GAP ANALYSIS ISO 27001/27001

SEGURIDAD DE LA INFORMACION

EVALUACIÓN ISO 17799 PARA LA SEGURIDAD DE LA INFORMACION

Objetivo y descripción

Evaluar el nivel de implementación de la norma ISO 27001/27002 en la organización con el fin de mejorar la seguridad de la información. Los objetivos de la seguridad de la información que buscan estas recomendaciones son: Confidencialidad, Integridad y Disponibilidad.

La recomendación ISO 27001/27002 se evalúa en los siguientes aspectos:

Clasificación y Control de activos.

El objetivo de esta sección es mantener una apropiada protección de los activos de la compañía y garantizar que los activos informáticos reciban un nivel apropiado de protección.

Continuidad del negocio

El objetivo de esta sección es eliminar las posibles interrupciones a las actividades propias del negocio y procesos críticos, con el fin de evitar fallas o desastres.

Administración de operaciones.

Los objetivos de esta sección son:

1) Garantizar operaciones seguras en sitios de procesamiento de la información.
2) Minimizar el riesgo de fallas de los sistemas.
3) Proteger la integridad del software y la información.
4) Mantener la integridad y la disponibilidad de los sistemas de información.
5) Garantizar la protección de las redes y la infraestructura de soporte.
6) Prevenir daños a los activos y fallas en la continuidad del negocio.
7) Prevenir perdida, modificaciones, o un mal uso de la información.

Conformidad con leyes civiles, contractuales y legales.

Los objetivos de esta sección son:

1) Evitar violaciones al cumplimiento o de algunos de los requerimientos de seguridad.
2) Garantizar cumplimiento de las políticas y estándares de seguridad.
3) Maximizar la efectividad y minimizar la interferencia de los procesos de auditoria.

Seguridad en aspectos relacionados con el recurso humano.

Los objetivos de esta sección son:

1) Reducir el riesgo de errores humanos, robos o fraude.
2) Soportar las políticas de seguridad de la compañía en el curso de su trabajo normal.
3) Minimizar el daño ocasionado por incidentes de seguridad y poder aprender de ellos.

Seguridad Física

Los objetivos de esta sección:

Prevenir acceso no autorizado con el fin de prevenir pérdidas, daños o interrupciones de las actividades del negocio, para evitar comprometer la información de los lugares donde están los sistemas de información.

Seguridad en la organización

Los objetivos de esta sección son:

1) Administrar la seguridad de la información dentro de la compañía.
2) Mantener la seguridad de los lugares donde se encuentran los sistemas de información y los activos de información utilizados por terceras partes.
3) Mantener la seguridad de la información cuando la responsabilidad se ha transferido en un proceso de outsourcing.

Políticas de seguridad

El objetivo de esta sección es proveer dirección de alto nivel y soporte para la seguridad de la información.

Sistemas de control de acceso

Los objetivos de esta sección:

1) Controlar el acceso a la información.
2) Prevenir el acceso no autorizado a los sistemas de información.
3) Protección de los servicios de redes.
4) Detectar actividades no autorizadas.
5) Garantizar seguridad con sistemas móviles o portátiles.

Desarrollo y mantenimiento de sistemas

Los objetivos de esta sección son:

1) Garantizar seguridad en los sistemas operacionales.
2) Prevenir perdidas, modificaciones o mal uso de los datos de las aplicaciones.
3) Proteger la confidencialidad, autenticidad e integridad de la información.
4) Garantizar que los proyectos de IT son conducidos de una manera segura.
5) Mantener la seguridad del software y sus respectivos datos.