

CIBERSEGURIDAD Y AUDITORÍAS DIGITALES

¿CÓMO PROTEGER LA INFORMACIÓN
DURANTE UNA AUDITORÍA?



¿Qué es una auditoría digital?

Una auditoría digital utiliza tecnologías para planificar, ejecutar y dar seguimiento a una auditoría, permitiendo el intercambio de información y evidencias de forma electrónica o mediante métodos remotos.

¿Por qué la ciberseguridad es importante?

Durante una auditoría se comparte información sensible, por ejemplo:

Procedimientos y políticas

Registros e indicadores

Datos de colaboradores

Información financiera

Evidencia de cumplimiento

**Proteger esta
información es
fundamental para
preservar su:**



Confidencialidad



Integridad



Disponibilidad



Riesgos en una auditoría digital

Accesos no autorizados

Robo o pérdida de información

Enlaces o archivos maliciosos

Uso de plataformas inseguras

Manipulación o alteración de evidencias

Fuga de información confidencial

Buenas prácticas para auditorías digitales

Antes de la auditoría

- ✓ Definir la plataforma a utilizar
- ✓ Verificar permisos de acceso
- ✓ Establecer responsables del manejo de la información

Durante la auditoría

- ✓ Compartir documentos por canales autorizados
- ✓ Utilizar autenticación multifactor cuando sea posible
- ✓ Verificar la identidad de los participantes
- ✓ Limitar el acceso únicamente a la información necesaria

Después de la auditoría

- ✓ Eliminar accesos temporales
- ✓ Resguardar la evidencia de auditoría
- ✓ Proteger los registros conforme a las políticas de la organización
- ✓ Revisar incidentes o vulnerabilidades detectadas

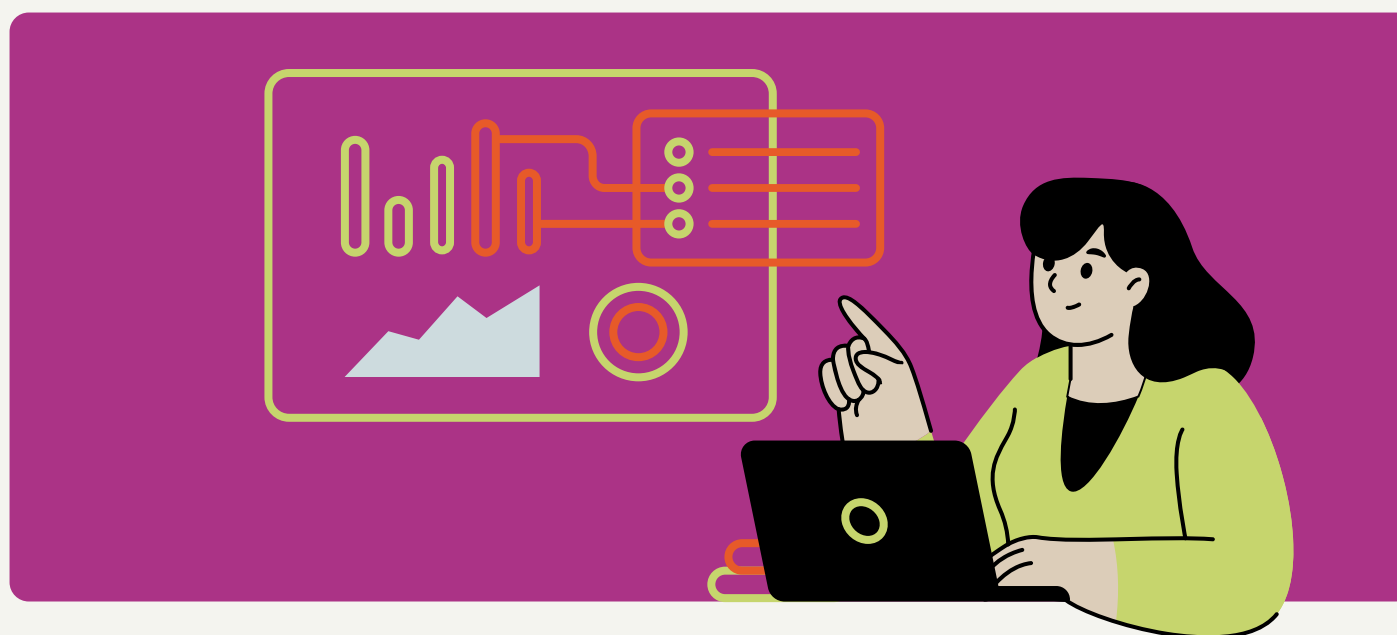
¿Qué normas apoyan este proceso?

ISO 19011

ISO/TS 17012

ISO/IEC 27001

ISO/IEC 42001



Referencias: NIST. *Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. 2024.

ENISA. *Guidelines on Security Measures for Digital Environments*. European Union Agency for Cybersecurity. 2023.



globalstd.com