

ISO 27001

Certificación de la Gestión de la Seguridad de la Información

Situación Actual

Para la mayoría de las empresas e instituciones, sus sistemas de información son los activos por excelencia, imprescindibles para su propia existencia y supervivencia.

Tanto las pymes como las multinacionales, reconocen el grado de criticidad que los sistemas de información representan para su funcionamiento y supervivencia y el alto grado de vulnerabilidad inherente a la propia naturaleza de estos sistemas. Y lo que es más grave, la insuficiencia de las políticas y normas de seguridad implantadas a la fecha.

Con frecuencia somos testigos y/o víctimas de ataques de virus, de hackers, e incluso de empleados o usuarios maliciosos que acceden a información confidencial y la utilizan de forma perjudicial para la empresa. En muchas ocasiones somos conscientes de los daños causados cuando es demasiado tarde o quizá nunca.

Otras situaciones reflejan retrasos o ineficiencias en los casos de fallos de aplicaciones, ausencias de personal cualificado, sistemas de respaldo incompletos o ineficientes que repercuten en un menor nivel de servicio, costes excesivos o baja rentabilidad.

Situación Deseada

Los Directores desean que sus negocios

funcionen sin interrupción y contar con un grado de riesgo que represente una baja probabilidad de que dichas interrupciones se materialicen. Además quieren que el trabajo que realiza su personal sea eficaz en tiempos y costes. Cada interrupción puede significar una cantidad ingente de dinero que se deja de ingresar, o retrasos en la facturación y/o pérdidas de imagen ante accionistas, inversores, empleados, proveedores o clientes.

La situación deseada es aquella en la que la continuidad del negocio se encuentra dentro de los límites asumibles por la Dirección. El logro de este objetivo lleva consigo una labor de gestión para la mitigación de los riesgos relativos a los sistemas de información que dan vida a la empresa.

Estándares Internacionales

El objetivo de conseguir y mantener la situación deseada tiene un carácter universal. Es decir, puede aplicar a cualquier empresa u organización de cualquier parte del mundo.

Por ello, la Organización ISO ha venido publicando distintas normas hasta la publicación de la Norma ISO 17799 en el año 2005 (ISO 27002), que es un Código de Buenas Prácticas orientadas a reducir los riesgos y a aproximarse a una continuidad del negocio derivada de

la adecuada Gestión de la Seguridad de la Información. Es un marco unificado de control de seguridad interno que recorre toda la compañía, desde la Dirección hasta los activos pasando por la seguridad física, la lógica, el cumplimiento legal, etc.

Sobre la base de la Norma ISO 17799:2005 se aprobó igualmente la Norma ISO 27001, que permite a las empresas certificar su Sistema de Gestión de la Seguridad de la Información (SGSI).

De esta manera, existe una referencia oficial orientada a que los usuarios de los servicios no sufran las consecuencias de la falta de continuidad del servicio de las empresas o instituciones que los ofrecen o de sentir la incertidumbre de si el futuro servicio es fiable o no.

La empresa que ostente este Certificado está diciendo a sus accionistas, clientes, empleados y proveedores que ha tomado y toma medidas preventivas diarias para asegurar la Gestión de la Seguridad de su Información, teniendo en consideración la continuidad de su servicio, a través de uno de los puntos generales de esta Norma, o lo que es lo mismo, para no dejarles en ningún momento desatendidos. Y lo más importante: que se optimizan y aseguran los procesos que generan un servicio con garantías de fiabilidad y de continuidad.

Preparación para la Certificación

La preparación de una empresa o institución para conseguir el certificado de su SGSI es un trabajo de especialistas que requiere amplios conocimientos de organización, gestión de los sistemas de información y de la tecnología actual relativa a la seguridad de la información. Si una empresa o institución está interesada en este Certificado y no dispone de especialistas, la opción más económica, práctica y rápida es contratar una consultora especializada en la Seguridad de la Información para llevar a cabo esta preparación. La función de esta consultora para que la empresa pase la auditoría de la Entidad de Certificación, es similar a la de un taller de automóviles para que un automóvil pase la ITV.

Qué supone implantar un SGSI

Asumir y hacer parte intrínseca de la organización determinados procesos, comportamientos y acciones para mejorar dicha organización.

Establecer y/o reordenar la gestión de la Seguridad de la información de una organización, en concordancia con sus Planes Estratégicos y su negocio.

Una Gestión eficaz de la Seguridad permite garantizar la Confidencialidad, la Integridad y la Disponibilidad de la información.

Se trata de ejercer el control interno sobre nuestros principales activos mediante un ciclo de mejora continua (Plan - Do - Check - Act):

Plan: Definir la política de seguridad. Establecer el alcance del SGSI. Realizar análisis de riesgos. Seleccionar los controles.

Do: Implantar el plan de gestión de riesgos. Implantar el SGSI. Implantar los controles.

Check: Revisar internamente el SGSI. Realizar auditorías internas del SGSI.

Act: Adoptar las acciones correctivas. Adoptar las acciones preventivas.



Fases del proyecto

01. Delimitación del Alcance
02. Análisis de Riesgos
03. Gestión de Riesgos
04. Declaración de Aplicabilidad
05. Políticas y Procedimientos
06. Plan Director de Seguridad
07. Plan de Continuidad de Negocio
08. Plan de Formación
09. Gestión de Incidencias
10. Desarrollo del SGSI
11. Auditoría Interna
12. **Certificación**

Beneficios

• Reducción de aquellos riesgos que, en caso de materializarse las amenazas que les originan, pueden representar

pérdidas ingentes de capital, bien por facturación fallida, por reposición de los daños causados, por pérdida de oportunidad de negocio, por reclamación de clientes, por sanciones legales etc.

• Ahorro de tiempo y dinero al afrontar y corregir situaciones nefastas antes de que ocurran y nos obliguen a resolverlas con prisas y a cualquier precio.

• Mejora de la imagen y revalorización de la confianza en la empresa de los accionistas, inversores, empleados, proveedores y clientes al mostrarles que se toman medidas diarias para garantizar la continuidad del negocio.

Sobre ESA Security

ESA Security es una consultora especializada únicamente en la Seguridad de la Información que ha realizado con éxito la preparación de empresas para que consigan su Certificación ISO 27001, además de haber obtenido su propia certificación en gestión de Seguridad de la Información.

Sus profesionales están altamente cualificados, incluyendo certificaciones CISA y CISM, y lo más importante: con la experiencia práctica de haber conseguido Certificaciones ISO y haber realizado en múltiples ocasiones Planes Directores de Seguridad, Planes de Continuidad de Negocio, Análisis y Gestión de Riesgos, Proyectos de Hacking Ético, Formación en Seguridad, Adecuaciones y Auditorías LOPD y servicios relativos a la Seguridad de la Información en general.