Guía de auditoría de sistemas.

Tabla de contenidos

1 Descripción

Este documento describe de forma detallada las tres fases fundamentales que componen una auditoría de seguridad de sistemas: **Planificación, Ejecución e Informe**. Está basado en las normas ISO 27001 y la guía interna de auditoría de sistemas de la empresa.

2 Fase de planificación

La planificación es la base del éxito de toda auditoría. Permite definir de forma clara los recursos, el enfoque, los objetivos específicos y los riesgos esperados del proceso.

Objetivos específicos:

- Evaluar el cumplimiento de políticas internas y normativas aplicables en seguridad de la información (ISO 27001, RGPD, LOPDGDD).
- Verificar el diseño y la implementación de la configuración segura de red, cifrado, gestión de accesos, sistemas críticos, VPN y backup.
- Identificar desviaciones respecto a los procedimientos establecidos en documentos oficiales y normativos de la empresa.

Actividades realizadas:

- **Definición del alcance**: La auditoría incluye toda la infraestructura de red (switches, firewall NGFW, VLANs segmentadas), servidores locales (backup, almacenamiento, virtualización), sistemas de cifrado y certificados (PKI), plataforma de telefonía IP, y personal técnico asociado (consultores, soporte, admins).
- **Establecimiento de objetivos de auditoría**:
    - Validar la segmentación de red por departamentos.
    - Comprobar uso adecuado de cifrado y certificados.
    - Verificar la eficacia del DRP local y sus pruebas de recuperación.
    - Auditar cumplimiento de controles de acceso lógico y físico.
- **Determinación de criterios**:
    - Políticas de seguridad y manual de la sede.
    - Procedimientos operativos y de configuración definidos por TI.
    - Directrices ISO 27001 y MAGERIT v3.0.
    - Requisitos legales aplicables (RGPD, LOPDGDD) por tratamiento de datos de clientes y usuarios.
- **Recopilación documental previa**:

    - Inventarios de hardware/software, topología de red, registros de incidentes, configuración de backup, políticas de cifrado, manuales operativos y DRP.
- **Asignación de roles**:
    - Auditor líder, auditores técnicos, responsables de IT y seguridad local, consultores de apoyo documental, y coordinadora de entrevistas.
- **Cronograma de auditoría**:
    - Plan detallado con fechas, entrevistas, fases técnicas, revisión documental y plazos de entrega.

3 Fase de ejecución

La ejecución es la fase más extensa y operativa. Se centra en la recolección y verificación de evidencias técnicas, organizativas y documentales, alineadas al alcance definido.

Actividades específicas aplicadas:

- **Reunión de apertura**
    - Revisión conjunta del objetivo, alcance, metodología, y roles asignados.
    - Aclaración de expectativas entre el equipo auditor y responsables de sede.
    - Confirmación del acceso a documentación y recursos críticos.
- **Recolección de evidencias**
    - **Entrevistas estructuradas**:
        - A administradores de red, responsables de seguridad, usuarios con privilegios altos.
        - Se recaba información sobre prácticas diarias, controles activos, problemas detectados y cultura organizativa.
    - **Revisión documental técnica**:
        - Procedimientos de seguridad, DRP, respaldo, gestión de certificados digitales, control de contraseñas, registros de acceso, y logs de incidentes.
    - **Pruebas técnicas realizadas**:
        - Escaneo de vulnerabilidades (usando Nessus, Nmap).
        - Revisión de configuraciones en firewalls, antivirus, servidores y endpoints (hardening).
        - Validación del uso correcto de MFA en accesos remotos y VPN.
        - Análisis de logs de seguridad: acceso, tráfico, eventos críticos.
        - Comprobación del uso correcto de VLANs (consultoría, atención al cliente, servidores, VoIP) y su aislamiento.
    - **Revisión de cifrado y certificados**:
        - Verificación del cumplimiento del ciclo de vida de los certificados: emisión, renovación, revocación y uso autorizado.
        - Supervisión del uso de HSM, tokens USB y control de claves.
    - **Inspección física y operativa**:
        - Validación del control de acceso físico (lector de tarjetas, CCTV).
        - Revisión del cumplimiento de la política de escritorio limpio.
        - Control de uso de dispositivos externos (solo cifrados, registrados).
        - Supervisión de salas técnicas, racks y ambiente físico seguro.

4 Fase de informe

Una vez finalizado el trabajo de campo, el equipo auditor estructura y documenta sus hallazgos, proponiendo mejoras claras y priorizadas para mitigar riesgos.

Elementos del informe:

- **Resumen ejecutivo**:
  - Dirigido a la alta dirección y responsables locales.
  - Incluye nivel de madurez observado, cumplimiento normativo, principales hallazgos críticos y recomendaciones clave.
- **Metodología aplicada**:
  - Normas utilizadas (ISO), herramientas técnicas, fuentes de evidencias y lógica de análisis.
- **Detalle de hallazgos**:
  - Clasificación: conformidades, no conformidades, oportunidades de mejora.
  - Cada hallazgo contiene:
    - Descripción clara del problema.
    - Evidencia verificable (capturas, logs, entrevistas).
    - Criterio incumplido.
    - Nivel de riesgo (alto, medio, bajo).
    - Recomendación específica y aplicable.
- **Plan de acción propuesto**:
  - Recomendaciones priorizadas.
  - Asignación de responsables locales.
  - Plazos sugeridos para corrección o mejora.
  - Inclusión de métricas de seguimiento.
- **Anexos**:
  - Registros de entrevistas, checklist aplicado, resultados de pruebas técnicas, cronograma ejecutado.

Reunión de cierre:

- Presentación del informe preliminar.
- Espacio para aclaración de hallazgos.
- Acuerdo sobre el cronograma de remediación.
- Establecimiento de la fecha de auditoría de seguimiento.