

Auditoría Total



Habitualmente las auditorías existentes en el mercado de la seguridad nos muestran la situación de la empresa en relación con un concepto, el verificado, y por lo tanto una imagen parcial de la realidad de la organización.

Nuestro servicio de auditoría total es la combinación de auditorías que permite a la entidad tener una visión general de su estado de la seguridad en las tres vertientes que configuran la gestión de la seguridad de la información

- **Auditoría de Seguridad en los Sistemas** que ponga de manifiesto las debilidades de la arquitectura de la entidad. Los aspectos principales contemplados en la auditoría son los siguientes:
 - **Information Gathering:** Mediante la fase de Information Gathering se pretende obtener toda la información de libre acceso disponible sobre la empresa o entidad a estudiar.
 - **Estudio y análisis de la red:** La fase de estudio de la red se efectúa desde un punto de conexión a la red a estudiar y se considera intrusiva, obteniéndose: Listado de equipos activos y sus servicios, mapa de red, etc.
 - **Detección de vulnerabilidades:** El objetivo es listar todas las posibles vulnerabilidades para todos los equipos y servicios detectados.
 - **Obtención de acceso:** En esta fase se pretende la obtención de contraseñas, elevación de privilegios, y acceso a datos, o ubicaciones restringidas.
 - **Análisis aplicaciones web mediante metodología OWASP:** La finalidad es la búsqueda de fallos de seguridad en aplicaciones desarrolladas con cualquier tecnología y lenguaje de programación.

- **Auditoría legal** que ponga de manifiesto el grado de cumplimiento por parte de la organización a las exigencias derivadas de la normativa vigente en materia de protección de datos de carácter personal. (LOPD y RMS). Dado que la normativa de protección de datos de carácter personal es un compendio de aspectos jurídicos, técnicos y organizativos, integramos en nuestra Auditoría:
 - Aspectos jurídicos derivados de las exigencias establecidas en la LOPD.
 - Requerimientos tecnológicos derivados del RLOPD.

- Aspectos organizativos necesarios para cumplir con la política de protección de datos implantada.
- **Auditoría procedimental del entorno en materia de seguridad de la información**, tomando como referencia los 133 puntos de control que establece la norma ISO 27002, marco de referencia internacional sobre las mejores prácticas en materia de seguridad de la información.

La realización de este tipo de auditoría permitirá a la organización contar con un informe que analizará de forma transversal el estado de situación en materia de seguridad de la información poniendo de manifiesto el “gap” frente a la normativa vigente (LOPD y RLOPD), las mejores prácticas en gestión de la seguridad de la información (ISO 27002) y las exigencias mínimas de seguridad a nivel de sistemas según metodologías internacionalmente conocidas (OWASP, OSSTMM). También propondrá un conjunto de acciones necesarias para eliminar las desviaciones así como recomendaciones de mejora.

Principios de la auditoría con Áudea

En las auditorías de Áudea se aplican una serie de principios metodológicos con independencia de la organización y sector de actividad:

- Independencia y objetividad
- Búsqueda de las evidencias que fundamenten las conclusiones
- Respeto a la cultura de la organización
- Equipo auditor con experiencia, conocimiento técnico y habilidades personales comunicativas
- La auditoría debe permitir una mejora en los procesos y métodos de trabajo