

Simulacro de Examen - Normativa de Ciberseguridad

**Selecciona la opción correcta para cada una de las siguientes preguntas. Solo hay una respuesta válida por pregunta.**

1. **¿Qué es el cumplimiento normativo o compliance penal?**

A) Programas para mejorar la productividad

B) Herramienta para el control de inventarios

C) Modelos para eximir de responsabilidad penal

D) Normativa para la protección de datos

1. **¿Cuál es una de las condiciones para la exención de responsabilidad penal de una persona jurídica?**

A) Supervisión deficiente

B) Adopción de modelos de organización eficaces

C) Omisión de medidas de seguridad

D) Desconocimiento de la normativa

1. **¿Qué papel cumple la OCDE en el cumplimiento normativo de las empresas?**

A) Aumentar los beneficios

B) Reducir el personal

C) Proporcionar principios de gobierno corporativo

D) Facilitar el fraude empresarial

1. **¿Qué establece la Ley 10/2010 de Prevención del Blanqueo de Capitales?**

A) Marco para la publicidad

B) Define el salario mínimo

C) Obliga a contratar seguros

D) Obligaciones para sujetos obligados

1. **¿Qué objetivo tienen los códigos éticos empresariales?**

A) Aumentar la producción

B) Regular la conducta empresarial

C) Establecer sanciones económicas

D) Incentivar la competencia desleal

1. **¿Cuál es la función principal de un compliance officer?**

A) Ejecutar todas las operaciones

B) Supervisar el cumplimiento normativo

C) Realizar auditorías financieras

D) Asegurar el rendimiento laboral

1. **¿Qué característica esencial debe tener un compliance officer?**

A) Independencia en sus funciones

B) Capacidad de supervisión general

C) Experiencia en ventas

D) Habilidad en marketing

1. **¿Qué implica la fase de detección en las funciones del compliance officer?**

A) Crear nuevos departamentos

B) Incrementar las ventas

C) Supervisión continua de riesgos

D) Establecer metas financieras

1. **¿Cuál es la responsabilidad penal del compliance officer según el art. 31 bis?**

A) No tiene responsabilidad legal

B) Responsable si actúa en nombre de la persona jurídica

C) Responsable solo en caso de fraude

D) Solo responsable en grandes empresas

1. **¿Qué fases componen las funciones del compliance officer?**

A) Prevenir, detectar e informar

B) Evaluar, seleccionar y contratar

C) Analizar, verificar y despedir

D) Planificar, ejecutar y concluir

1. **¿Qué establece la ISO 31000:2018 en la evaluación de riesgos?**

A) Evaluación sistemática y colaborativa

B) Evaluación informal del riesgo

C) Revisión opcional del riesgo

D) Análisis parcial de riesgos

1. **¿Qué tipo de riesgos se incluyen en un mapa de riesgos de compliance?**

A) Solo financieros

B) Solo operativos

C) Penales, operativos y financieros

D) Solo penales

1. **¿Qué herramienta se utiliza para evaluar riesgos en ciberseguridad?**

A) Photoshop

B) GIMP

C) Metasploit

D) ISO 31000

1. **¿Qué normativa se aplica para la protección de datos personales en España?**

A) LOPDGDD

B) ISO 27001

C) NIST

D) GDPR

1. **¿Qué regula la Ley Orgánica 3/2018 en España?**

A) Mejora de procesos empresariales

B) Auditoría financiera

C) Gestión de inventarios

D) Protección de datos personales

1. **¿Qué función cumple el delegado de protección de datos?**

A) Asesorar y supervisar el cumplimiento de la normativa

B) Automatizar procesos financieros

C) Desarrollar software

D) Crear políticas de ventas

1. **¿Qué principio garantiza la interoperabilidad en el acceso electrónico?**

A) Neutralidad

B) Proporcionalidad

C) Adaptabilidad

D) Facilidad

1. **¿Cuál es el objetivo del Esquema Nacional de Seguridad (ENS)?**

A) Optimizar la velocidad del sistema

B) Garantizar la seguridad

C) Incrementar la eficiencia

D) Facilitar la instalación de software

1. **¿Cuál de los siguientes es un beneficio de la ISO 22301?**

A) Mejora de la ciberseguridad

B) Reducción de la memoria del sistema

C) Eliminación de archivos

D) Aceleración de procesos

1. **¿Qué regula la Ley PIC en relación con la Directiva NIS?**

A) Solo servicios digitales

B) Infraestructuras críticas

C) Comercio electrónico

D) Ciberseguridad en redes sociales

1. **¿Qué debe incluir un Plan de Seguridad del Operador (PSO)?**

A) Mejora del rendimiento del sistema

B) Política general y marco de gobierno

C) Eliminación automática de virus

D) Configuración remota de dispositivos

1. **¿Qué ley regula el acceso electrónico a servicios públicos en España?**

A) Ley 45/2018

B) Ley 39/2015

C) Ley 32/2020

D) Ley 50/2016

1. **¿Qué se requiere para las comunicaciones electrónicas seguras?**

A) Certificados reconocidos

B) Antivirus

C) Contraseñas simples

D) Redes VPN

1. **¿Qué establece el Real Decreto 43/2021?**

A) Mejora de la velocidad de internet

B) Designación de un responsable

C) Eliminación de malware

D) Actualización de software

# Caso Práctico: Incumplimiento normativo en una entidad pública

**Durante una auditoría interna en una entidad pública que gestiona datos sensibles, se detecta que no se han implementado correctamente las políticas exigidas por la Ley Orgánica 3/2018, ni se ha designado formalmente un Delegado de Protección de Datos (DPD). Además, la entidad no ha notificado ciertos incidentes al CCN-CERT y carece de un Plan de Seguridad del Operador (PSO) actualizado. El informe también refleja que no se está aplicando el Esquema Nacional de Seguridad (ENS) en sus procesos tecnológicos. Como consecuencia, se inician medidas correctivas y se contacta con el organismo competente para evitar sanciones administrativas.**

1. **¿Qué normativa se ha incumplido por no designar un DPD?**

A) Ley PIC

B) ISO 27001

C) GDPR

D) Ley Orgánica 3/2018

1. **¿Qué organismo debe recibir la notificación de los incidentes detectados?**

A) AEPD

B) INCIBE

C) CCN-CERT

D) RedIRIS

1. **¿Qué documento es obligatorio y estaba ausente según el caso?**

A) Plan de recuperación ante desastres

B) Plan de continuidad de negocio

C) Plan de Seguridad del Operador (PSO)

D) Plan de formación de usuarios

1. **¿Qué marco regulador se aplica a los sistemas tecnológicos de la entidad pública?**

A) ENS

B) ISO 22301

C) LOPDGDD

D) NIS 2

1. **¿Qué acción es prioritaria tras identificar estos incumplimientos?**

A) Notificar en redes sociales

B) Revisar los perfiles de redes sociales del DPD

C) Aplicar medidas correctivas y actualizar políticas

D) Incrementar la publicidad institucional

1. **¿Qué principio de seguridad se ha vulnerado al no aplicar el ENS correctamente?**

A) Interoperabilidad

B) Disponibilidad

C) Integridad

D) Confidencialidad