



GRUPO ACMS Consultores

Cómo crear un Plan Director de Seguridad efectivo



(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.



(SI-0021/2020)

Índice de Contenidos

- 1. ¿Qué es el Plan Director de Seguridad?
- 2. Beneficios de la implantación del Plan Director
- 3. Plan Director de Seguridad: Guía para su implementación
- 4. Consultoría Seguridad de la Información

1. ¿Qué es el Plan Director de Seguridad?

El plan director de seguridad conforme a la norma ISO 27032 es una herramienta que se utiliza para realizar una planificación de las actividades que se tendrán que llevar a cabo para proteger y mejorar la seguridad digital de la empresa.

Implementar un Plan Director de Seguridad ayudará a la empresa a proteger la información y a prevenir robos, filtraciones, pérdidas o modificaciones de información valiosa.

Los riesgos y amenazas se podrán evaluar y será posible establecer medidas para reducirlos. Además, el Plan Director de Seguridad fomentará una cultura de seguridad en la empresa, concienciando a los trabajadores sobre la importancia de la seguridad de la información y su rol en la protección.

Para determinar el nivel de seguridad que desea la empresa, se tiene que responder a varias preguntas para concretar el objetivo y las medidas a seguir. Debemos conocer, por tanto, que es exactamente lo que se quiere proteger, hacer un listado de posibles incidentes que podrían ocurrir, saber cómo se realizará la prevención y cómo se reaccionará ante el riesgo.

Dicha planificación recogerá las prioridades que se hayan determinado, los nombres de los responsables, el total de recursos que se va a utilizar y los proyectos legales, técnicos y organizativos.

Es importante que cuando definamos el alcance del Plan (PDS) determinemos los activos y procesos de negocio críticos, para que la protección sea máxima sobre la seguridad de la información en la empresa.

Definir correctamente los objetivos en materia de ciberseguridad ayudará a identificar y mejorar las áreas más vulnerable, de nuestro negocio, que podrían ser atacadas.

2. Beneficios del Plan Director de Seguridad

Disponer de un Plan Director conforme a la norma ISO 27032 ofrece a las organizaciones una guía de procedimientos y políticas para proteger los activos y la información crítica.

El periodo de vigencia del Plan suele ser de entre 2 y 4 años y se puede utilizar un calendario de inversiones que esté relacionado con una tendencia de reducción de riesgos y de los costes procedentes de ellos.

Dado que se basa en la mejora continua, una vez implementado es necesario iniciar de nuevo el proceso, ya que siempre hay un margen de mejora.

3. Plan Director de Seguridad: Guía para su implementación

Detallamos a continuación las fases necesarias para realizar una correcta implementación del Plan Director:

- Antes de iniciar el Plan se tiene que tener documentación detallada de la situación de la empresa.
- Conocimiento de la estrategia que está siguiendo la organización
- Tener el Informe de análisis de riesgos
- Determinación de las iniciativas y del proyecto en sí.
- Clasificación y Priorización
- Aprobación por la Dirección
- Implementación

4. Consultoría Seguridad de la Información

Grupo ACMS Consultores puede asesorarle sobre el Plan Director a corto, medio y largo plazo en detalle.

Si desea implantar Sistemas de Seguridad de la información bajo la Norma ISO 27001 podemos asesorarle. Rellene el formulario de contacto y nos pondremos en contacto con su organización.

5. Contenidos relacionados

NORMA ISO 27032

ISO 33000

ISO 27001

RGPD

LOPDGDD

INCIBE

ISO 20000



Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com