**Actividad Evaluable 1. ISO 22301**



Daniel Escaño Hernández CET Ciberseguridad

# **1. Índice**

[**1. Índice**](#_u3m2w22qmzkq) **1**

[**2. Cuestiones**](#_kfo1iwg0dqcu) **2**

[**2.1 ¿Puede describir brevemente requerimientos de ISO 27001 e ISO 22301?**](#_bcwoq23ur7dq) **2**

[**2.1.1 ¿Cuáles son las fases de la implementación ?**](#_esel7s8x6gh1) **2**

[**2.1.2 ¿Cuál es la mínima documentación que se necesita desarrollar?**](#_y2x8amsibazr) **2**

[**2.2 ¿Cuáles son los problemas más comunes que ha encontrado en los proyectos de implementación de ISO 27001 y cuál fue su enfoque para resolverlos?**](#_7zq1tsqzgcib) **3**

[**2.3 ¿Cuál es la longitud habitual de un proyecto de implementación? ¿De qué depende?**](#_29xe7xx0168z) **3**

[**2.4 ¿Cómo definiría el alcance del proyecto?**](#_y7m9p8dwk1nm) **3**

[**2.5 ¿Qué sugiere en relación a definir responsabilidades para ejecutar tareas específicas en el proyecto?**](#_gmtk3y3e2cs) **4**

# **2. Cuestiones**

## **2.1 ¿Puede describir brevemente requerimientos de ISO 27001 e ISO 22301?**

-Desarrollar un Sistema de Gestión de la Seguridad de la Información de acuerdo a la norma ISO-27001.

-Recoger evidencias documentales de los procedimientos desarrollados, así como los registros asociados.

-Definir y comunicar una política de seguridad de la información.

-Desarrollar objetivos orientados a la mejora continua del sistema.

-Asegurar el compromiso de la dirección.

-Designar un responsable del Sistema de Gestión De la Seguridad de la Información.

-Realizar una evaluación de riesgos de seguridad de la información.

-Llevar a cabo un proceso de tratamiento de los riesgos.

### **2.1.1 ¿Cuáles son las fases de la implementación ?**

-Analizar el contexto de la organización y definir un alcance.

-Designar una persona o equipo de personas que se encargue de la implantación y mantenimiento del Sistema de Gestión de la Seguridad de la Información.

-Establecer y comunicar una política de seguridad de la información.

-Realizar un análisis de riesgos, definiendo las amenazas y vulnerabilidades oportunas.

-Realizar la formación y concienciación de los trabajadores.

-Desarrollar un Sistema de Gestión de la Seguridad de la Información.

-Documentar todos aquellos requisitos exigidos por la norma.

-Poner en funcionamiento el Sistema de Gestión.

-Realizar la auditoría interna.

-Revisión por la Dirección.

-Solicitar la auditoría de certificación.

### **2.1.2 ¿Cuál es la mínima documentación que se necesita desarrollar?**

-Alcance

-Política de seguridad de la información

-Proceso de evaluación de riesgos para la seguridad de la información

-Proceso de tratamiento de riesgos de seguridad de la información

-Declaración de aplicabilidad

-Los objetivos de seguridad de la información

-Evidencia de la competencia

-Los resultados de las evaluaciones de riesgos realizadas

-Los resultados el tratamiento de la información de riesgos de seguridad

-La evidencia de la de la monitorización de la información de desempeño de seguridad y los resultados de medición

-Programa de auditoría interna y los resultados de la auditoría

-Procedimiento de auditoría interna

-La evidencia de todos los resultados de las revisiones por la dirección

-La evidencia de la naturaleza de las no conformidades y de cualquier acción tomada posteriormente, y los resultados de cualquier acción correctiva

## **2.2 ¿Cuáles son los problemas más comunes que ha encontrado en los proyectos de implementación de ISO 27001 y cuál fue su enfoque para resolverlos?**

Cumplimiento del marco regulatorio y de otros requisitos legales: Así, esta norma permite identificar cuáles son estos requerimientos y posteriormente, definir cómo realizar el cumplimiento sistematizado de la misma.

Incidentes de seguridad: se integran en un mismo sistema de gestión.

Reducir costos originados por los incidentes de seguridad: En primer lugar, dispone de determinados apartados para la alta dirección, como por ejemplo en qué forma involucrarse en la seguridad de la información y qué información tiene que recibir.Y en segundo lugar, incluye un lenguaje de negocios, que facilitará a los responsables del sistema de gestión el trabajo frente a los altos cargos.

## **2.3 ¿Cuál es la longitud habitual de un proyecto de implementación? ¿De qué depende?**

De 1 a 2 años, depende de varios factores, la extensión de la empresa, número de empleados, políticas internas, etc…

## **2.4 ¿Cómo definiría el alcance del proyecto?**

El alcance de un proyecto es el conjunto de procesos necesarios para dar por finalizado el proyecto. En este sentido, procesos como su diseño, ejecución y control. El alcance está establecido por los interesados en el proyecto

## **2.5 ¿Qué sugiere en relación a definir responsabilidades para ejecutar tareas específicas en el proyecto?**

-Determina qué debe hacerse

-Identifica brechas en las responsabilidades

-Especifica los roles con una matriz

-Pide comentarios a los miembros del equipo