Procedimiento Operativo — Auditoría de Ciberseguridad

Ubicación: Sede Barcelona
Empresa: TechSys Solutions S.L.

1- Objetivo

Establecer los pasos operativos y responsabilidades para llevar a cabo una auditoría de ciberseguridad en la sede Barcelona de TechSys Solutions S.L. El procedimiento asegura la trazabilidad, el cumplimiento normativo y la identificación de vulnerabilidades técnicas y organizativas, alineado con los estándares de seguridad vigentes.

2- Alcance

Aplica a la infraestructura, sistemas, procesos y documentación vinculados a la seguridad de la información en la sede Barcelona. Incluye entrevistas al personal clave, revisión de políticas internas, escaneo de vulnerabilidades, análisis de configuraciones, y validación del cumplimiento con políticas técnicas y organizativas.

3- Identificación de criterios de auditoría

Para evaluar correctamente el estado de la seguridad en la sede Barcelona de TechSys Solutions S.L., se establecen como referencia los siguientes criterios:

- **Normas internacionales aplicables:**
    - ISO/IEC 27001: Gestión de la Seguridad de la Información
- **Políticas internas de TechSys Solutions S.L.:**
    - Política de Seguridad de la Información (versión vigente)
    - Procedimientos de control de accesos, gestión de contraseñas, respaldo y continuidad
    - Procedimientos documentados por el departamento de TI
- **Documentación técnica operativa:**

    - Configuraciones base y guías de hardening de sistemas
    - Procedimientos de gestión de incidencias y mantenimiento
- **Requisitos legales o contractuales aplicables:**
    - Reglamentos de protección de datos personales (LOPDGDD y RGPD)
    - Compromisos específicos establecidos por contratos con clientes

Estos criterios guiarán tanto la revisión documental como las entrevistas y pruebas técnicas, y servirán como base para clasificar hallazgos, detectar desviaciones y proponer recomendaciones.

4- Asignar roles y responsabilidades

Rol	Función principal	Responsable(s)	Sede
Auditor líder	Supervisión general, planificación, calidad del informe, coordinación con el cliente	Jordi	Madrid
Auditor técnico	Pruebas técnicas, escaneos, análisis de configuraciones, recopilación de evidencias	Pablo, Aníbal	Barcelona
Documentador	Registro de entrevistas, organización de evidencias, soporte en trazabilidad	Javier	Madrid
Responsable IT del cliente	Facilitación de accesos, información técnica, coordinación con equipo interno	Verónica (apoyo: Jorge)	Barcelona
Responsable de seguridad	Validación de hallazgos, contexto sobre controles y políticas internas	Jorge	Barcelona
Coordinadora / Stakeholder	Logística, coordinación de entrevistas, gestión de agenda	Natasha	Madrid
Representante legal	Gestión de acuerdos legales, NDA, validación normativa	Natasha	Madrid
Consultora / apoyo documental	Soporte en revisión de políticas y documentación técnica interna	Elisabeth	Barcelona

5- Establecer cronograma

Fase	Actividad principal	Duración estimada	Observaciones
Reunión de apertura	Presentación de objetivos, alcance y metodología.	1 hora	Participan auditores y responsables del cliente.
Entrevistas	Reuniones con responsables de IT, seguridad, usuarios clave.	1–2 horas por área	Según cantidad de áreas involucradas.
Revisión documental	Análisis de políticas, procedimientos, configuraciones y registros.	1 jornada	Puede realizarse en paralelo con entrevistas.
Pruebas técnicas	Escaneos, análisis de configuraciones, logs, controles de acceso.	2–3 jornadas	Según cantidad de sistemas y profundidad técnica.
Análisis de hallazgos	Organización de evidencias, clasificación y redacción preliminar del informe.	Interno del equipo	No requiere participación del cliente.
Reunión de cierre	Presentación de hallazgos, recomendaciones y recolección de feedback.	1–2 horas	Participan todas las partes involucradas.
Entrega del informe final	Envío del informe completo con plan de acciones y prioridades.	Fecha acordada	Puede ser presencial o por medios digitales.

6- Revisar información preliminar

Antes del inicio de las actividades de campo, el equipo auditor revisará la documentación técnica y organizativa disponible, con el objetivo de comprender el entorno, identificar riesgos previos y ajustar el enfoque de la auditoría. Esta revisión permite optimizar el tiempo durante las entrevistas y pruebas técnicas.

Los documentos e insumos que se solicitarán y analizarán incluyen:

Tipo de documento	Contenido esperado	Responsable de entrega
Mapa de red actual	Diagrama con segmentación de red, dispositivos clave, zonas Wi-Fi, DMZ, etc.	Jorge / Pablo
Inventario de activos	Listado de equipos, servidores, aplicaciones críticas, dispositivos móviles.	Jorge / Aníbal
Política de Seguridad de la Información	Versión vigente de la política general aprobada por dirección.	Elisabeth

Procedimientos internos	Gestión de accesos, contraseñas, backups, continuidad, actualizaciones.	Elisabeth / Aníbal
Registros y evidencias	Logs de accesos, reportes de incidentes, auditorías internas previas.	Jorge / Elisabeth
Configuraciones base	Guías o capturas de configuración de firewalls, antivirus, endpoints.	Pablo / Aníbal
Otros documentos relevantes	Manuales, esquemas de red, controles físicos, informes anteriores.	Jorge / Pablo

7- Comunicación inicial

Antes del inicio formal de la auditoría, se realiza una comunicación estructurada con todas las áreas implicadas de la sede Barcelona. Esta etapa asegura que cada responsable esté al tanto del proceso, sus tiempos y requisitos, y permite resolver posibles dudas anticipadamente.

Las acciones que se ejecutan en esta fase son:

- **Enviar aviso de auditoría:**
  Se notifica formalmente a los responsables de las áreas involucradas mediante correo institucional. El aviso incluye el objetivo general, alcance, fechas clave y personas de contacto.

- **Compartir agenda preliminar y requerimientos:**
  Se entrega un documento con el cronograma tentativo de entrevistas, revisión documental y pruebas técnicas. También se lista la documentación e información que debe estar disponible para el equipo auditor antes del inicio.

- **Establecer canales de comunicación y protocolos:**
  Se definen los medios oficiales para el intercambio de información durante la auditoría (por ejemplo, correo electrónico corporativo y Microsoft Teams).
  Además, se acuerda con el Responsable de Seguridad de TechSys cómo se reportarán los hallazgos preliminares sensibles, priorizando la confidencialidad y la rápida atención cuando corresponda.

8- Realización de la auditoría

a) Reunión de apertura

La auditoría se inicia formalmente con una reunión de apertura entre el equipo auditor y los responsables designados por TechSys Solutions S.L. en su sede de Barcelona. Esta

reunión establece un marco común de entendimiento y coordinación para el resto del proceso.

Los objetivos de esta instancia son:

- **Presentar los objetivos, el alcance y la metodología:**
  El Auditor Líder expone qué se va a auditar, bajo qué criterios, y qué técnicas o herramientas se emplearán. También se aclaran las reglas de intervención del equipo auditor y del personal de TechSys durante la auditoría.

- **Alinear expectativas con los responsables de las áreas:**
  Se repasan los tiempos estimados, la participación esperada de cada área, la modalidad de entrevistas y los canales de contacto.
  Cualquier ajuste logístico o aclaración se registra para evitar malentendidos durante la auditoría.

b) Recopilación de evidencias

Durante esta fase se obtienen datos cualitativos y cuantitativos que permiten evaluar el estado real de la seguridad de la información en la sede Barcelona. Las evidencias pueden ser obtenidas de forma directa (entrevistas, observaciones) o indirecta (documentación, pruebas técnicas).

Las acciones contempladas incluyen:

- **Entrevistas con personal clave:**
  Se mantendrán reuniones estructuradas con:
    - Administradores de sistemas y redes
    - Responsables de seguridad y cumplimiento
    - Usuarios con acceso privilegiado o funciones críticas
- El objetivo es obtener contexto operativo, identificar posibles desviaciones entre lo documentado y lo ejecutado, y detectar controles no formalizados.
- **Revisión documental:**

  Se analizarán los siguientes elementos:
    - Políticas de seguridad de la información vigentes
    - Procedimientos internos de TI y seguridad

    - Registros de accesos, eventos, incidentes y mantenimientos
    - Evidencias de cumplimiento (copias de seguridad, reportes, controles)

- **Pruebas técnicas:**
  El auditor técnico ejecutará acciones planificadas y autorizadas que incluyen:
    - Escaneo de vulnerabilidades sobre segmentos seleccionados de red
    - Revisión de configuraciones en sistemas operativos y dispositivos (hardening)
    - Análisis de logs de sistemas clave (firewalls, antivirus, servidores)
    - Pruebas de accesos lógicos (verificación de perfiles, contraseñas, privilegios)
    - Validación de accesos físicos a salas, racks, o dispositivos sensibles
- **Herramientas utilizadas (según alcance definido):**
    - Nmap
    - Nessus
    - WireShark

---

c) Observación directa

Complementando las fases anteriores, se realizarán inspecciones en campo para verificar que las medidas de seguridad definidas se apliquen de forma efectiva en el entorno real.

Se evaluará el cumplimiento de aspectos como:

- Aplicación de la política de escritorio limpio
- Control de acceso físico a zonas restringidas
- Uso correcto de credenciales personales
- Presencia de cartelería, señalización o bloqueos físicos
- Prácticas de seguridad visibles en el uso de equipos y dispositivos

Estas observaciones serán documentadas como evidencias adicionales para el análisis posterior.

9- Análisis de evidencias

Finalizada la recopilación, el equipo auditor analiza las evidencias obtenidas comparándolas con los criterios definidos previamente. Esta fase tiene como objetivo transformar la información bruta en hallazgos concretos, con valor práctico para la organización.

Las acciones que se desarrollan son:

- **Comparar las evidencias contra los criterios definidos:**
  Se verifica si las prácticas actuales de la sede Barcelona cumplen con las políticas internas, normas internacionales y procedimientos establecidos como referencia.

- **Clasificar los hallazgos:**
  Cada situación identificada se categoriza según su impacto y grado de cumplimiento:

    - **Conformidades:** aspectos que cumplen adecuadamente con los criterios.

    - **No conformidades:** desviaciones claras respecto a los requisitos establecidos.

    - **Oportunidades de mejora:** controles que podrían optimizarse, aunque no representen un incumplimiento directo.

- **Evaluar los riesgos asociados:**
  Para cada no conformidad u oportunidad de mejora se analiza el riesgo, considerando:

    - **Impacto:** qué consecuencias podría generar esa debilidad si se materializa.

    - **Probabilidad:** qué tan factible es que ocurra en el contexto de la sede.

Este análisis permite priorizar las recomendaciones del informe final según la criticidad de los hallazgos.

10- Registro de hallazgos

Una vez analizadas las evidencias, cada hallazgo identificado durante la auditoría se documenta de manera estructurada y precisa. Esta documentación es clave para la

trazabilidad del proceso y para facilitar la toma de decisiones por parte de TechSys Solutions S.L.

Cada hallazgo debe contener los siguientes elementos:

- **Descripción clara:**
  Explicación breve y directa del problema detectado, sin tecnicismos innecesarios.

- **Evidencia recopilada:**
  Datos, capturas, registros, testimonios u observaciones que respalden el hallazgo.

- **Criterio de incumplimiento:**
  Norma, política interna o procedimiento que no se está cumpliendo o se aplica de forma parcial.

- **Grado de criticidad:**
  Evaluación del nivel de riesgo que representa el hallazgo, clasificado como:

  - **Bajo:** impacto mínimo, no compromete la seguridad general.

  - **Medio:** puede generar riesgos si no se corrige en el mediano plazo.

  - **Alto:** representa una vulnerabilidad seria o incumplimiento crítico.

- **Recomendación específica:**
  Acción concreta sugerida para corregir la situación, alineada con buenas prácticas y el entorno operativo de la sede Barcelona.

11- Elaboración del informe de auditoría

Finalizada la etapa de análisis y registro de hallazgos, el equipo auditor elabora un informe formal que recoge todo el trabajo realizado y proporciona a TechSys Solutions S.L. una visión clara del estado de la seguridad en su sede de Barcelona.

El informe contendrá los siguientes elementos:

- **Resumen ejecutivo:**
  Presenta de forma concisa las principales conclusiones, el nivel general de cumplimiento observado y los riesgos más relevantes. Está dirigido a la dirección y responsables clave, con lenguaje claro y no técnico.

- **Detalle de hallazgos y evidencias:**
  Se documentan todos los hallazgos identificados durante la auditoría, incluyendo las evidencias que los sustentan y los criterios de evaluación utilizados.

- **Recomendaciones priorizadas:**
  Cada hallazgo incluye una recomendación específica, clasificada según su urgencia e impacto. Esto facilita la toma de decisiones y la asignación de recursos.

- **Plan de acción sugerido:**
  Se propone un plan con acciones correctivas concretas, responsables sugeridos y plazos tentativos para su implementación, ajustado a la operativa y estructura de TechSys Barcelona.

12- Reunión de cierre

Una vez finalizado el informe, se realiza una reunión de cierre con los responsables y partes interesadas de TechSys Solutions S.L. en la sede de Barcelona. Esta instancia permite validar los resultados y asegurar una comprensión compartida de los hallazgos.

Los objetivos de la reunión de cierre son:

- **Presentar hallazgos y recomendaciones:**
  El equipo auditor expone los puntos clave del informe, explicando los hallazgos detectados, su criticidad y las acciones recomendadas.

- **Aclarar dudas y comentarios:**
  Se abre un espacio para que los responsables técnicos, de seguridad y de dirección puedan realizar consultas, pedir aclaraciones o complementar información.

- **Recoger feedback sobre el proceso de auditoría:**
  Se solicita la opinión de los participantes sobre el desarrollo de la auditoría, la claridad del enfoque, la utilidad de las observaciones y la coordinación durante las distintas fases.

13- Seguimiento

Tras la entrega del informe y la reunión de cierre, se establece un proceso de seguimiento para asegurar que las acciones correctivas recomendadas sean implementadas de forma efectiva en la sede Barcelona.

Las actividades de seguimiento incluyen:

- **Acordar con la organización el plan de acciones correctivas:**
  TechSys definirá, en base al informe recibido, qué medidas adoptará, asignando responsables internos y fechas objetivo para su implementación.

- **Establecer fechas de verificación:**
  Se coordinarán puntos de control posteriores (reuniones o entregas) para validar si las mejoras han sido aplicadas correctamente y si han mitigado los riesgos identificados.

- **Actualizar el estado de los hallazgos:**
  Cada hallazgo será marcado según su evolución:

    - **Pendiente:** aún no abordado.

    - **En proceso:** acción iniciada pero no completada.

    - **Cerrado:** solución implementada y validada.

14-Herramientas recomendadas en procedimientos operativos

Durante la auditoría en la sede Barcelona, se utilizarán herramientas específicas que permiten una ejecución técnica efectiva, un control riguroso de los hallazgos y una documentación ordenada del proceso.

Herramientas sugeridas por tipo de actividad:

- **Para pruebas técnicas:**

    - **Nmap:** escaneo de puertos y detección de servicios.

    - **Nessus:** escaneo de vulnerabilidades.

    - **Wireshark**. escaneo de tráfico

- **Para gestión de hallazgos:**

    - Hojas de cálculo estructuradas (Excel o Google Sheets)

    - **Jira** o plataformas similares para el seguimiento de acciones correctivas

- **Para documentación:**

    - **Microsoft Word / Excel:** elaboración de informes y matrices de control

- Sistemas internos de gestión documental: almacenamiento y trazabilidad de evidencias