ISO 27001:2005

Introducción

La tendencia hacia un mercado global y sus correspondientes desafíos hace que muchas organizaciones, especialmente sus sistemas de información y redes de trabajo, se vean enfrentadas a continuas amenazas de seguridad.

Proteger la información no basta, las empresas buscan desarrollar su actividad empresarial de la manera más segura posible y, a la vez, explotar su información con el objetivo de crecer en el mercado y ser una empresa competitiva.

Uno de los mayores desafíos de las empresas actuales (independientemente de su tamaño o sector) es la implantación de Sistemas de Gestión de Seguridad de la Información (SGSI´s) que garantice que el principal activo de cualquier empresa, la INFORMACIÓN, se encuentra protegido.

La certificación bajo la norma ISO 27001 garantiza que una empresa tiene implantado un SGSI y refuerza su imagen de marca.

ISO 27001

La ISO 27001 es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información, siendo la norma de referencia en este ámbito, que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información.

Esta norma desarrolla un modelo para el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información en cualquier tipo de organización.

El objetivo es la seguridad de la información, preservando su confidencialidad, integridad y disponibilidad, así como todo lo relacionado con su tratamiento.

ISO 27001

La definición de procedimientos y controles es uno de los factores fundamentales a la hora de establecer un SGSI, podemos decir que los pilares básicos sobre los que se apoya la norma ISO 27001 son:

- Establecimiento de una política, un alcance y unos objetivos para la seguridad de la información.
- Elaboración de un análisis de riesgos proporcionado a la naturaleza y valoración de los activos y de los riesgos a los que los activos están expuestos.
- Selección de los controles adecuados, de acuerdo con los objetivos que se pretenden obtener con los mismos, justificando la selección.
- Seguimiento y revisión de la eficiencia del SGSI.
- Mejora continua.

ISO 27001- LOPD

La implantación de un Sistema de Seguridad de Sistemas de la Información garantiza la fiabilidad de la información y de los sistemas de la información, la confidencialidad, la integridad y disponibilidad de la información, todo ello es fundamental para el mantenimiento de la competitividad, la liquidez, la rentabilidad y la imagen comercial de las organizaciones.

Cuando una empresa ha implantado la norma ISO 27001, le resulta degran ayuda para el cumplimiento de la LOPD.

Con la implantación de un SGSI se mejora la gestión a nivel corporativo y aumenta la garantía para las partes interesadas, tales como inversores, clientes, consumidores y proveedores.

ISO 27001- LOPD

La Ley Orgánica de Protección de Datos (LOPD) tiene como principal finalidad **proteger derechos fundamentales de las personas,** como son el derecho al honor, la intimidad personal y la propia imagen

Por lo tanto la LOPD, con el objeto de garantizar los derechos indicados, limita y regula el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal, así como la información en soporte Documental (papel). La LOPD se aprobó el 13 de diciembre de 1999 y está vigente desde el 14 de enero de 2000.

Toda empresa o autónomo que tenga y trate datos de carácter personal, ya sea en un sistema informático o en soporte papel, está obligada al cumplimiento de la LOPD.

Fases para implantar la ISO 27001

ETAPA 1
IMPLANTACIÓN SGSI

En esta fase la empresa debe centrarse en el desarrollo e implementación de un plan efectivo a medio y largo plazo que evite o atenúe los posibles riesgos para la seguridad de la información.

En esta fase, se iniciará también la formación e información del personal de la empresa, de forma que se garantice la correcta implementación del SGSI.

En esta fase la empresa suele ayudarse de una consultora

Fases para implantar la ISO 27001

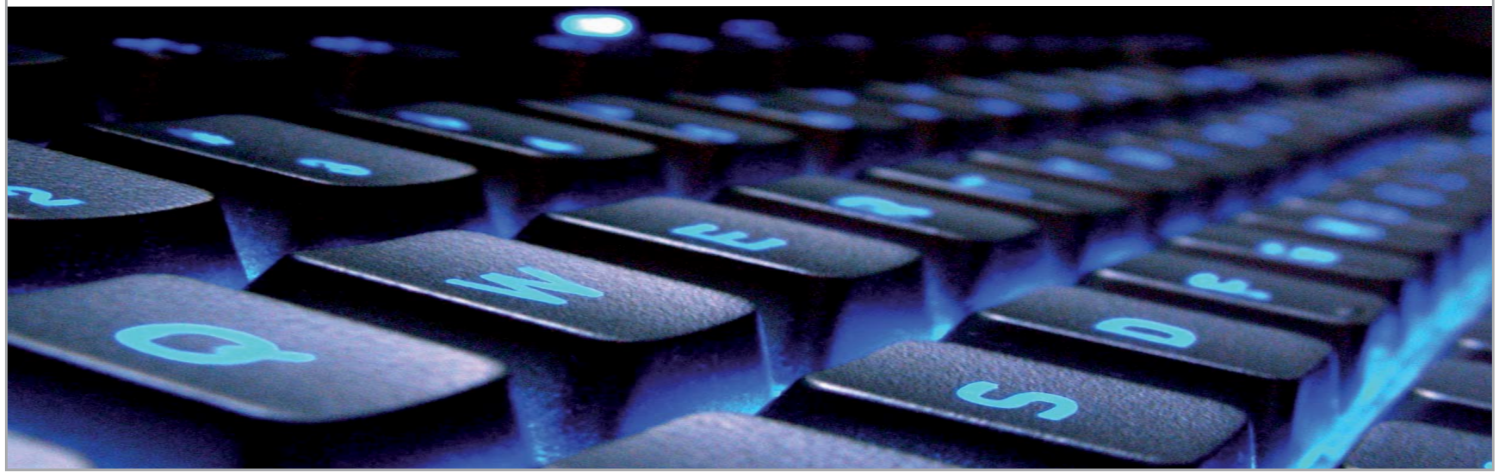
ETAPA 2
CERTIFICACIÓN DE LA NORMA ISO 27001:2007

Cuando la empresa considera que su implantación esta lista para pasar la auditoria, la entidad de certificación, como es EQA, verifica que la empresa cumple con todos los requisitos de la norma ISO 27001:2007.

Un auditor de EQA, experto en el sector de la empresa, revisa el funcionamiento de la empresa. En caso de que el auditor observe diferencias, estas deberán ser corregidas por la empresa antes de que la entidad de certificación pueda emitir el certificado.

Los sistemas de gestión, una vez certificados, deben pasar una revisión anual y someterse a una auditoria de renovación al tercer año.

Esta fase la realiza una entidad de certificación, como es EQA



Fases para implantar la ISO 27001

ETAPA 2
CERTIFICACIÓN DE LA NORMA ISO 27001:2007

Fases de la certificación

Certifiación del Sistema de Gestión

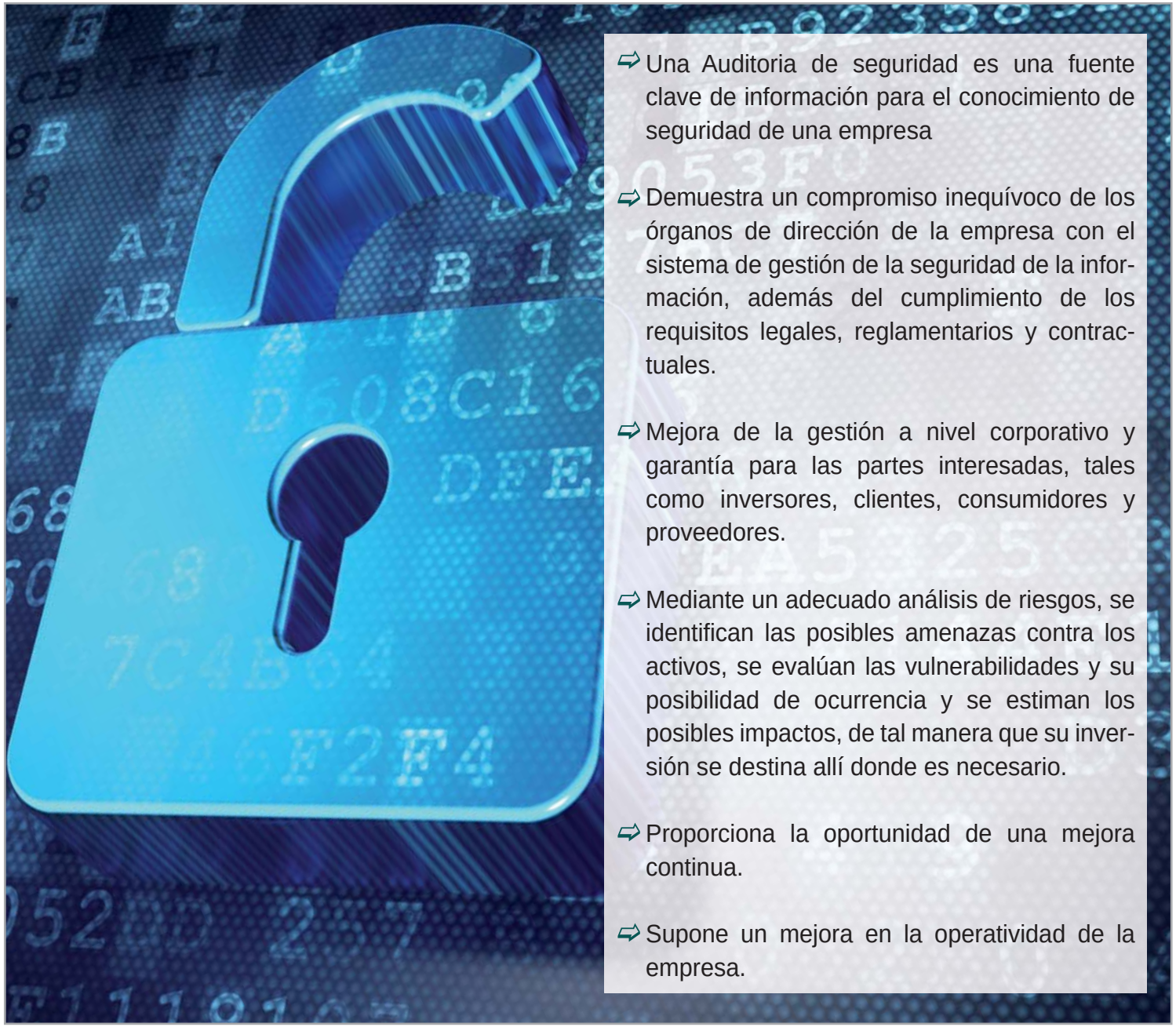
Certificación Inicial

Planificación ➤ Fase 1 ➤ Fase 2 ➤ Emisión Certificado

Mantenimiento del Certificado

Seguimiento Anual 1 ➤ Seguimiento Anual 2 ➤ Recertificación

Beneficios de la norma ISO 27001



- Una Auditoria de seguridad es una fuente clave de información para el conocimiento de seguridad de una empresa
- Demuestra un compromiso inequívoco de los órganos de dirección de la empresa con el sistema de gestión de la seguridad de la información, además del cumplimiento de los requisitos legales, reglamentarios y contractuales.
- Mejora de la gestión a nivel corporativo y garantía para las partes interesadas, tales como inversores, clientes, consumidores y proveedores.
- Mediante un adecuado análisis de riesgos, se identifican las posibles amenazas contra los activos, se evalúan las vulnerabilidades y su posibilidad de ocurrencia y se estiman los posibles impactos, de tal manera que su inversión se destina allí donde es necesario.
- Proporciona la oportunidad de una mejora continua.
- Supone un mejora en la operatividad de la empresa.

Certificación ISO 27001

La organización que ha superado satisfactoriamente su proceso de auditoría y certificación demuestra poseer un Sistema de Gestión de Seguridad de la Información de acuerdo con esta norma, lo que implica una mayor confianza de clientes y proveedores y de la sociedad en general.

EQA

ISO 27001

EMPRESA CERTIFICADA

EQA

Contacto

Camino de la Zarzuela, 15 | Bloque 2, 1ª Planta | 28023 Madrid

902 44 9001 · +34 91 307 86 48 | Fax: 91 357 40 28

www.eqa.es | info@eqa.es

Andalucía | Cataluña | C. Valenciana | Galicia | Madrid