e-ICEBERG TOOLS

En un entorno tan cambiante como el de las tecnologías de la información, la organización está expuesta a amenazas, que, en caso de materializarse, puede poner en peligro uno de los activos más valorados de la organización: **la información.**

Por ello, es fundamental que las organizaciones evalúen periódicamente los riesgos mediante un análisis de los mismos y un posterior tratamiento o respuesta a estos riesgos, es decir, **la organización tiene que conocer y tratar sus riesgos**, tiene que gestionarlos, de forma que pueda garantizar las tres dimensiones fundamentales de la seguridad de la información: ***confidencialidad***, ***integridad*** y ***disponibilidad***.

La gestión de riesgos ha de realizarse continuamente, de forma sistemática y de manera diligente, para garantizar que se cumplan los objetivos marcados por la organización, y que el uso de las tecnologías de la información no suponga un obstáculo o amenaza para la consecución de estos objetivos de negocio.

La mejor estrategia para una óptima gestión de la seguridad es a través de un sistema que permita mantener, operar, análizar y monitorizar todas las acciones y recursos empleados a la hora de gestionar la seguridad, lo que permitirá de forma cíclica la mejora continua de este proceso.

Debido a la globalización económica, es necesario establecer normas de reconocimiento internacional con el fin de homogeneizar aspectos como la seguridad, la salud o el entorno para las empresas y compañías de todo el mundo y el encargado de ello es la Organización Internacional de Normalización (International Organization for Standardization – ISO).

El cumplimiento de las normativas ISO es voluntario, pero, para poder trabajar de forma eficaz y segura en la era de la digitalización, las empresas deberían cumplir con las estrictas normativas referentes a la seguridad de la Información.

¿Qué es la norma internacional ISO 27001?

Con la norma internacional ISO 27001, una organización puede establecer **estándares para la seguridad de la información**. Se trata de una norma estructurada de manera que ni el tamaño ni el sector de la empresa son relevantes a la hora de ponerla en práctica. Una vez se cumplan las prescripciones, puede pedirse, además, una certificación ISO 27001. Con ella se da a conocer, tanto de cara a los clientes como a los socios comerciales, que se trata de una **organización fiable** y que se toma en serio la seguridad de la información.

e-ICEBERG TOOLS

e-ICEBERG TOOLS es una herramienta para facilitar la implantación y mantenimiento de un sistema de gestión de seguridad de la información (***SGSI***).

La herramienta incluye módulos específicos que permiten atender los diferentes requisitos de seguridad de la información de la organización, independientemente, de si la organización se quiere certificar en ***ISO/IEC 27001***, ya que desde ***Fersoft***, entendemos que no hay mejores prácticas de seguridad para una empresa como las que plantea esta norma ISO.

Con la implantación de un Sistema de Gestión de Seguridad de la Información, la organización consigue garantizar el cumplimiento de los requisitos de seguridad de la información, siguiendo las buenas prácticas marcadas por la norma ISO/IEC 27001, ***sin la necesidad de estar certificado****.*

Reduce tiempos y costos

Minimiza riesgos ya que simplifica la documentación y registros

Ahorre recursos ya que conocerá los riesgos que realmente deberá tratar en su empresa.

Con e-ICEBERG TOOLS podrá llevar la implantación, gestión, mantenimiento y revisión de un Sistema de Gestión de Seguridad de la Información de forma automatizada.

La herramienta está dirigida a:

- A profesionales que realicen implantación y mantenimiento de un SGSI en las organizaciones clientes.
- A organizaciones interesadas en obtener la certificación ISO/IEC 27001 o simplemente cumplir con la norma.
- A organizaciones interesadas en implantar y mantener un Sistema de Gestión de Seguridad de la Información.
- A administraciones públicas interesadas en obtener la declaración de conformidad del ENS soportándose en un Sistema de Gestión de Seguridad de la Información.

MÓDULOS

Gestión de proyectos

Desde la propia herramienta, pueda llevar a cabo una gestión de los proyectos de implantación y mantenimiento de un SGSI, así como la creación de nuevos proyectos en función de las necesidades de la organización.

Organización

Definir el contexto, alcance, roles y responsabilidades de la organización.

Política de seguridad

Repositorio para el marco documental de seguridad de la información de la organización. En él podremos encontrar las plantillas necesarias para organizar un SGSI y un repositorio para subir la documentación una vez aprobada y firmada.

Gestión de riesgos

Gestionar los riesgos que puedan afectar a los activos que la organización utiliza para gestionar la seguridad de la información.

Gestión de incidentes

Registro de los incidentes en la seguridad de la información que pueda ocurrir en la organización.

Competencia

Con el fin de que la organización pueda determinar la competencia necesaria de las personas de la organización, poner en marcha las acciones formativas oportunas y conservar la información relativa, así como registrar las certificaciones que los empleados puedan tener.

Registros

Este módulo se encarga de registrar todas las actividades y acciones realizadas en el SGSI, para que haya evidencias de las mismas.

Evaluación del desempeño

Para registrar la revisión del propio SGSI por parte de dirección, registros de usuarios y registros de auditorías realizadas y medición de la efectividad y eficiencia de los controles implantados.

Beneficios

- Simplificación del proceso de implantación y mantenimiento del SGSI.
- Control y seguimientos de los requisitos de seguridad de la Norma ISO/IEC 27001 y controles ISO 27002 y ENS.
- Gestión de proyectos y tareas para las operaciones del sistema de gestión.
- Acceso a plantillas de políticas y procedimientos para completar el marco documental.
- Aumentar el nivel de madurez de la gestión de la seguridad de la información.
- Mejorar la capacidad de protección, detección, respuesta y recuperación de incidentes.
- Demostración de proactividad y cultura de ciberseguridad
- Mayor grado de confianza y reputación.

Características

- Complete su marco documental de seguridad con el repositorio de plantillas de políticas, procedimientos y normas de seguridad incluidas en la plataforma.

- Gestione las operaciones de seguridad mediante los proyectos maestros que le guiarán durante el proceso de implantación y mantenimiento.

- Analice los riesgos IT desde la propia herramienta a través de su módulo específico basado en la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

- Gestione los riesgos mediante la creación del plan de tratamiento en base al análisis de riesgos y las salvaguardas seleccionadas.

Ventajas

Cuatro ámbitos empresariales diferentes se benefician de esta norma: por un lado, la certificación ISO 27001 es una base para aplicar **requerimientos legales**. Además, aporta una **ventaja competitiva**, ya que no todas las empresas disponen de ella. Las que sí han obtenido dicho certificado pueden **demostrar a sus clientes** que gestionan informaciones delicadas de forma segura. Puesto que, con el cumplimiento de la norma, se **reduce el riesgo de incidentes** en la seguridad de la información, ISO 27001 también permite **reducir costes** al evitar las caras reparaciones de tales incidentes.

Una certificación ISO 27001, además, optimiza los procesos en la empresa. Los tiempos de inactividad de los trabajadores se minimizan gracias a la documentación de los principales procesos empresariales.

Otras ventajas:

- La reducción de los riesgos empresariales.
- La reducción de los riesgos de responsabilidad.
- Primas de seguros más bajas .
- Un reconocimiento fiable de problemas y amenazas.
- Le permitirá diferenciarte de la competencia.
- Protección y continuidad del negocio.
- Desarrollará una adecuada gestión de los riesgos.
- Optimizará recursos e inversión en tecnología.
- Reducirá costes en su empresa.
- Generará credibilidad y confianza entre sus clientes.

¿Quiénes somos?

Fersoft nació hace más de 30 años en el sector de las Nuevas Tecnologías de la Información y de la Comunicación. En la actualidad, ha llegado a expandir su área de actuación hasta lograr una situación estratégica en los sectores productivos, comerciales y asistenciales más diversos a lo largo de toda la geografía nacional.

Enmarcado en una política de innovación continua, ***Fersoft*** invierte en acciones de I+D+i dirigidas a la creación de nuevas líneas de productos y servicios, adaptados a la creciente demanda tecnológica.

El principal objetivo es atender las necesidades del cliente, superando sus expectativas con innovación y dinamismo, y poniendo a su alcance soluciones con alto valor añadido que mejoren sus procesos de gestión y además permitan incrementar sus resultados.

Fersoft centra su filosofía en dos pilares: innovación y calidad.

fer Soft®

+34 957 46 35 47

info@fersoft.es
www.fersoft.es

Calle Noruega, nº8 parcelas 180-181
Pol. Ind. Tecnocórdoba
14014 - Córdoba (España)