

Auditorías de Seguridade



Laboratorio
de Seguridade
da Información

Unha Auditoría de Seguridade da Información é o proceso para verificar e asegurar que os recursos e procesos involucrados nos sistemas de información cumpren cos procedementos establecidos e se axustan a criterios de integridade, eficiencia, seguridade, efectividade e legalidade.

Os auditores sustentan o seu traballo en normas e principios internacionais que á súa vez apoian con procesos, estándares e boas prácticas.

Os **aspectos clave** para a súa execución dun **proceso de auditoría**, baseado nas normas e estándares de ISACA son:

- **Planificación:** desenvolver un Plan de auditoría no que se detalle a natureza e obxectivos da auditoría, os prazos, alcance e recursos requiridos.
- **Avaliación de riscos:** examinar unidades auditables e seleccionar áreas que teñan maior exposición a riscos e incluílas no programa de auditoría.
- **Evidencias de auditoría:** información que obtén o auditor para extraer conclusións nas cales sustenta as súas opinións. A conclusión dunha auditoría debe estar baseada en evidencias suficientes e apropiadas para chegar a conclusións razoables.
- **Informe de auditoría:** documento para informar das observacións e recomendacións á xerencia, inclúe todos os aspectos relacionados co traballo levado a cabo.

Todo o proceso de auditoría vaise deseñando e recollendo no chamado Programa de Auditoría.

Detalle do Programa de Auditoría:

Suxeito da auditoría

- Identificar a área a auditar

Obxecto da auditoría

- Identificar o propósito da Auditoría

Alcance

- Identificar os sistemas específicos, a función ou unidade a ser incluída na revisión

Planificación

- Identificar as habilidades e recursos técnicos necesarios
- Identificar as fontes de información a revisar
- Identificar a localización das instalacións a auditar

Avaliación de riscos

- Seleccionar as áreas con maior exposición a riscos e incluílas no programa de auditoría

Procedementos para a recollida de datos

- Identificar métodos para probar os controis
- Desenvolver ferramentas e metodoloxías para verificar os controis

Procedementos para a revisión de resultados

- Utilización de procedementos específicos para a avaliación das probas

Comunicación coa xerencia

- Comunicación dos resultados obtidos

Informe de auditoría

- Elaboración do informe final do traballo realizado