



HISPASEC SISTEMAS

Seguridad y Tecnologías de la Información



Gestión de la seguridad de la Información según **ISO 27001**

L.O.P.D.

GESTIÓN DE LA SEGURIDAD ISO 27001

Los sistemas de Gestión de la Seguridad de la Información según ISO 27001 permiten aplicar una norma global de seguridad a su organización.

FASES



DESCRIPCIÓN

Inicio del proyecto

Aprenda cómo afrontar el proyecto de implementación ISO 27001 y los requisitos primordiales: compromiso de la dirección, selección del personal que afrontará en primera instancia el proyecto y campaña de sensibilización inicial. En esta fase se procederá a la recolección inicial de datos para plantear el sistema.

Diagnosis

Con los datos recopilados, se procede a realizar una diagnosis inicial de la empresa en materia de seguridad. Se realizará un informe completo de situación basado en los diez puntos de control de la norma ISO 27001.

Definición del SGSI

En la definición del sistema de gestión de la seguridad de la información (SGSI) se establece el alcance del sistema, así como sus limitaciones, una vez conocida la situación inicial de la empresa.

DESCRIPCIÓN

Diseño del SGSI

En esta etapa se unifican los puntos anteriores. Se elaborarán las políticas de seguridad, el manual de seguridad, los procedimientos e instrucciones de trabajo.

Gestión del Riesgo

La gestión del riesgo es crucial en un SGSI. Comprenda qué riesgos están presentes en su organización, qué implicaciones tienen, cuál es la frecuencia de aparición y el impacto de los mismos. Aprenda a equilibrar los costes de minimización con las tasas de ocurrencia.

La implementación de controles y la correcta aplicación de activos repercutirá en la adopción de un adecuado nivel de riesgo, compatible con el normal desenvolvimiento de la organización y el coste de las operaciones.

Formación. Recursos humanos

Los SGSI requieren la participación de los recursos humanos. Entienda las debilidades que pueden suponer en la cadena del sistema. Conozca las maneras más eficientes de implicar a los recursos humanos y evitar problemas por el desconocimiento de las medidas. En esta fase se pretende diseminar el concepto de seguridad de la información a todos los estamentos implicados, profundizando en el conocimiento que deben tener para mantener del modo más elevado los estándares de seguridad.

Seguimiento

Una vez definido el sistema y puesto en marcha, tras un período de consolidación, se procede a la revisión del mismo, confrontando estos datos con la situación inicial, buscando de un modo comparativo las mejoras y los puntos donde deben emplearse acciones de mejora.

Mejora continua. Auditorías de control.

Los sistemas de esta índole deben estar en constante revisión y por tanto es necesario mantener controles que permitan evaluar el rendimiento del mismo. Esto se logra con las auditorías, cuya periodicidad será establecida según las necesidades y complejidad del sistema.

Hispacec Sistemas S.L.

Avda Juan López Peñalver 17
Edificio Centro de Empresas CEPTA
Parque Tecnológico de Andalucía
29590 Campanillas (Málaga)

Telf: (+34) 902 161 025

Fax: (+34) 952 028 694

Información General

info@hispacec.com

Comercial

comercial@hispacec.com

www.hispacec.com