Preguntas clave para evaluar el estado de la ciberseguridad

Guía de supervisión de ciberseguridad para directivos no técnicos

1 ¿Se ha aprobado un plan?

SABER CÓMO ACTUAR ANTE UN INCIDENTE

Tener un **plan de respuesta** . Sin este plan (y comprobando que funcione) cualquier ataque puede tener consecuencias mucho más graves.

2 ¿Qué datos tenemos y dónde están?

PROTEGER LO MÁS VALIOSO

Saber qué datos tenemos y dónde con un **inventario** actualizado de la información y su ubicación.

3 ¿Hacemos pruebas prácticas?

REVISAR PARA MEJORAR

La seguridad hay que revisarla cada cierto tiempo. **Simular ataques** o situaciones de riesgo es útil para ver cómo responde el equipo y detectar puntos débiles.

4 ¿Quién accede a qué?

CONTROLAR LOS ACCESOS

No todo el mundo necesita ver todo. Cada persona debe tener **acceso sólo a lo necesario** para su trabajo. Es necesario tener los permisos actualizados.

5 ¿Funciona la formación?

FORMAR EQUIPO

La formación ayuda a evitar errores, reconocer amenazas y actuar con rapidez. Enviar **pruebas controladas** ayuda a saber si el equipo está atento y preparado.

6 ¿Cuánto tardamos en detectar un problema?

SUPERVISAR LA ACTIVIDAD

El **tiempo de reacción** es clave. Detectar y resolver incidentes rápidamente reduce el impacto.

7 ¿Tenemos acuerdos claros con proveedores?

COLABORAR DE FORMA SEGURA

Los **contratos** deben establecer responsabilidades y cómo actuar en caso de incidente.

8 ¿Funcionan las copias de seguridad?

RECUPERARSE TRAS UN INCIDENTE

Es fundamental realizar **copias de seguridad** de manera periódica para no perder información de producción, y comprobar que los datos se pueden recuperar.

9 ¿Conocemos los nuevos reglamentos y normativas?

CUMPLIR CON LA NORMATIVA

Las **leyes** cambian, y cada sector tiene sus propias obligaciones. Estar al día evita sanciones y protege la reputación.

10 ¿Comunicamos bien a la dirección?

MEDIR EL PROGRESO

Sin **indicadores**, no se puede saber si las cosas mejoran. Número de incidentes, tiempo de respuesta o nivel de formación del personal son buenas métricas.

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD