustos y seguros en organizaciones de cualquier índole, sean estas privadas o públicas. Para ello, propone una metodología estructurada que incluye los siguientes pasos:

- Identificación de los requerimientos de seguridad mediante la evaluación de los riesgos a los que se enfrenta la organización.
- Evaluación sistemática de los riesgos de seguridad para determinar las prioridades en la gestión de riesgos y en la implementación de controles.
- Selección de controles adecuados para mitigar los riesgos identificados a un nivel aceptable.
- Establecimiento de un punto de inicio de seguridad, por ejemplo, mediante la implementación de un conjunto esencial de controles.
- Identificación de factores críticos de éxito para la efectiva implementación de la seguridad de la información en la organización.
- Desarrollo y adaptación de controles específicos a las necesidades y particularidades de cada organización.

Implementar estos pasos permite a las organizaciones fortalecer su postura de seguridad, protegiendo así su información crítica frente a las crecientes amenazas en el panorama digital actual.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Objeto y ámbito de aplicación

La ISO 27002 es una normativa que establece objetivos de control y controles específicos con el fin de responder a los requerimientos de seguridad identificados mediante la evaluación de riesgos en las organizaciones.

Diseñada para ser aplicada por cualquier tipo de organización, pública o privada, esta normativa no solo define controles recomendados sino que también proporciona una guía inicial para el desarrollo e implementación de medidas de seguridad propias.

Su objetivo es fomentar un entorno de confianza y participación activa de todas las áreas organizativas en la gestión de la seguridad de la información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Términos y definiciones

- Control: Conjunto de políticas, procedimientos, prácticas y estructuras organizacionales, ya sean administrativas, técnicas, de gestión o legales, diseñadas para manejar los riesgos.
- Medios de Procesamiento de la Información: Cualquier sistema, servicio o infraestructura utilizados en el procesamiento de la información.
- Seguridad de la Información: La protección de la confidencialidad, integridad y disponibilidad de la información. También incluye la autenticidad, responsabilidad, no repudiación y confiabilidad.
- Incidente de Seguridad de la Información: Eventos inesperados que, de tener lugar, poseen un significativo potencial para comprometer las operaciones de negocio y la seguridad de la información.
- Análisis del Riesgo: Método sistemático utilizado para identificar fuentes de riesgo y estimar el riesgo.
- Evaluación del Riesgo: Proceso de comparación del riesgo estimado contra un criterio de riesgo predeterminado para determinar la importancia del riesgo.
- Gestión del Riesgo: Conjunto de actividades orientadas a la dirección y control de una organización con respecto al riesgo.
- *Tratamiento del Riesgo*: Proceso de selección e implementación de medidas para modificar el riesgo.

Estos términos y definiciones fundamentan la estructura sobre la que se construye la gestión de la seguridad de la información según la ISO 27002, proporcionando un marco común de referencia para la identificación, evaluación y tratamiento de los riesgos de seguridad de la información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Estructura de la norma

- Introducción: Proporciona un panorama general sobre la importancia de la seguridad de la información.
- Alcance (Cláusula 1): Define los límites de la aplicación de la norma.
- Normativa de Referencia (Cláusula 2): Enumera las normas que complementan o son necesarias para la aplicación de la ISO/IEC 27002.
- Términos, Definiciones y Conceptos Clave (Cláusula 3): Clarifica el significado de los términos más importantes utilizados en la norma.

A partir de aquí, la norma despliega un conjunto de controles y directrices agrupados en diversas categorías, los cuales están diseñados para abordar aspectos específicos de la seguridad de la información:

Controles Organizacionales: Focused on the governance of information security within the organization.

Controles de Seguridad Física: Dirigidos a proteger los aspectos físicos y el entorno de trabajo.

Controles Técnicos: Incluyen medidas tecnológicas para proteger los sistemas e información.

Controles Relacionados con el Personal: Se enfocan en la gestión y formación de los empleados en materia de seguridad de la información.

La norma ISO/IEC 27002 es dinámica y se actualiza regularmente para reflejar las prácticas contemporáneas en la gestión de la seguridad de la información. Por lo tanto, es importante consultar la versión más reciente para obtener información detallada sobre los controles específicos y su aplicación.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Evaluación y tratamiento del riesgo

Establece directrices detalladas para la evaluación y tratamiento del riesgo en el contexto de la seguridad de la información. Este proceso se divide en dos etapas clave:

- Evaluación de los Riesgos de Seguridad de la Información: Consiste en la identificación, cuantificación y priorización de los riesgos frente a los criterios y objetivos específicos de la organización. Se consideran factores como la magnitud del daño potencial y la probabilidad de que los riesgos identificados se concreten.
- Tratamiento de los Riesgos de la Seguridad de la Información: En esta fase, se toman decisiones informadas sobre la aceptación o mitigación de los riesgos. Los riesgos son generalmente aceptados cuando son bajos y se justifica asumirlos, o cuando, incluso con los costes del tratamiento aplicado, el riesgo se reduce significativamente.

La norma sugiere un enfoque proactivo para manejar los riesgos de seguridad de la información y fomenta una cultura de mejora continua en la gestión de la seguridad de la información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Política de seguridad

La norma ISO/IEC 27002 hace énfasis en la importancia de establecer una política de seguridad de la información que sea coherente con los objetivos de una organización. Es esencial que la dirección apruebe y difunda un documento que:

- Establezca la Política de Seguridad: Definir claramente la política de seguridad de la información que alinee con las metas y objetivos de la organización.
- Acceso al Documento: Asegurarse de que el documento esté disponible y sea accesible para todos los empleados y partes externas relevantes para la empresa.
- Revisión Periódica: Implementar un procedimiento para la revisión sistemática de la política de seguridad, asegurando su actualización y relevancia continua.
- Actualización en Cambios Significativos: Actualizar la política en respuesta a cambios importantes en la organización o el entorno que puedan afectar la seguridad de la información.

Esta política actúa como un punto de referencia para todos los niveles de la organización, asegurando que todos los empleados y colaboradores externos comprendan su rol en la protección de los activos de información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Organización de la seguridad de la información

Proporciona directrices para estructurar la seguridad de la información dentro de las organizaciones, abarcando tanto aspectos internos como la interacción con agentes externos.

Internamente, es vital establecer un marco organizativo que involucre a todos los miembros de la empresa en el apoyo y garantía de la seguridad de la información. Esto incluye la creación de una infraestructura robusta de recursos técnicos que sean capaces de implementar y mantener un sistema de gestión de la información seguro y confiable.

El liderazgo y la alta dirección tienen un papel crucial en el respaldo y coordinación de los diferentes roles implicados en la seguridad de la información. La dirección debe asegurar la asignación clara de responsabilidades y la definición de los procesos para mantener la integridad, confidencialidad y disponibilidad de la información.

En relación con los agentes externos, la organización debe garantizar que cualquier acceso a su información por parte de terceros no comprometa su seguridad. Esto implica realizar evaluaciones de riesgo adecuadas y establecer acuerdos con dichos agentes externos sobre los controles necesarios para preservar la seguridad de la información en todo momento.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Gestión de activos

La gestión de activos en el contexto de la seguridad de la información es un proceso crítico que busca la protección adecuada de los activos de la organización. Según la ISO/IEC 27002, los activos pueden ser bienes tangibles o intangibles que posee una empresa u organización, y la información es uno de los activos intangibles más valiosos.

Para lograr una protección efectiva, es esencial que la organización:

- Realice un Inventario Completo: Identificar y documentar todos los activos, tanto físicos como digitales.
- Asigne Propiedad: Designar a los propietarios responsables de cada activo, garantizando que haya claridad en las responsabilidades de gestión y protección.
- Clasifique la Información: Determinar y documentar la clasificación de la información basada en su nivel de confidencialidad e importancia para la organización.
- Establezca Niveles de Protección: Asignar y aplicar medidas de seguridad apropiadas para cada clasificación de información, proporcionando una protección adicional a los datos más sensibles o críticos.

Este enfoque sistemático asegura que todos los activos estén bajo control y protegidos adecuadamente contra amenazas y vulnerabilidades, alineando la gestión de activos con los objetivos estratégicos de seguridad de la información de la organización.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Seguridad ligada a los recursos humanos

Establece la necesidad de implementar controles en la gestión de recursos humanos para asegurar la seguridad de la información en todas las fases de la relación laboral:

- Antes del Empleo: Se deben prevenir riesgos de seguridad desde el proceso de selección, incluyendo controles en la verificación de antecedentes y en el acuerdo de obligaciones contractuales que establezcan claras expectativas de seguridad.
- Durante el Empleo: La organización debe asegurarse de que los empleados comprenden sus responsabilidades y están formados para desempeñar sus funciones de manera segura. Esto se logra a través de una formación continua y concienciación sobre la política de seguridad de la información.
- Terminación o Cambio de Empleo: Al finalizar la relación laboral, es crucial garantizar que el acceso a la información y a los recursos de la organización sea revocado de manera oportuna y efectiva, y que los activos de la empresa sean devueltos.

La definición y documentación de los roles y responsabilidades de seguridad de la información son fundamentales para asegurar que todos los empleados, contratistas y otros usuarios estén comprometidos y alineados con la política de seguridad de la organización.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Seguridad física y del entorno

Proporciona una serie de controles para garantizar la seguridad física y del entorno de una organización:

- Controles de Acceso: Implementar medidas que prevengan el acceso físico no autorizado, daños o interferencias en las instalaciones y la información de la organización.
- Ubicación de los Medios Físicos: Colocar los medios de procesamiento de información en áreas seguras, con perímetros de seguridad definidos, barreras físicas y controles de acceso apropiados.
- Protección de la Información Crítica: Asegurar que la información sensible y confidencial reciba niveles más altos de protección física para salvaguardarla contra amenazas tanto físicas como ambientales, como la exposición directa a la luz solar o la acumulación de polvo en entornos con maquinaria.

Estos controles son esenciales para proteger tanto los activos físicos como la información vital de la organización de cualquier riesgo potencial que pueda afectar a su confidencialidad, integridad y disponibilidad.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Gestión de las comunicaciones y operaciones

La gestión de las comunicaciones y operaciones dentro de una organización es crucial para asegurar la seguridad en el tratamiento de la información. Se deben establecer procedimientos operativos que definan claramente las responsabilidades de cada persona involucrada en el proceso y garantizar el correcto funcionamiento de los sistemas de información.

Los procedimientos de actuación se deben documentar para asegurar una respuesta efectiva frente a incidencias, reduciendo así el riesgo de negligencia o mal uso de los sistemas. Es fundamental que la gestión de la información con terceros cumpla con los estándares de seguridad acordados y mantenga la integridad de la información compartida.

Los procedimientos operativos deben incluir:

- Control de Cambios: Supervisión y registro de alteraciones significativas en los sistemas de información.
- Respaldo de Datos: Implementación de copias de seguridad para proteger la información crítica.
- Segregación de Responsabilidades: División de tareas y responsabilidades para minimizar el riesgo de acciones no autorizadas.
- Respuesta a Incidentes: Desarrollo de procesos para abordar y resolver incidentes de seguridad.
- Prohibición de Software No Autorizado: Creación de políticas que restrinjan el uso de programas no aprobados.
- Revisión de Software: Auditorías periódicas para asegurar la actualización y seguridad del software.
- Seguridad en Redes: Aplicación de medidas de protección para la información en las redes.
- Acuerdos de Intercambio de Información: Establecimiento de términos claros con terceros para el manejo seguro de datos.

Estos procedimientos son esenciales para prevenir, detectar y responder a problemas de seguridad y para asegurar que las operaciones de la organización sean seguras y eficientes.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Control de acceso

Se resalta la importancia de implementar un conjunto de procedimientos formales para el control de acceso en las organizaciones. Estos procedimientos están diseñados para garantizar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información y para mantener la integridad, confidencialidad y disponibilidad de los sistemas de información de la organización.

Las medidas recomendadas incluyen:

- Uso de Identificadores Únicos: Asignar IDs de usuarios únicos para asegurar accesos autorizados y establecer niveles de acceso diferenciados.
- Gestión de Cambios de Empleo: Bloquear o eliminar los derechos de acceso cuando un empleado cambia de puesto o termina su relación laboral con la empresa.
- Gestión de Claves Secretas: Implementar un proceso formal para el manejo de contraseñas y claves de acceso.
- Revisiones Periódicas: Realizar auditorías regulares de los derechos de acceso por parte de la gerencia.
- Concientización de Usuarios: Informar a los usuarios sobre el uso adecuado y la responsabilidad que implica la gestión de contraseñas.
- Políticas de Escritorio Limpio: Salvaguardar información confidencial, asegurándose de que esté bajo llave cuando no esté en uso.
- Control de Acceso a la Red: Asegurar la protección de los servicios de red mediante controles adecuados para prevenir accesos no autorizados.
- Restricciones a Sistemas Operativos: Limitar el acceso a sistemas operativos mediante autenticación y registro de actividades.
- Seguridad Móvil: Establecer medidas de seguridad para el uso de dispositivos móviles y comunicaciones.
- Procedimientos de Teletrabajo: Definir políticas y procedimientos para las actividades de teletrabajo.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Adquisición, desarrollo y mantenimiento de los sistemas de información

La seguridad debe ser considerada un componente esencial durante el diseño, desarrollo y mantenimiento de los sistemas de información. Esto requiere la integración de requisitos de seguridad desde la etapa inicial de definición de los proyectos, garantizando que todas las áreas de la organización colaboren para identificar y acordar estos requerimientos. La adecuada identificación de los requisitos de seguridad es crítica para que la implementación final del sistema refleje las necesidades de protección de la información de la empresa.

Gestión de incidentes de seguridad de la información

Es crucial contar con procedimientos formalizados para la gestión de incidentes que puedan comprometer la seguridad de la información. Dichos procedimientos deben detallar el proceso de reporte, especificando la información a comunicar, las personas a quienes se debe informar, y la metodología y tiempos para hacerlo. Esto permite a la organización aprender de los incidentes, mejorar la supervisión y respuesta a futuras incidencias y garantizar una gestión efectiva desde su detección hasta la resolución.

Estos procedimientos y prácticas deben ser conocidos por todos los usuarios que manejen información para fomentar una cultura de seguridad y mejorar la capacidad de la organización para responder de manera efectiva ante cualquier brecha de seguridad.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Gestión de la continuidad del negocio

La gestión de la continuidad del negocio, según la Norma ISO/IEC 27002, aboga por integrar la seguridad de la información dentro de los procesos clave para asegurar la resiliencia organizacional. Los fallos en la seguridad de la información pueden tener consecuencias devastadoras, afectando la estabilidad y continuidad operacional de la organización.

Definición de Continuidad del Negocio: Se refiere a la capacidad de la organización para mantener o restaurar sus operaciones críticas durante y después de enfrentar una interrupción significativa.

La norma enfatiza en:

- Identificación de Procesos Críticos: Es fundamental determinar aquellas funciones y procesos esenciales que, en caso de interrupción, impactarían significativamente en la organización.
- Integración de Requerimientos de Seguridad: Los procesos críticos deben incluir consideraciones de seguridad de la información para proteger contra amenazas y vulnerabilidades.
- Implementación de Controles Preventivos: Se deben establecer medidas proactivas para minimizar los riesgos a la seguridad de la información que puedan impactar en la continuidad del negocio.
- Desarrollo de Medidas de Continuidad: Es necesario tener planes y procedimientos que permitan la rápida recuperación y continuidad de las operaciones críticas, asegurando la disponibilidad de la información.

A través de estos pasos, la norma ISO/IEC 27002 proporciona un marco para que las organizaciones desarrollen una estrategia robusta de continuidad del negocio que incluya la protección integral de la seguridad de la información.

Norma ISO 27002. Código de buenas prácticas para la gestión de la seguridad de la información

Estructura de la Norma ISO/IEC 27002

Cumplimiento

El cumplimiento en el contexto de la Norma ISO/IEC 27002 se centra en asegurar que todos los aspectos legales, estatutarios, regulatorios y contractuales relacionados con la seguridad de la información se gestionen adecuadamente. Esto es esencial para evitar violaciones de ley o reglamentaciones que puedan acarrear consecuencias negativas para la organización, tanto en términos de sanciones como de reputación.

Para lograr un nivel adecuado de cumplimiento, la norma sugiere:

- Identificación de Requerimientos: Es vital identificar y comprender todos los requerimientos de seguridad estatutarios, regulatorios y contractuales que afectan a la organización.
- Asesoría Legal: Se recomienda la consulta con profesionales legales especializados para interpretar correctamente la legislación y los reglamentos aplicables.
- Auditorías Periódicas: Realizar auditorías regulares de los sistemas de información permite detectar posibles incumplimientos y actuar en consecuencia para remediarlos.
- Adaptación a la Normativa Vigente: Asegurar que las políticas y procedimientos de seguridad de la información estén alineados con los requerimientos legales actuales, especialmente en áreas críticas como la protección de datos personales y los derechos de propiedad intelectual.

Este enfoque integral no solo cumple con la ley sino que también refuerza la confianza de clientes y stakeholders en la gestión de la seguridad de la información de la organización.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Introducción

La metodología ITIL (Information Technology Infrastructure Library) es un conjunto de prácticas consolidadas para la gestión de servicios de tecnología de la información (TI). Su propósito es alinear los servicios de TI con las necesidades de los negocios y mejorar la eficiencia y eficacia de esos servicios. ITIL ofrece un marco detallado de procesos y funciones que ayudan a las organizaciones a gestionar sus infraestructuras y operaciones de TI de manera más efectiva.

Las prácticas ITIL abarcan el ciclo de vida completo de los servicios de TI, desde la concepción y estrategia hasta el diseño, transición, operación y mejora continua de esos servicios. Esta metodología se enfoca en la calidad del servicio y en el desarrollo eficaz y eficiente de los procesos de TI, contribuyendo a la reducción de costes y al aumento de la satisfacción del cliente.

ITIL se estructura en varios niveles o volúmenes, cada uno centrado en diferentes aspectos de la gestión de servicios de TI:

- Estrategia del Servicio: Define la perspectiva, posición, planes y patrones que una organización debe ejecutar para alcanzar sus objetivos de negocio.
- Diseño del Servicio: Se enfoca en el diseño y desarrollo de servicios y sistemas de gestión de servicios para cumplir con los objetivos estratégicos.
- Transición del Servicio: Gestiona los cambios en el entorno de TI, garantizando que los servicios se entreguen de manera efectiva y eficiente.
- Operación del Servicio: Abarca las actividades y procesos necesarios para entregar y gestionar servicios a niveles acordados.
- Mejora Continua del Servicio: Proporciona una guía para medir y mejorar la calidad, eficacia y eficiencia de los servicios y procesos de TI.

Adoptar ITIL puede traer numerosos beneficios a las organizaciones, incluyendo una mayor alineación entre TI y el negocio, mejor gestión de riesgos, reducción de costes y una mejora en la calidad de los servicios de TI ofrecidos.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Un poco de historia

La historia de ITIL (Information Technology Infrastructure Library) comienza en los años 80, desarrollada inicialmente por la Central Computing and Telecommunications Agency (CCTA), una agencia gubernamental del Reino Unido. El propósito era crear un conjunto de recomendaciones estandarizadas para mejorar la gestión y la entrega de los servicios de tecnologías de la información (TI) en el gobierno británico.

Etapas Clave en la Evolución de ITIL:

- Finales de los años 80: ITIL surge con la publicación de los primeros libros, cubriendo aspectos como la gestión de niveles de servicio y la gestión de centros de ayuda.
- 1990-1999 (ITIL v1): La primera versión de ITIL se expande con más de 30 volúmenes que cubren una amplia gama de prácticas de gestión de servicios de TI.
- 2000-2006 (ITIL v2): ITIL v2 consolida la biblioteca en 9 volúmenes, enfocándose en la gestión de servicios y procesos de soporte y entrega de servicios.
- 2007 (ITIL v3/2011): ITIL v3 introduce el concepto del ciclo de vida del servicio, con 5 publicaciones principales. En 2011, esta versión se actualizó para clarificar ciertos conceptos y procesos.
- Junio de 2019 (ITIL 4): ITIL 4 se lanza para abordar las necesidades de la era digital y la economía del servicio, incorporando prácticas ágiles, Lean IT y DevOps.

Desde su creación, ITIL ha sido adoptada por organizaciones en todo el mundo como un marco para la gestión de servicios de TI, ofreciendo un lenguaje común y prácticas estandarizadas. ITIL se ha mantenido relevante mediante actualizaciones periódicas que reflejan los cambios en la tecnología y las prácticas de negocio. Actualmente, ITIL es propiedad de Axelos, una empresa conjunta entre el gobierno del Reino Unido y Capita plc, que se encarga de desarrollar, gestionar y operar la certificación ITIL.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

Un poco de historia

La historia de ITIL (Information Technology Infrastructure Library) comienza en los años 80, desarrollada inicialmente por la Central Computing and Telecommunications Agency (CCTA), una agencia gubernamental del Reino Unido. El propósito era crear un conjunto de recomendaciones estandarizadas para mejorar la gestión y la entrega de los servicios de tecnologías de la información (TI) en el gobierno británico.

Etapas Clave en la Evolución de ITIL:

- Finales de los años 80: ITIL surge con la publicación de los primeros libros, cubriendo aspectos como la gestión de niveles de servicio y la gestión de centros de ayuda.
- 1990-1999 (ITIL v1): La primera versión de ITIL se expande con más de 30 volúmenes que cubren una amplia gama de prácticas de gestión de servicios de TI.
- 2000-2006 (ITIL v2): ITIL v2 consolida la biblioteca en 9 volúmenes, enfocándose en la gestión de servicios y procesos de soporte y entrega de servicios.
- 2007 (ITIL v3/2011): ITIL v3 introduce el concepto del ciclo de vida del servicio, con 5 publicaciones principales. En 2011, esta versión se actualizó para clarificar ciertos conceptos y procesos.
- Junio de 2019 (ITIL 4): ITIL 4 se lanza para abordar las necesidades de la era digital y la economía del servicio, incorporando prácticas ágiles, Lean IT y DevOps.

Desde su creación, ITIL ha sido adoptada por organizaciones en todo el mundo como un marco para la gestión de servicios de TI, ofreciendo un lenguaje común y prácticas estandarizadas. ITIL se ha mantenido relevante mediante actualizaciones periódicas que reflejan los cambios en la tecnología y las prácticas de negocio. Actualmente, ITIL es propiedad de Axelos, una empresa conjunta entre el gobierno del Reino Unido y Capita plc, que se encarga de desarrollar, gestionar y operar la certificación ITIL.

Metodología ITIL. Librería de infraestructuras de las tecnologías de la información

ITIL V4 y el Sistema de valor del servicio

ITIL 4 es la última evolución del marco de gestión de servicios de tecnología de la información (TI) más ampliamente reconocido y adoptado a nivel mundial. ITIL 4 ofrece un enfoque práctico y flexible para la gestión de servicios de TI, alineando los servicios de TI con las necesidades del negocio y soportando la transformación digital.

ITIL 4 se construye sobre las versiones anteriores, introduciendo el Sistema de Valor del Servicio (SVS) que proporciona una visión holística de cómo todos los componentes y actividades de la organización trabajan juntos para facilitar la creación de valor.

Los siete principios guía de ITIL 4, que son recomendaciones que pueden guiar a una organización en todas las circunstancias, independientemente de los cambios en sus metas, estrategias, tipo de trabajo o estructura de gestión, son:

- Enfocarse en el valor: Todo lo que hagas debe aportar valor al negocio o a las partes interesadas.
- Empieza donde estás: No comiences desde cero sin considerar lo que ya está disponible para ser reutilizado.
- Progreso iterativo con retroalimentación: Avanza en pasos manejables y revisa tu progreso constantemente.
- Colaborar y promover la visibilidad: Trabaja juntos a través de fronteras y mantén la transparencia.
- Pensar y trabajar holísticamente: Ningún servicio, o elemento dentro de un sistema, es independiente de los demás.
- Mantenerlo simple y práctico: Elimina lo que no es necesario y mantén las cosas simples.
- Optimizar y automatizar: Haz uso de la tecnología para optimizar el trabajo y eliminar tareas manuales innecesarias.

Estos principios son fundamentales para la implementación y gestión efectiva de una estrategia de servicios de TI que sea ágil, flexible y alineada con las necesidades del negocio.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Introducción

La Ley Orgánica de Protección de Datos Personales y garantía de Derechos Digitales (LOPDGDD), aprobada en España mediante la Ley Orgánica 3/2018 el 5 de diciembre, es una normativa esencial para la protección de datos personales y la garantía de derechos digitales en España. Esta ley se alinea con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, estableciendo un marco legal detallado para el tratamiento seguro y respetuoso de los datos personales de los ciudadanos.

El artículo 18 de la Constitución Española subraya la importancia de la protección de la intimidad personal y familiar, limitando el uso de la informática para asegurar el honor, la intimidad personal y familiar, y el pleno ejercicio de los derechos. La LOPDGDD profundiza en esta protección, definiendo las obligaciones para los responsables y encargados del tratamiento de datos personales, tanto en el ámbito público como en el privado.

Esta ley cubre diversos aspectos, incluyendo el consentimiento para el tratamiento de datos, los derechos de acceso, rectificación, supresión, y oposición (derechos ARCO), así como la portabilidad de los datos. También introduce conceptos relacionados con la transparencia en el tratamiento de datos y establece directrices claras para la seguridad de la información, la notificación de brechas de seguridad y la protección de datos desde el diseño y por defecto.

Uno de los elementos distintivos de la LOPDGDD es su enfoque en los derechos digitales, tales como el derecho a la desconexión digital en el trabajo, el derecho al olvido en entornos digitales, y la protección de menores en internet. Estos aspectos subrayan la evolución de la protección de datos hacia la inclusión de preocupaciones digitales modernas, haciendo de esta ley un instrumento crucial para adaptarse a las nuevas realidades tecnológicas y sociales.

La implementación adecuada de la LOPDGDD por parte de las organizaciones no solo es una obligación legal sino también un paso importante hacia la construcción de la confianza de los usuarios y clientes en la era digital, garantizando así la protección de sus derechos fundamentales en el ámbito digital.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Ámbito de aplicación

El ámbito de aplicación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), abarca el tratamiento de datos personales dentro de los sectores público y privado. Esta normativa tiene como principal objetivo regular el tratamiento de los datos personales por parte de entidades públicas y privadas, así como garantizar los derechos digitales de los ciudadanos dentro del territorio español.

La LOPDGDD es aplicable a cualquier dato de carácter personal registrado en soporte informático o físico, que lo haga susceptible de tratamiento, y no solo establece cómo se deben tratar estos datos, sino también cómo se deben proteger los derechos digitales en el contexto de la sociedad de la información.

Esta legislación se alinea con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, aplicándose a:

- Entidades que traten datos personales en el marco de sus actividades.
- Tratamientos de datos personales de personas que se encuentren en España.
- Tratamientos de datos fuera de la UE cuando los interesados sean residentes en España y se les ofrezcan bienes o servicios, o se monitorice su comportamiento.

La ley establece una serie de principios y obligaciones para los responsables y encargados del tratamiento de datos, incluyendo medidas de seguridad, derechos de los interesados, y procedimientos para garantizar la protección de datos personales y la privacidad de los ciudadanos en el entorno digital .

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Ámbito de aplicación

Se establecen ciertas exclusiones a su aplicación para determinados casos específicos. Aunque la ley tiene un amplio ámbito de aplicación, no se aplica en los siguientes contextos:

- Datos de personas fallecidas: La legislación de protección de datos se centra en la protección de datos de personas vivas. Los datos de personas fallecidas no están sujetos a las mismas restricciones, aunque la LOPDGDD introduce normas sobre el tratamiento de los datos de personas fallecidas en su artículo 3, reconociendo ciertos derechos a los herederos y allegados.
- Materias clasificadas del Estado: Los ficheros que contienen datos relacionados con la seguridad del Estado y sus materias clasificadas no se rigen por esta ley.
- Ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas: conocida como "excepción doméstica", se refiere al tratamiento de datos que no se lleva a cabo en un contexto profesional o comercial.

Estas exclusiones se establecen para equilibrar el derecho a la protección de datos personales con otros derechos y libertades, incluyendo la libertad de expresión y el derecho a la privacidad en el ámbito personal. Sin embargo, es crucial recordar que incluso en estos casos, se recomienda aplicar buenas prácticas en el manejo de datos personales para evitar posibles perjuicios a terceros .

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Conceptos fundamentales

Datos personales: Se refiere a cualquier información relacionada con personas físicas que pueden ser identificadas o identificables directa o indirectamente. Esto incluye una amplia gama de datos como nombre, identificación, datos de localización, identificadores en línea, o elementos específicos de la identidad física, genética, mental, económica, cultural o social de esa persona natural.

Fichero: Un conjunto organizado de datos personales, ya sea centralizado, descentralizado, o repartido de forma funcional o geográfica, que es accesible según criterios específicos. Este concepto abarca tanto el tratamiento manual como automatizado de los datos.

Tratamiento de datos: Incluye cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por medios automáticos o no. Esto cubre desde la recopilación, registro, organización, estructuración y almacenamiento hasta su consulta, uso, divulgación por transmisión, y eliminación o destrucción.

Responsable del tratamiento: La entidad (persona física o jurídica, autoridad pública, servicio u otro organismo) que determina los fines y medios del tratamiento de los datos personales.

Encargado del tratamiento: Es quien trata datos personales por cuenta del responsable del tratamiento, siguiendo sus instrucciones.

Afectado o interesado: La persona física a quien pertenecen los datos personales que están siendo tratados.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Conceptos fundamentales

Consentimiento del interesado: Es la aprobación expresa, libre, informada e inequívoca por parte del titular de los datos, para el tratamiento de sus datos personales.

Cesión o comunicación de datos: La revelación de datos a un tercero.

Fuentes accesibles al público: Incluye cualquier fuente de datos a la que cualquier persona pueda tener acceso, como censos promocionales, repertorios telefónicos, listas profesionales, diarios y boletines oficiales, y medios de comunicación.

La comprensión de estos conceptos es crucial para aplicar adecuadamente las disposiciones de la LOPDGDD y para garantizar una protección efectiva de los datos personales dentro del marco legal español y europeo.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

Principio de calidad

El principio de calidad en la protección de datos personales es uno de los pilares fundamentales para asegurar una adecuada gestión y tratamiento de estos datos. Este principio establece que los datos personales deben ser precisos, adecuados, pertinentes y, en la medida de lo posible, actualizados respecto a las finalidades para las cuales se recogen y tratan.

La importancia del principio de calidad radica en la necesidad de garantizar que los datos personales reflejen con fidelidad la realidad del individuo al que conciernen, evitando así posibles perjuicios derivados de errores, inexactitudes o desactualizaciones. Este principio implica la adopción de todas las medidas necesarias para corregir o eliminar los datos que resulten ser inexactos o incompletos.

En el marco de la protección de datos, el principio de calidad obliga a los responsables del tratamiento de datos a:

- Verificar la exactitud de los datos personales en el momento de su recogida.
- Mantener los datos personales actualizados, realizando las modificaciones necesarias para corregir inexactitudes o completar información parcial.
- Asegurar que los datos sean pertinentes y no excesivos en relación con las finalidades del tratamiento.
- Eliminar o rectificar sin dilación los datos personales que resulten ser inexactos o incompletos.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

Principio de información

Este principio asegura que cualquier persona cuyos datos personales van a ser recogidos y tratados debe ser informada de manera clara, precisa e inequívoca sobre diversos aspectos del tratamiento de sus datos.

Bajo este principio, los responsables del tratamiento de los datos deben proporcionar al interesado, en el momento de la recogida de sus datos, información detallada sobre:

- La identidad y los datos de contacto del responsable del tratamiento, así como del representante del responsable, si es aplicable.
- La finalidad del tratamiento para el cual se destinan los datos personales recogidos.
- La base legal para el tratamiento de los datos, destacando si se basa en el consentimiento, en la necesidad de ejecutar un contrato, el cumplimiento de una obligación legal, entre otros.
- Los destinatarios o las categorías de destinatarios de los datos personales, si existen.
- La posibilidad de ejercer los derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad de los datos.
- La transferencia de datos a terceros países o organizaciones internacionales, en caso de que esto ocurra, y las garantías bajo las cuales se realiza tal transferencia.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

Principio de consentimiento del afectado

El tratamiento de estos datos requiere la autorización previa, libre, específica, informada e inequívoca del individuo a quien pertenecen. Este consentimiento debe ser otorgado de manera clara, ya sea por una acción afirmativa o una declaración que indique el acuerdo del titular de los datos para su tratamiento .

Sin embargo, existen excepciones a este principio, situaciones en las que el tratamiento de datos personales puede llevarse a cabo sin obtener el consentimiento del afectado:

- Cuando la ley lo disponga: Existen normativas que permiten el tratamiento de datos personales sin necesidad del consentimiento del individuo, siempre que se cumplan ciertos requisitos y se justifique en el marco de una ley .
- Intereses vitales del afectado o de otra persona: En casos donde es necesario tratar datos personales para proteger intereses vitales del titular de los datos o de otra persona, especialmente cuando el titular no está en capacidad de dar su consentimiento .
- Ejercicio de funciones públicas o poderes públicos: El tratamiento de datos personales sin consentimiento es permitido cuando es necesario para el ejercicio de funciones públicas, asignadas a un responsable del tratamiento por el derecho de la Unión o de los Estados miembros .
- Relaciones contractuales: Cuando el tratamiento de datos personales es necesario para la ejecución de un contrato en el que el interesado es parte, o para tomar medidas a solicitud del interesado antes de celebrar un contrato .
- Intereses legítimos perseguidos por el responsable o por un tercero: En situaciones donde el tratamiento es necesario para los intereses legítimos de un responsable del tratamiento o de un tercero, siempre que sobre estos intereses no prevalezcan los derechos y libertades del afectado .

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

Datos especialmente protegidos

Los datos especialmente protegidos son una categoría de datos personales que, debido a su naturaleza sensible, reciben un nivel de protección más elevado. Estos datos son aquellos que pueden revelar aspectos muy personales de una persona, y su tratamiento indebido podría afectar a los derechos y libertades fundamentales de los individuos.

Entre los tipos de datos especialmente protegidos se incluyen:

- Ideología, religión y afiliación sindical: Datos que revelan las creencias políticas, religiosas o filosóficas de una persona, o su pertenencia a sindicatos.
- Origen racial o étnico: Información sobre el origen racial o el origen étnico de una persona.
- Salud: Datos relativos a la salud física o mental de una persona, incluyendo la provisión de servicios de atención médica.
- Vida sexual: Información sobre la vida sexual o la orientación sexual de una persona.
- Datos genéticos: Datos personales relativos a las características genéticas heredadas o adquiridas de una persona que dan información única sobre la fisiología o la salud de esa persona.
- Datos biométricos: Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen su identificación única, como huellas dactilares o reconocimiento facial.

El tratamiento de estos datos está sujeto a restricciones y solo puede realizarse bajo circunstancias específicas (consentimiento expreso; obligaciones y derechos específicos en el ámbito del empleo y la seguridad social y protección social; protección de intereses vitales del interesado o de otra persona física, …)

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

Datos relativos a la salud. La gestión de datos personales relacionados con la salud por parte de instituciones y centros sanitarios, tanto públicos como privados, así como por los profesionales correspondientes, está estrictamente regulada. Estos datos solo pueden ser tratados cuando las personas acudan a estos centros o requieran tratamiento, asegurando así su privacidad y protección.

El principio de seguridad de los datos implica que el responsable del tratamiento debe implementar medidas tanto técnicas como organizativas adecuadas para salvaguardar los datos de carácter personal. Esto incluye la prevención de acceso no autorizado, divulgación, alteración o destrucción de la información personal. Estas medidas deben ser proporcionales al riesgo y a la sensibilidad de los datos tratados, particularmente cuando se trata de datos de salud, que son considerados especialmente sensibles y protegidos.

El principio de deber de confidencialidad establece que todas las personas involucradas en el tratamiento de datos personales, no solo el responsable de su tratamiento, deben mantener la confidencialidad de la información. Este deber de confidencialidad es fundamental para mantener la confianza en el sector sanitario y asegurar que la información de salud de los pacientes se maneje con el máximo cuidado y discreción. Este principio está respaldado por el artículo 5.1.f) del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que establece claramente la importancia de tratar los datos personales de manera segura y confidencial .

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Principios fundamentales

El principio de deber de confidencialidad establece que el responsable del tratamiento de datos personales, así como cualquier persona que participe en este tratamiento, debe mantener la confidencialidad de la información manejada. Este mandato se encuentra en el artículo 5.1.f) del Reglamento General de Protección de Datos (RGPD) de la Unión Europea y subraya la importancia de proteger los datos personales de accesos no autorizados o divulgaciones indebidas .

El principio de comunicación de datos señala las condiciones bajo las cuales los datos personales pueden ser compartidos con terceros. Es esencial que cualquier transferencia de datos se haga:

- Con el consentimiento explícito del interesado.
- Para fines que estén directamente relacionados con las obligaciones legítimas del emisor y el receptor de los datos.
- Garantizando que el interesado esté plenamente informado sobre quién recibirá sus datos y con qué propósito .

El principio de acceso a los datos por cuenta de terceros indica que cualquier acceso a los datos personales por parte de terceros debe cumplir con las normas establecidas. Si una persona o entidad diferente al responsable original del tratamiento accede a los datos, esta se convierte en encargada del tratamiento y debe operar bajo un acuerdo contractual que especifique las condiciones y limitaciones de este acceso. Esto asegura que el tratamiento de los datos se realice de manera segura y conforme a la ley .

Estos principios son pilares fundamentales del RGPD, destinados a proteger la privacidad y seguridad de los datos personales y a asegurar que su tratamiento se realice de forma transparente, segura y con pleno respeto a los derechos de los individuos.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Derecho de las personas

Derecho de acceso: Este derecho permite a cualquier persona saber si sus datos personales están siendo tratados y, en caso afirmativo, acceder a ellos. Este derecho está detallado en el artículo 15 del Reglamento General de Protección de Datos (RGPD).

Derecho de rectificación: Permite al interesado solicitar la corrección de datos inexactos o incompletos. Es un derecho vital para garantizar la precisión de los datos personales tratados.

Derecho de supresión (también conocido como "el derecho al olvido"): Habilita a la persona a solicitar la eliminación de sus datos cuando, entre otros motivos, los datos ya no son necesarios para los fines que fueron recogidos o el consentimiento se retira.

Derecho de oposición: Otorga el derecho a oponerse al tratamiento de los datos personales en determinadas circunstancias, como en el caso de la toma de decisiones automatizada, incluida la elaboración de perfiles.

Derecho a la limitación del tratamiento: Este derecho permite a los interesados solicitar la suspensión del tratamiento de sus datos en ciertas situaciones, como cuando se impugna la exactitud de los datos, mientras se verifica esta exactitud.

Derecho a la portabilidad: Facilita a las personas el derecho a recibir sus datos personales en un formato estructurado y de uso común, y a transmitirlos a otro responsable del tratamiento sin impedimentos por parte del responsable al que se los había proporcionado inicialmente.

Estos derechos constituyen una parte fundamental de la protección de datos en la Unión Europea, reforzando el control que las personas tienen sobre sus propios datos personales y asegurando que estos sean tratados de manera justa, legal y transparente
.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Seguridad y de los datos y el documento de seguridad

La LOPDGDD es esencial para las organizaciones, ya que clarifica aspectos no cubiertos por el Reglamento General de Protección de Datos (RGPD), brindando así una guía más detallada para la gestión diaria de los datos personales.

Esta ley establece roles clave para garantizar un tratamiento adecuado de los datos:

- Responsable de tratamiento de datos: Encargado de planificar y organizar las acciones técnicas para garantizar el uso correcto de los datos en la organización.
- Encargado de tratamiento de datos: Responsable de realizar labores organizativas y técnicas, incluido el control de actividades relacionadas con el uso de los datos.
- Delegado de Protección de Datos (DPD): Encargado de supervisar y conservar los datos, representando los compromisos de protección y privacidad a nivel europeo.

El DPD es obligatorio en ciertas condiciones, como cuando el tratamiento de datos es realizado por organismos públicos, o cuando se realizan actividades de volumen considerable o relacionadas con condenas y delitos.

Aunque la responsabilidad última recae en el responsable de tratamiento, tanto este como el encargado deben cumplir con sus obligaciones y pueden ser supervisados independientemente por las autoridades de protección de datos.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Seguridad y de los datos y el documento de seguridad

Medidas de seguridad de los datos. Varían según el responsable del tratamiento de datos:

Para el responsable de tratamiento de datos:

- Implementación de medidas para garantizar el cumplimiento del Reglamento General de Protección de Datos.
- Elección del encargado de tratamiento de datos.
- Contratación exclusiva de encargados que ofrezcan garantías suficientes para cumplir con los requisitos del RGPD.

Para el encargado de tratamiento de datos:

- Mantenimiento de un registro de actividades de tratamiento.
- Determinación de medidas de seguridad para los tratamientos que realiza.
- Designación de un Delegado de Protección de Datos cuando sea necesario.
- Adhesión a códigos de conducta.
- Certificación como instrumento para demostrar la adecuación a la normativa.

Para asegurar una correcta gestión de los datos, la relación entre el responsable y el encargado debe estar respaldada por un contrato que detalle aspectos esenciales como la finalidad del tratamiento y la obligación del encargado de suprimir o devolver los datos una vez finalizada la relación.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Seguridad y de los datos y el documento de seguridad

Medidas de seguridad de los datos.

Las medidas de protección de los datos deben cumplir con el principio de responsabilidad proactiva, lo que implica:

- Realizar un análisis del riesgo asociado al tratamiento de los datos.
- Mantener un registro detallado de las actividades de tratamiento.
- Integrar la protección de datos desde el diseño y por defecto, incluyendo la implementación de medidas de seguridad.
- Notificar cualquier violación de seguridad de los datos.
- Realizar evaluaciones de impacto sobre la protección de datos para identificar y abordar posibles riesgos.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Seguridad y de los datos y el documento de seguridad

Medidas de seguridad de los datos.

Las medidas de seguridad de los datos deben adaptarse al principio de responsabilidad proactiva considerando variables como el coste de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades.

Estas medidas incluyen:

- Definir y establecer funciones y obligaciones de usuarios con acceso a datos, con autorizaciones correspondientes.
- Establecer un procedimiento de notificación y gestión de incidencias, con controles de acceso.
- Identificar y inventariar soportes y documentos con datos personales.
- Implementar medidas para la identificación y autenticación de usuarios.
- Realizar copias de respaldo periódicas y establecer procedimientos de recuperación de datos.
- Verificar semestralmente la definición y aplicación de procedimientos de copias de seguridad y recuperación de datos.
- Proteger dispositivos de almacenamiento no automatizados con mecanismos de seguridad.
- Designar responsables de seguridad y realizar auditorías internas y externas regularmente.
- Establecer registros de entrada y salida de soportes y limitar intentos de acceso no autorizado.
- Identificar soportes mediante sistemas de etiquetado y cifrar datos.
- Conservar copias de seguridad en ubicaciones distintas y almacenar registros de acceso durante al menos dos años.
- Revisar mensualmente la información de control registrada y elaborar informes de las revisiones realizadas.
- Almacenar ficheros no automatizados en áreas con acceso restringido y protegido.
- Controlar la reproducción de documentos y adoptar medidas al trasladar físicamente la documentación.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

La Agencia Española de Protección de Datos

La Agencia Española de Protección de Datos (AEPD) es un ente público con plena independencia de las Administraciones Públicas, dotado de personalidad jurídica y capacidad tanto pública como privada.

Sus principales funciones son:

- Controlar y promover la aplicación del Reglamento General de Protección de Datos y demás normativa relacionada.
- Sensibilizar al público sobre los riesgos, normas y derechos en materia de tratamiento de datos, con especial atención a actividades dirigidas a niños.
- Asesorar a instituciones y organismos sobre medidas legislativas y administrativas para proteger los derechos y libertades de las personas respecto al tratamiento de datos.
- Promover la sensibilización de responsables y encargados del tratamiento respecto a sus obligaciones según el Reglamento.
- Facilitar información a interesados sobre sus derechos según el Reglamento y cooperar con autoridades de control de otros Estados miembros cuando sea necesario.

En general, la AEPD verifica la legalidad de los tratamientos de datos, sancionando incumplimientos y difundiendo normativa relacionada con la protección de datos.

Nota: La AEPD ofrece su página web agpd.es para consultas sobre protección de datos.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Infracciones y sanciones

Las infracciones y sanciones en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) son importantes para garantizar el cumplimiento de la normativa de protección de datos. Algunos aspectos relevantes son:

- La LOPDGDD establece distintos tipos de infracciones, que van desde leves hasta muy graves, dependiendo de la gravedad y las circunstancias del incumplimiento.
- Las multas por infracciones pueden ser significativas, alcanzando hasta 20 millones de euros o, en el caso de empresas, el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.
- Las infracciones pueden incluir el tratamiento de datos sin consentimiento, la falta de medidas de seguridad adecuadas, la falta de cumplimiento de las obligaciones en relación con los derechos de los interesados, entre otros.
- La Autoridad de Control, como la Agencia Española de Protección de Datos (AEPD), es la encargada de investigar y sancionar las infracciones, garantizando así el cumplimiento de la normativa.

Ley Orgánica de protección de Datos personales y garantía de los derechos digitales

Infracciones y sanciones

Las infracciones y sanciones en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) son importantes para garantizar el cumplimiento de la normativa de protección de datos. Algunos aspectos relevantes son:

- La LOPDGDD establece distintos tipos de infracciones, que van desde leves hasta muy graves, dependiendo de la gravedad y las circunstancias del incumplimiento.
- Las multas por infracciones pueden ser significativas, alcanzando hasta 20 millones de euros o, en el caso de empresas, el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.
- Las infracciones pueden incluir el tratamiento de datos sin consentimiento, la falta de medidas de seguridad adecuadas, la falta de cumplimiento de las obligaciones en relación con los derechos de los interesados, entre otros.
- La Autoridad de Control, como la Agencia Española de Protección de Datos (AEPD), es la encargada de investigar y sancionar las infracciones, garantizando así el cumplimiento de la normativa.

Normativas más frecuentemente utilizadas para la gestión de la seguridad física

La seguridad física es fundamental para proteger la información y los recursos de una organización. La norma ISO/IEC 27002 aborda esta cuestión en su sección 9, "Seguridad Física y del Entorno". A continuación, se detallan las medidas recomendadas:

Áreas Seguras

- Perímetro de Seguridad Física: Implementar barreras y controles de acceso para proteger las áreas de procesamiento de información.
- Controles Físicos de Entrada: Utilizar sistemas de autenticación, como tarjetas de acceso, para garantizar que solo el personal autorizado acceda a áreas sensibles.
- Seguridad de Oficinas, Habitaciones y Medios: Aplicar medidas físicas de seguridad para restringir el acceso a directorios y teléfonos internos.
- Protección contra Amenazas: Adoptar medidas para prevenir daños por fuego, inundaciones, terremotos y otras amenazas naturales o causadas por el hombre.
- Trabajo en Áreas Seguras: Establecer directrices para el trabajo en estas áreas, prohibiendo dispositivos como cámaras fotográficas o de vídeo, salvo autorización.
- Áreas de Carga y Descarga: Controlar los accesos a estas zonas para evitar intrusiones no autorizadas, restringiendo el acceso al personal identificado.

Estas medidas contribuyen a mitigar riesgos y garantizar la integridad de los activos de la organización.

Normativas más frecuentemente utilizadas para la gestión de la seguridad física

Seguridad de los equipos

La seguridad de los equipos es esencial para evitar pérdidas, daños o interrupciones en las actividades de la organización. Aquí se detallan medidas clave para proteger los activos contra amenazas físicas y ambientales:

- Ubicación y Protección del Equipo: Colocar el equipo en espacios que minimicen los riesgos ambientales y los accesos no autorizados, como el uso de membranas de protección del teclado en entornos industriales.
- Servicios Públicos de Soporte: Proteger el equipo contra interrupciones de suministro eléctrico con sistemas de alimentación interrumpida (SAI) para mantener la electricidad durante cortes.
- Seguridad del Cableado: Proteger el cableado para evitar daños y interferencias, como separar los cables de alimentación de los de comunicaciones.
- Mantenimiento de los Equipos: Garantizar un mantenimiento adecuado realizado por personal autorizado para preservar la disponibilidad y la integridad del equipo.
- Seguridad de los Equipos Fuera de las Instalaciones: Aplicar medidas específicas, como contratar seguros adecuados, para proteger el equipo utilizado fuera de las instalaciones contra robos o daños.
- Reutilización o Retirada Segura de Equipos: Realizar controles para asegurar que la información en los equipos sea borrada de forma segura, sin posibilidad de recuperación, antes de su reutilización o retirada.
- Retirada de Propiedades de la Organización: No retirar equipo ni otros activos de la organización sin autorización previa para proteger la información y los recursos.

Resumen

La información es un activo crucial en las organizaciones modernas, donde puede circular globalmente en segundos. La norma ISO/IEC 27002 ofrece directrices para establecer, implementar y difundir medidas de seguridad, abordando aspectos como la evaluación de riesgos y la gestión de activos. Es fundamental garantizar un nivel adecuado de seguridad física en las áreas seguras y los equipos de la organización.

Además de seguir las recomendaciones de la ISO/IEC 27002, es vital integrar las tecnologías de la información en todos los procesos organizativos. Para ello, se puede recurrir a ITIL, una biblioteca de buenas prácticas que busca mejorar la gestión de servicios de TI.

La protección de los datos personales es esencial debido a su carácter fundamental, respaldado por la Constitución española. La Ley Orgánica 3/2018 sobre Protección de Datos Personales y Garantía de los Derechos Digitales establece los derechos individuales sobre los datos personales y los requisitos de tratamiento y protección según su grado de intimidad.