Intedya
International Dynamic Advisors

ISO/IEC 27001 - Sistemas de Gestión de Seguridad de la Información

Ya vivimos en la **sociedad de la información**, una gran parte de nuestras actividades diarias se valen del almacenamiento, la utilización y la transmisión de información.
La **información** en las organizaciones es un **activo** tangible o intangible que tiene un determinado **valor** para el desarrollo de sus procesos de negocio, por lo cual debe ser protegida de manera proporcional a ese valor.
La **seguridad de la información** debe ser aplicada a toda la información independientemente de cual sea su fuente, su tipo, su estado y su forma, sin equiparar los términos de seguridad de la información y de seguridad informática. Si bien la seguridad informática forma parte de la seguridad de la información, todos tenemos un expediente almacenado en papel.
La norma **ISO/IEC 27001** define los mecanismos, controles y medidas necesarios para que las organizaciones puedan proteger sus activos y la información que estos gestionan en base a las dimensiones de seguridad de la información (Confidencialidad – Integridad – Disponibilidad).
Esta norma **ISO/IEC 27001** basa su funcionamiento en la **gestión de los riesgos** de seguridad de la información asegurando que estos son identificados, evaluados y gestionados, adaptándose así a las características de cualquier tipo de organización.

Principales **REQUISITOS**

- El **LIDERAZGO** imprescindible de la alta dirección;
- La consideración del **CONTEXTO** como factor estratégico;
- EVALUACIÓN, GESTIÓN y TRATAMIENTO del **RIESGO**, como elemento clave;
- **MEDIDAS ORGANIZATIVAS, TÉCNICAS y LEGALES** , para lograr la protección de la información;
- Establecimiento de **MECANISMOS DE CONTROL** de acceso físico, lógico, control de red y criptográficos;
- **Asegurar** la **seguridad de la información** en el **SERVICIO A TERCEROS** y en el **INTERCAMBIO** de la información;
- Disponer de **CONTRATOS DE CONFIDENCIALIDAD** con los empleados;
- Formalización de **ACUERDOS CON PROVEEDORES** que incluyan requisitos de seguridad;
- Cumplimiento con la **LEGISLACIÓN APLICABLE** en materia de protección de datos personales;
- **USO DE SOFTWARE** con licencias;
- GESTIÓN DE INCIDENCIAS relativas a la seguridad de la información;
- La importancia de la gestión desde el punto de vista seguridad de la información debe comunicarse dentro de la organización, la **TOMA DE CONCIENCIA Y EL COMPROMISO de todas las personas es imprescindible para que el sistema funcione;**
- Proporcionar la **FORMACIÓN** necesaria para **garantizar la competencia de las personas** que realizan tareas relacionadas con la seguridad de la información;
- **PRESERVACIÓN DE LA CONTINUIDAD** de los recursos de formación, realización de pruebas.

Ejemplos de **ACCIONES PRÁCTICAS A IMPLEMENTAR**

- Realización del análisis de riesgos de seguridad de la información.
- Formalización de contratos de confidencialidad con los empleados y proveedores.
- Formalización de acuerdos prestación de servicio.
- Uso de credenciales de acceso a las instalaciones para visitantes.
- Mecanismos que obstaculicen el acceso a las áreas seguras: dispositivos biométricos, etc.
- Uso de dispositivos de alimentación interrumpida.
- Uso de controladores de temperatura CPD.
- Uso de licencias legales.
- Realización de planes de continuidad
- Planes de prueba: caída de suministro eléctrico, fallos en los servidores, fallo comunicaciones, incendio edificio, etc.
- Política de gestión de contraseñas.
- Limitar la utilización de usuarios genéricos y los permisos de administración.
- Restringir los puertos USB a puestos determinados.
- Implantar y configurar un antivirus para todos los equipos de la organización, incluyendo los dispositivos móviles
- Instalación de Firewalls, VPN.
- Controlar y prohibir el acceso remoto hacia la propia organización.
- Limitar la navegación a páginas de ciertos contenidos y Sistemas de Detección de Intrusos.
- Realización de copias de seguridad.
- Segmentación de redes y conexiones seguras.
- Proteger las claves de acceso a sistemas, datos y servicios, almacenándolas de forma cifrada.
- Uso certificado digitales para el intercambio de información.

*Las acciones indicadas son sólo ejemplos, estás deberán ser adaptadas a la realidad y necesidades de cada organización

Ventajas para **LA ORGANIZACIÓN**

Muchas organizaciones no conocen la información que gestionan o no conocen la importancia de la información que gestionan hasta que se produce una incidencia que les enfrenta a la dura realidad.

Las organizaciones están expuestas a múltiples amenazas (fallos energéticos, virus informáticos, fraude, error humano, fallo de elementos, accesos indebidos, desastres naturales, vandalismo, …) a las que son más o menos vulnerables y para cuya gestión deben estar preparadas.
La implantación en las organizaciones de un sistema de gestión de seguridad de la información bajo los requisitos de la norma ISO/IEC 27001 les permite minimizar la probabilidad de materialización de las amenazas y estar preparados para minimizar su impacto en caso de que se materialicen (pérdidas financieras, litigios laborales, multas, pérdida de clientes, daños de imagen, interrupción de las operaciones, costes de recuperación, …).
La norma ISO/IEC 27001 nos lleva a establecer diferentes políticas, procedimientos, aplicaciones informáticas o elementos físicos necesarios para definir la seguridad de nuestros activos de manera proporcionada.

Ventajas para **LOS CLIENTES**

Los clientes de una organización que implanta y mantiene un sistema de gestión de seguridad de la información bajo los requisitos de la norma ISO/IEC 27001 saben que la información gestionada por su proveedor para la prestación del servicio o para la generación del producto que reciben dispone de todos los controles necesarios para garantizar su protección y preservación.

Ventajas para **EL MERCADO**

Empresas comprometidas con la seguridad de la información, que garantizan una adecuada gestión de la información con la que trabajan.

Sectores **DE APLICACIÓN**

La **norma ISO 27001** tiene **vocación universal**, aplicable a organizaciones de **todos los sectores y tamaños,** y que describe de qué debe constar un **sistema de gestión de la seguridad de la información en cualquier tipo de organización.**

La norma es especialmente útil cuando la **protección de la información es crítica,** como por ejemplo, en las áreas de **gobierno, banca y finanzas, salud, empresas de servicios de tecnología de la información o comunicaciones** , o cualquier otro ámbito donde los activos de información requieran de una adecuada protección.