¿Cómo se puede implantar la 27001?

RESUMEN: Os vamos a mostrar cuáles son los pasos para implantar la 27001, después de hacer el estudio inicial de la empresa.

CATEGORÍAS: CIBERSEGURIDAD

Nº HIPERVINCULOS: 1

Para implantar la 27001 previamente se debe hacer un estudio inicial de la empresa y a partir de ese momento, seguir los siguientes pasos:

1. Definir los objetivos y redactar una política de seguridad

Antes de empezar cada negocio debe tener muy bien definidos todos sus objetivos y señalar cuáles son las expectativas que debe cumplir en cada momento, para poder obtener la certificación.
Dentro de esos objetivos se encuentran: las metas de seguridad de la información, definir el alcance, los requisitos legales que se deben cumplir, la metodología de evaluación de riesgos, las posibles amenazas, los puntos débiles de la empresa y definir la política de seguridad.

2. Definir los riesgos

Una vez tenemos ya pensada una Política de Seguridad, el siguiente paso que debemos dar será identificar los riesgos a los que se puede enfrentar la empresa, quién se encargará de gestionarlos y cuáles son las vulnerabilidades.

3. Evaluar y analizar los riesgos

Una vez se han identificado los riesgos a los que se expone la empresa, se debe analizar el impacto que podrían generar dichas amenazas sobre la empresa y con cuánta frecuencia podrían producirse.
Y a continuación, se debe realizar un tratamiento de riesgos, es decir, ver qué riesgos se pueden reducir y eliminar. De la misma forma, debemos buscar cuáles serán los métodos para gestionar dichos riesgos en caso de que ocurran. Durante esta fase del proceso, es ideal contar con un servicio de auditoría que te ofrezca servicios de control y supervisión que cuenten con una mirada experta.

4. Realizar la declaración de la aplicabilidad

Una vez ya se ha realizado el tratamiento de riesgos, se deben definir los objetivos de control, ver cuáles se pueden aplicar y cuáles no, cómo se hará y por qué se hará. Todo esto deberá quedar recogido en un documento llamado "Declaración de Aplicabilidad".

5. Poner en marcha la implementación del sistema de gestión de seguridad de la información

Una vez que se ha pasado la fase de planificación, es el momento de implementar el **SGSI,** y, por tanto, el plan de tratamiento del riesgo previsto. Se deberán introducir nuevas tecnologías y prácticas que ayuden a alcanzar los objetivos marcados y realizar controles de seguridad.

6. Capacitación y concienciación

En este paso, es primordial la formación del personal en cuanto a las nuevas tecnologías aplicadas y los nuevos protocolos que se hayan establecido. La puesta en marcha no se podrá llevar a cabo correctamente si no se forma a los empleados para que puedan actuar siguiendo las nuevas medidas impuestas.

7. Monitoreo

Es importante que, antes de obtener la certificación, se controle y revise cómo funciona el sistema y si está permitiendo que se alcancen los objetivos establecidos.