📜 Incidentes de Ciberseguridad – UD1.4

Auditorías Internas de Cumplimiento en Materia de Prevención

IES Chan do Monte – Curso 2025/26

Docente: Simal Paz, Daniel

Índice

---

1. Introducción

Las auditorías internas de cumplimiento en materia de prevención son procesos sistemáticos que verifican la eficacia de los planes de concienciación, formación y medidas de seguridad.
No se limitan a revisar documentos: buscan comprobar si las personas, procesos y tecnologías responden bien frente a amenazas como el *phishing*, la ingeniería social o el malware.
Aplicadas de forma periódica, habilitan un ciclo real de mejora continua.

💡 **Una auditoría interna permite:**

- Identificar fallos en la aplicación de medidas.
- Medir el impacto real de la formación.
- Fomentar la mejora continua.

📌 ISO 19011 – Directrices para auditorías de sistemas de gestión

---

2. Objetivos de las auditorías internas

Objetivos principales:

- Comprobar si la capacitación del personal es efectiva.
- Verificar que las medidas técnicas y organizativas funcionan correctamente.
- Asegurar el cumplimiento del ENS, RGPD, LOPDGDD e ISO/IEC 27001.

Objetivos estratégicos:

- Reducir vulnerabilidades antes de incidentes graves.
- Aportar evidencias objetivas ante reguladores y auditorías externas.
- Fortalecer la cultura de prevención en toda la organización.

📌 Guía del CCN-CERT sobre auditorías ENS

---

3. Métricas e indicadores de logro

Un cuadro de mando con indicadores claros permite medir la eficacia del plan de concienciación y seguridad.

Indicadores comunes

- Clics en correos de phishing.
- Participación en simulacros de ataques.
- Resultados de encuestas y cuestionarios.
- Reportes de incidentes.
- Cumplimiento en formación.
- Certificaciones de personal técnico.

Métricas adicionales:

Métrica	Descripción	Justificación
Tiempo medio de respuesta ante incidentes simulados	Tiempo de reacción del personal.	Evalúa rapidez de respuesta.
Cumplimiento de políticas de contraseñas	Usuarios que cumplen las políticas de contraseñas.	Refleja disciplina de seguridad.
Participación en simulacros	Número de empleados que participan.	Mide compromiso y preparación.

📌 INCIBE – Guía de métricas de ciberseguridad

A continuación se proponen indicadores frecuentes y métricas adicionales:

Métrica / Indicador	Qué mide	Por qué importa
Clics en correos de phishing	Capacidad para detectar fraudes	Reduce la tasa de compromiso
Caídas en ingeniería social	Resiliencia ante manipulaciones	Señala necesidad de refuerzo
Incidentes reportados	Disposición a comunicar anomalías	Acelera la respuesta organizada
Participación en formación	Implicación del personal	Relaciona aprendizaje con desempeño
Resultados de cuestionarios	Asimilación de contenidos	Evidencia conocimiento práctico
Certificaciones técnicas	Competencia del personal técnico	Sustenta la madurez del equipo
Incidentes antes/después del plan	Efectividad global del programa	Permite evaluar impacto
Reinstalaciones por malware	Impacto de infecciones	Refleja superficie de ataque
Tiempo medio de respuesta (simulacros)	Rapidez al detectar y reportar	Limita el daño del ataque
Cumplimiento de política de contraseñas	Disciplina en contraseñas y MFA	Bloquea accesos indebidos
Participación en simulacros	Entrenamiento práctico	Mejora la preparación real

---

4. Metodología de auditoría (fases y herramientas)

Fases:

- **Planificación:** Definir alcance, criterios, responsables e indicadores; preparar cronograma.
- **Ejecución:** Recoger evidencias: análisis documental, entrevistas, simulaciones, observación directa.
- **Informe:** Redactar hallazgos, no conformidades, riesgos y plan de acciones correctivas.
- **Seguimiento:** Verificar la eficacia de acciones y consolidar mejoras en auditorías posteriores.

Herramientas recomendadas:

- Listas de verificación (*checklists*) y guías de entrevistas.
- Plataformas para simulaciones de *phishing* o reporting.
- Cuestionarios online para evaluación de conocimientos.
- Dashboards o hojas de cálculo para métricas y tendencias.

---

5. Beneficios de las auditorías internas

- Previenen sanciones por incumplimientos normativos.
- Mejoran de forma continua el plan de seguridad y concienciación.
- Reducen el riesgo humano, principal origen de incidentes.
- Aumentan la confianza de clientes, socios y autoridades.
- Refuerzan la cultura preventiva como compromiso permanente.

📌 ENISA – Guidelines for Security Audits

---

6. Ejemplos prácticos claros y concretos

Ejemplo 1: Reporte insuficiente de *phishing*

- *Hallazgo:* Aunque el 80 % reconoce correos maliciosos, solo el 20 % los reporta.
- *Acciones:* Implementar un botón de “Reportar *phishing*” y una campaña recordatoria; definir un KPI de reporte mensual ≥ 60 %.
- *Resultado esperado:* Aumento del reporte y reducción del tiempo de contención.

Ejemplo 2: Formación incompleta

- *Hallazgo:* El 30 % no ha completado la formación obligatoria.
- *Acciones:* Sesiones de refuerzo, recordatorios automáticos y *microlearning*; política de obligatoriedad con certificación anual.

- *Resultado esperado:* ≥ 95 % de cumplimiento en 3 meses.

Ejemplo 3: Contraseñas débiles

- *Hallazgo:* Baja adopción de MFA y contraseñas reutilizadas.
- *Acciones:* Activar MFA por defecto, usar gestor de contraseñas corporativo y establecer caducidad razonable.
- *Resultado esperado:* ≥ 98 % de cuentas con MFA; reducción de accesos indebidos.

---

7. Plantillas operativas

Checklist mínimo (extracto)

- Políticas y procedimientos actualizados y comunicados.
- Registro de formación: asistentes, fechas, resultados.
- Simulaciones realizadas y métricas (clics, reportes, tiempos de respuesta).
- Gestión de contraseñas y MFA aplicada.
- Registro de incidentes y lecciones aprendidas.
- Plan de acciones correctivas con responsables y plazos.

Cronograma tipo (RACI – extracto)

Actividad	Responsable (R)	Aprueba (A)	Consulta (C)	Informa (I)
Planificación y alcance	CISO / Responsable de Seguridad	Dirección	IT / Legal	Toda la organización
Simulaciones y encuestas	Equipo de Seguridad	CISO	RR. HH.	Plantilla
Análisis y hallazgos	Auditor interno	CISO	IT / Unidades	Dirección
Acciones correctivas	Propietarios de proceso	CISO	Auditor interno	Interesados
Seguimiento	Auditor interno	Dirección	CISO / IT	Toda la organización

---

8. Recursos y referencias (con hipervínculos)

- ISO 19011 – Directrices para auditorías de sistemas de gestión
- CCN-CERT – Esquema Nacional de Seguridad (ENS) y guías STIC
- INCIBE – Métricas y concienciación en ciberseguridad
- ENISA – Buenas prácticas de auditoría y gestión de riesgos

---

9. Glosario

- **Auditoría interna:** Evaluación sistemática del cumplimiento y eficacia de controles.
- **Phishing:** Técnica de suplantación para obtener credenciales o datos.
- **Métrica / Indicador:** Valor cuantitativo que mide la eficacia de una acción.
- **No conformidad:** Desviación respecto a lo planificado o a un requisito.
- **MFA (Multi-Factor Authentication):** Autenticación que combina dos o más factores de seguridad.

---

10. Conclusiones

Las auditorías internas de cumplimiento permiten verificar con datos si la capacitación y las medidas de seguridad funcionan en la práctica.
Con métricas claras, metodología en cuatro fases y un plan de mejora continua, las organizaciones elevan su madurez, cumplen la normativa y reducen de forma sostenida los riesgos asociados al factor humano.