SEGURIDAD INFORMÁTICA

Conceptos básicos sobre ISO 27001

- Gestión de la seguridad de la información
- Cuatro fases del sistema de gestión de seguridad de la información
- Documentos de ISO 27001
- La Fase de planificación
- La Fase de implementación
- La Fase de verificación
- La Fase de mantenimiento y mejora
- Otras normas relacionadas con seguridad de la información

Gestión de la seguridad de la información

- La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información.
- La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.
- A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

Cuatro fases del sistema de gestión de seguridad de la información

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

- La Fase de planificación: esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).
- La Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
- La Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.
- La Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

Documentos de ISO 27001

La norma ISO 27001 requiere los siguientes documentos:

- el alcance del SGSI;
- la política del SGSI;
- procedimientos para control de documentación, auditorías internas y procedimientos para medidas correctivas y preventivas;
- todos los demás documentos, según los controles aplicables;
- metodología de evaluación de riesgos;
- informe de evaluación de riesgos;
- declaración de aplicabilidad;
- plan de tratamiento del riesgo;
- registros.
- La cantidad y exactitud de la documentación depende del tamaño y de las exigencias de seguridad de la organización; esto significa que una docena de documentos serán suficientes para una pequeña organización, mientras que las organizaciones grandes y complejas tendrán varios cientos de documentos en su SGSI.

La Fase de planificación

Esta fase está formada por los siguientes pasos:

- determinación del alcance del SGSI;
- redacción de una Política de SGSI;
- identificación de la metodología para evaluar los riesgos y determinar los criterios para la aceptabilidad de riesgos;
- identificación de activos, vulnerabilidades y amenazas;
- evaluación de la magnitud de los riesgos;
- identificación y evaluación de opciones para el tratamiento de riesgos;
- selección de controles para el tratamiento de riesgos;
- obtención de la aprobación de la gerencia para los riesgos residuales;
- obtención de la aprobación de la gerencia para la implementación del SGSI;
- redacción de una declaración de aplicabilidad que detalle todos los controles aplicables, determine cuáles ya han sido implementados y cuáles no son aplicables.

La Fase de implementación

Esta fase incluye las siguientes actividades:

- redacción de un plan de tratamiento del riesgo que describe quién, cómo, cuándo y con qué presupuesto se deberían implementar los controles correspondientes;
- implementación de un plan de tratamiento del riesgo;
- implementación de los controles de seguridad correspondientes;
- determinación de cómo medir la eficacia de los controles;
- realización de programas de concienciación y capacitación de empleados;
- gestión del funcionamiento normal del SGSI;
- gestión de los recursos del SGSI;
- implementación de procedimientos para detectar y gestionar incidentes de seguridad.

La Fase de verificación

Esta fase incluye lo siguiente:

- implementación de procedimientos y demás controles de supervisión y control para determinar cualquier violación, procesamiento incorrecto de datos, si las actividades de seguridad se desarrollan de acuerdo a lo previsto, etc.;
- revisiones periódicas de la eficacia del SGSI;
- medición la eficacia de los controles;
- revisión periódica de la evaluación de riesgos;
- auditorías internas planificadas;
- revisiones por parte de la dirección para asegurar el funcionamiento del SGSI y para identificar oportunidades de mejoras;
- actualización de los planes de seguridad para tener en cuenta otras actividades de supervisión y revisión;
- mantenimiento de registros de actividades e incidentes que puedan afectar la eficacia del SGSI.

La fase de mantenimiento y mejora

Esta fase incluye lo siguiente:

- implementación en el SGSI de las mejoras identificadas;
- toma de medidas correctivas y preventivas y aplicación de experiencias de seguridad propias y de terceros;
- comunicación de actividades y mejoras a todos los grupos de interés;
- asegurar que las mejoras cumplan los objetivos previstos.

Otras normas relacionadas con seguridad de la información

- Además de la ISO 27001 (antiguamente BS 7799-2), la norma ISO 27002 (antiguamente ISO 17799) es una norma "auxiliar" que proporciona más información sobre cómo implementar los controles de seguridad especificados en la ISO 27001.
- Otras normas que también pueden resultar útiles son la ISO 27005, que describe los procedimientos de evaluación de riesgos con mayor profundidad, y la BS 25999-2, que proporciona una descripción detallada de la gestión de la continuidad del negocio.