Auditoría interna y métricas

La auditoría interna es un proceso dentro de un sistema de gestión de seguridad de la información (SGSI) maduro que permite revisar de manera sistemática y periódica el cumplimiento de políticas, controles y procesos, así como detectar brechas y mejorar el sistema.

Funciona como un sello de calidad que garantiza la confiabilidad y efectividad del SGSI, al identificar desviaciones y proponer correcciones antes de la auditoría de certificación. Si el objetivo no es la certificación, la auditoría interna sigue siendo una herramienta estratégica importante.

Su finalidad no es sancionar, sino detectar brechas y oportunidades de mejora antes de que se conviertan en incidentes críticos. Por ejemplo, la auditoría ISO 27001 es un proceso sistemático que evalúa si la organización cumple los requisitos de la norma. Una auditoría efectiva aporta valor a la empresa al corregir desviaciones y preparar la organización para auditorías externas.

Para comunicar sus resultados, se utilizan métricas (KPI/KRI) e informes ejecutivos que resumen los hallazgos en términos de negocio. Por ejemplo, un informe de auditoría bien diseñado presenta indicadores de

riesgo, desempeño y resultados de manera comprensible para la alta dirección.

En este módulo se profundiza en cómo planificar las auditorías anuales, gestionar hallazgos y acciones correctivas, documentar evidencia con cadena de custodia y definir y presentar métricas de seguridad (KPI/KRI) que impulsan la mejora continua. Se abordará la importancia de la evidencia confiable y la forma de comunicar resultados a la dirección. Finalmente, se aprenderá a usar cuadros de mando y narrativas de datos para informar efectivamente, planificar un roadmap trimestral de controles y aplicar lecciones aprendidas, todo con ejemplos prácticos para pymes.

Unidad 1. Auditoría y no conformidades

1.1. Programa anual de auditorías internas

Un programa anual de auditorías internas es el calendario que define qué procesos o áreas se auditarán, con qué frecuencia y por quién. Toda organización certificada debe elaborar este programa de manera planificada.

Este programa actúa como el plan maestro en el que se detallan qué áreas se auditarán, cuándo y por quién, y permite informar sobre la planificación de las auditorías internas dentro del SGSI.

En una pyme, un programa típico incluye, por ejemplo, una auditoría general de seguridad y revisiones específicas de áreas críticas, como redes, accesos y proveedores.

Al definir el alcance y el calendario con antelación, se asegura la cobertura de todos los procesos y se cumple con el enfoque de mejora continua. Incluso con pocos recursos, es posible agrupar procesos semejantes o auditar por zonas, siempre documentándolo en el plan anual.

Entre los elementos clave a incluir se encuentran los siguientes:

- **Alcance.** Procesos, departamentos o áreas a auditar.
- **Objetivos:** propósito de cada auditoría, como verificar conformidad normativa, medir efectividad o identificar mejoras.
- **Criterios:** normas, políticas y procedimientos a evaluar, por ejemplo, ISO 27001 o reglamentos internos.
- **Fechas estimadas:** calendario anual, trimestral o semestral con periodos tentativos.
- **Auditores designados:** personas capacitadas e imparciales responsables de cada auditoría.

El programa debe revisarse anualmente o ante cambios organizacionales, como la implementación de nueva tecnología o una reorganización. En pymes con pocos recursos, este programa puede gestionarse con herramientas sencillas, como una hoja de cálculo compartida o un tablero en Trello o Asana, donde se liste cada auditoría con su fecha y responsable. De esta manera, sin realizar grandes inversiones, se asegura que todas las áreas críticas sean auditadas al menos una vez al año.

Auditoría técnica: introducción a las pruebas de penetración (o pentesting)

Hoy en día, la seguridad de la información se ha convertido en una prioridad para las empresas que buscan proteger sus datos sensibles y mantener la confianza de sus clientes.

La ciberseguridad es un pilar fundamental para organizaciones de todos los tamaños, dado el riesgo que representan las amenazas digitales a nivel mundial. La información confidencial, como los datos de los clientes y la propiedad intelectual, es un activo valioso que requiere protección frente al acceso no autorizado. Además, los ciberataques pueden interrumpir las operaciones diarias y generar pérdidas financieras significativas.

Las consecuencias de un ataque son graves: una filtración de datos puede afectar la confianza de los clientes y la reputación pública, provocando pérdidas comerciales y problemas legales.

De esta manera, los profesionales de la ciberseguridad tienen la responsabilidad de crear y mantener una estructura de seguridad organizacional sólida que abarque todas las áreas del negocio. Entre sus funciones se incluyen:

- identificar y corregir vulnerabilidades en la red;
- implementar protocolos de seguridad;
- realizar un seguimiento para detectar comportamientos sospechosos.

Para las empresas, una estrategia sólida de ciberseguridad deja de ser una opción y se convierte en una necesidad, ya que protege tanto sus intereses como los de sus clientes. En este contexto, el pentest, o prueba de penetración, se presenta como una herramienta relevante en la ciberdefensa, ya que permite identificar y corregir

vulnerabilidades antes de que los ciberdelincuentes puedan explotarlas.

***Pentest* (abreviatura de prueba de penetración) es una práctica esencial donde los expertos simulan ataques a sistemas de información para identificar vulnerabilidades. El objetivo es encontrar y corregir fallas antes de que personas malintencionadas puedan explotarlas.**

La metodología del pentest puede implicar varios pasos, comenzando por definir el alcance y continuando con las fases de reconocimiento, acceso, mantenimiento del acceso y análisis de resultados. Es mediante esta evaluación en profundidad que las empresas pueden fortalecer sus defensas frente a amenazas reales.

La realización de un test de penetración utiliza diversas herramientas específicas, que pueden incluir escáneres de vulnerabilidades, herramientas de craqueo, marcos de

pruebas de intrusión y simulaciones de ataques de distintos tipos y niveles de complejidad.

Las debilidades que se pueden identificar mediante los pentests van desde configuraciones inadecuadas hasta fallos de software o problemas de hardware. Al detectar estas vulnerabilidades, las empresas pueden aplicar acciones correctivas para mitigar los riesgos y garantizar una infraestructura de TI más segura.

Ventajas de un pentest

La prueba pentest no solo permite la identificación y resolución de vulnerabilidades, sino que también fortalece la postura de seguridad frente a amenazas constantes. Algunas de las principales ventajas de esta herramienta para las empresas se mencionan a continuación.

Identificación proactiva de vulnerabilidades —

el pentest facilita la detección activa de fallos de seguridad, lo que permite a la empresa anticiparse a posibles ataques externos. Este análisis es fundamental, ya que revela las debilidades antes de que puedan ser explotadas por terceros.

Evaluación de la postura de seguridad

mediante el pentest, las empresas obtienen un diagnóstico preciso de cómo responden sus defensas ante diferentes estrategias de ataque, lo que orienta la planificación estratégica de seguridad.

Mitigación de riesgos

la información obtenida mediante el pentest orienta el desarrollo de soluciones efectivas para reducir riesgos, disminuyendo la probabilidad de incidentes de seguridad que puedan afectar a la empresa.

Cumplimiento de normas

muchas industrias exigen el cumplimiento de estándares de seguridad. Las empresas que realizan pentests demuestran su compromiso con estos requisitos, evitando posibles sanciones.

Formación del equipo de seguridad

el pentest también funciona como herramienta de capacitación, enseñando al equipo de seguridad dónde enfocar sus esfuerzos y cómo reaccionar ante amenazas reales.

Ahorro de costos a largo plazo —

invertir en pruebas de penetración puede generar ahorro económico, al prevenir gastos derivados de incidentes de seguridad, daños en los sistemas o pérdida de datos.

Protección de la reputación empresarial —

la realización de pentests evidencia responsabilidad y cuidado por la seguridad, preservando la imagen de la empresa y evitando daños a su reputación que podrían derivarse de violaciones de seguridad.

La importancia de *pentest* para los diferentes sectores del mercado

Con la transformación digital, la realización del *pentest* se ha vuelto imprescindible para empresas de todos los segmentos del mercado, no solo para las tecnológicas. Además, es adaptable a la realidad de cada sector, considerando sus particularidades y normativa específica. A continuación, se muestra cómo cada área puede beneficiarse de estas pruebas.

Sector financiero

las instituciones financieras están constantemente expuestas a ciberataques. El pentest contribuye a proteger los datos financieros y de los clientes, detectando debilidades antes de que puedan ser explotadas.

Salud

la información de salud es extremadamente sensible. Una evaluación rigurosa mediante pentest garantiza la integridad y privacidad de los datos de los pacientes, cumpliendo al mismo tiempo con estrictas normas de seguridad.

Educación

universidades y escuelas suelen almacenar datos de estudiantes e investigaciones valiosas. Las pruebas de penetración ayudan a mantener la seguridad de esta información, evitando pérdida de datos o exposiciones no deseadas.

Comercio electrónico

en un entorno de continuas transacciones monetarias en línea, el pentest permite identificar y corregir vulnerabilidades, lo cual es

crucial para mantener la confianza del cliente y la integridad del sistema.

Gobierno y servicios públicos —

para los organismos gubernamentales, la ciberseguridad es fundamental para proteger la información confidencial del Estado y de los ciudadanos. Las pruebas de penetración aseguran que los sistemas sean robustos frente a ataques y fugas de información.

Hacking **vs.** *cracking*

Es importante entender la diferencia entre hacking y cracking: mientras que el hacking ético busca fortalecer la seguridad, el cracking se centra en violar sistemas con intenciones maliciosas. En este trabajo, el enfoque estará en el aspecto ético del hacking, fundamental para la protección digital.

El pentesting, o pruebas de penetración, es una práctica clave dentro del hacking ético. Este proceso implica simular ataques controlados para identificar vulnerabilidades y evaluar la resistencia de sistemas y redes. El pentesting se alinea con el objetivo de fortalecer la seguridad al revelar posibles brechas antes de que los ciberdelincuentes puedan explotarlas.

Tipos principales de pentest

Hoy en día, existen tres tipos principales de pentest, cada uno de los cuales ofrece diferentes niveles de análisis y contexto durante la evaluación de seguridad. A continuación, se describen resumidamente.

- **Pentesting de caja negra:** en este tipo de pentest, el evaluador tiene poco o ningún

conocimiento previo sobre los sistemas de destino. Se imita a un atacante externo que realiza el exploit sin información privilegiada, lo que proporciona una perspectiva realista de lo que un atacante podría descubrir y explotar.

- **Pentesting de caja blanca:** a diferencia del de caja negra, el pentest de caja blanca se realiza con pleno conocimiento de la infraestructura a probar. Es una auditoría de seguridad interna detallada en la que el evaluador tiene acceso a diagramas de red, códigos fuente y otra información relevante, lo que permite una evaluación de vulnerabilidad más profunda.

- **Pentesting de caja gris:** en el pentest de caja gris, el enfoque es intermedio. El tester cuenta con un conocimiento parcial del sistema, simulando un ataque por parte de alguien que tiene algún nivel de acceso o conocimiento interno. Este tipo de prueba ayuda a evaluar qué tan bien resiste un sistema los ataques internos.

Principales metodologías pentest

Antes de iniciar una prueba de penetración, es fundamental comprender las metodologías involucradas en este proceso.

Estas guían a los evaluadores a lo largo del reconocimiento, definen el alcance de las pruebas y aseguran que todos los aspectos de la aplicación o sistema se examinen según los estándares establecidos. Algunas de las metodologías más utilizadas son las siguientes:

- **Guía de pruebas OWASP (metodología OWASP).** La Guía de pruebas de OWASP es un recurso integral que proporciona herramientas y técnicas para evaluar la seguridad de aplicaciones web. Se trata de un enfoque estructurado para probar y mejorar la seguridad de las aplicaciones, que incluye varias metodologías y pruebas específicas. Detalla un proceso de prueba en cuatro fases y cubre todo, desde la planificación y preparación hasta la recopilación de información y la identificación de vulnerabilidades. Es una referencia imprescindible para los profesionales que realizan pentests en la web.

- **Estándar NIST SP 800-115.** Conocido como la Guía técnica para pruebas y evaluaciones de seguridad de la información, es un enfoque gubernamental para pentest. Se trata de un manual técnico que orienta a las

organizaciones en la planificación, ejecución y análisis de pruebas de seguridad de la información. Hace énfasis en la planificación y documentación detalladas y recomienda procedimientos para identificar vulnerabilidades en los sistemas. Incluye métodos para evaluar la eficacia de las medidas de seguridad y, con frecuencia, se utiliza junto con otros estándares para pruebas de cumplimiento.

- **PTES (*penetration testing execution standard* o estándar de ejecución de pruebas de penetración).** PTES proporciona un marco estandarizado para realizar pentests, ofreciendo orientación sobre la definición del alcance y los procedimientos a seguir. Este estándar ayuda a garantizar que todas las pruebas se realicen con rigor y coherencia, cubriendo desde la fase previa al compromiso hasta la elaboración del informe final. Promueve una comprensión clara de qué se está evaluando y por qué, lo cual es esencial para obtener resultados efectivos.

Diferencia entre pentest y análisis de vulnerabilidad

El pentest y el análisis de vulnerabilidad son dos enfoques fundamentales para la seguridad de la información. Sin embargo, cada uno tiene objetivos distintos dentro del contexto de evaluación y fortalecimiento de la infraestructura de TI.

A continuación, se presenta una tabla con las principales diferencias entre ambos:

Tabla 1. Diferencias entre pentest y análisis de vulnerabilidad

	Análisis de vulnerabilidad	Pruebas de penetración (pentest)
Enfoque principal	Identificación de debilidades en sistemas y redes.	Simulación de ataques para identificar y explotar vulnerabilidades.
Metodología	Automatizado, mediante software específico.	Combinación de técnicas automatizadas y manuales, que requieren habilidades avanzadas.
Profundidad	Superficial, ya que no explota activamente las vulnerabilidades encontradas.	Intensivo y detallado, que implica la ejecución de ataques controlados para pruebas.

Fuente: elaboración propia

Un análisis de vulnerabilidad sirve como paso inicial para identificar posibles fallos de seguridad, mientras que el pentest tiene como objetivo evaluar la eficacia de las medidas de seguridad existentes, ofreciendo una visión más realista de la resistencia de un sistema frente a ataques reales.

En resumen, el análisis de vulnerabilidad busca detectar fallas, mientras que el pentest pretende explotarlas de manera ética para comprender las implicaciones reales de una posible infracción.

¿Cuándo es el momento adecuado para realizar un *pentest*?

En el ámbito de la seguridad de la información, realizar una prueba de penetración es fundamental para evaluar la resistencia de una organización frente a ataques. Algunos momentos recomendados para llevar a cabo un pentest son los siguientes:

1. **Después de importantes cambios en la infraestructura.** Cuando se producen modificaciones en el entorno de TI, como la implementación de nuevos sistemas o actualizaciones significativas.

2. **Antes del lanzamiento de aplicaciones o sistemas:** para garantizar que las nuevas aplicaciones sean seguras antes de su puesta en producción o acceso público.

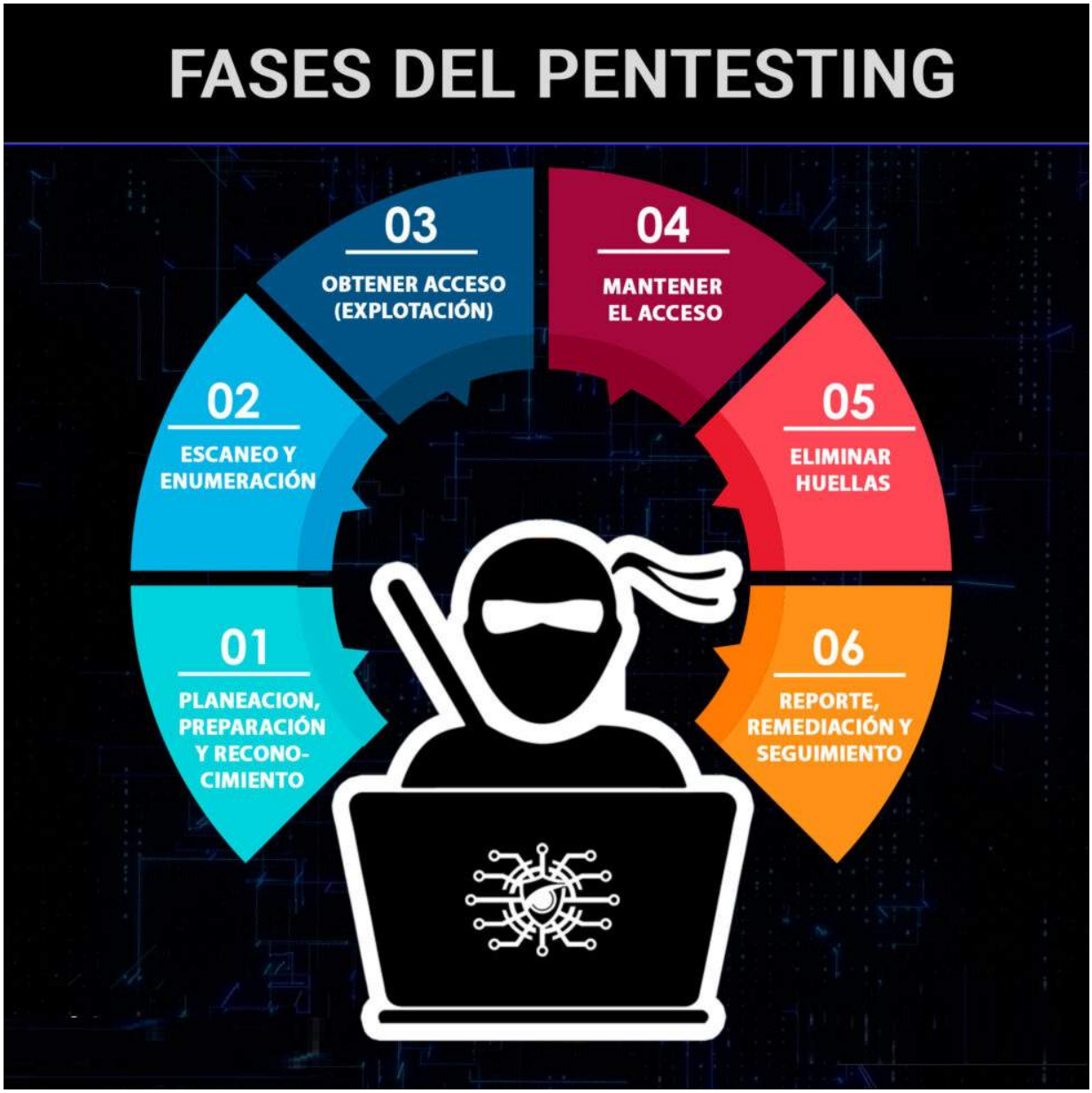
3. **Después de incidentes de seguridad:** si la empresa ha experimentado algún incidente, un pentest posterior puede identificar otras vulnerabilidades que no se habían detectado previamente.

Asimismo, muchas normas y regulaciones exigen la realización periódica de pruebas de penetración como requisito para cumplir con los estándares de seguridad. Por ello, se recomienda que la mayoría de las organizaciones realicen un pentest al menos una vez al año, mientras que las empresas de sectores altamente regulados o con alta presencia en línea pueden necesitar una frecuencia mayor.

Fases de una prueba de penetración del sistema

El proceso estructurado de un *pentest* comprende varias fases, que van desde la planificación hasta la ejecución de ataques controlados con el fin de identificar vulnerabilidades en el sistema.

Figura 1. Fases de una prueba de penetración del sistema



Fuente: Laprovittera, 2025, https://goo.su/oHMAQ

Para ofrecer una evaluación de seguridad integral, se utiliza una metodología o un marco de *pentest* que permite examinar exhaustivamente la seguridad de una organización.

Una prueba de penetración típica se desarrolla en seis fases durante una intervención. A continuación, se describen estas fases tal como se aplican en la práctica.

Paso 1

Planificación, preparación y reconocimiento

Esta fase puede pensarse en dos pasos:

- **Identificación y planificación:** al inicio de un pentest, esta etapa es fundamental para establecer el alcance y los objetivos de la prueba. Incluye definir qué sistemas se evaluarán y qué métodos se emplearán, aspectos necesarios para una planificación adecuada.
- **Recopilación de información (preparación y reconocimiento):** es el paso previo a los ataques reales. Implica un reconocimiento detallado mediante la búsqueda de datos públicos que puedan ayudar a identificar posibles puntos de entrada al sistema. Para ello, pueden utilizarse herramientas de escaneo de vulnerabilidades.

Paso 2

Escaneo y enumeración. Detección de vulnerabilidades

En esta fase se utilizan herramientas y técnicas para identificar fallas que puedan explotarse. Este paso permite elaborar un mapa de las debilidades de seguridad existentes en el sistema bajo prueba.

Paso 3

Obtención de acceso. Explotación de vulnerabilidades

Durante esta etapa, se intenta explotar las fallas detectadas en la fase anterior. Se ponen a prueba vulnerabilidades como la inyección SQL y, si la explotación tiene éxito, se puede obtener acceso no autorizado al sistema.

Paso 4

Posexplotación (mantenimiento del acceso)

Una vez logrado el acceso, se analiza hasta dónde es posible avanzar dentro del sistema comprometido y si es viable mantener el acceso durante un período prolongado, siempre dentro del alcance definido de la prueba.

Paso 5

Eliminación de huellas

En esta fase se revisan y eliminan los rastros generados durante la prueba, con el objetivo de simular el comportamiento de un atacante real y evaluar la capacidad del sistema para detectar intrusiones.

Paso 6

Informes, remediación y seguimiento. Análisis de datos e informes

Tras los intentos de explotación, se realiza el análisis de la información obtenida y se elabora el informe final. En él se documentan las vulnerabilidades detectadas y se formulan recomendaciones para reducir los riesgos identificados. La comunicación de resultados debe ser clara, precisa y orientada a la toma de decisiones.

Junto con esta metodología, se emplean herramientas que apoyan la realización de las pruebas. Estas permiten automatizar tareas que demandan mucho tiempo y llevar a cabo operaciones ofensivas de forma más eficiente.

Recomendaciones pos-pentest

Tras realizar un pentest, es fundamental adoptar medidas que garanticen que la seguridad de la información de la empresa quede reforzada. Algunas recomendaciones son las siguientes:

- **Análisis detallado del informe.** El equipo de TI debe examinar minuciosamente los resultados, comprendiendo las vulnerabilidades identificadas.

- **Priorización de vulnerabilidades:** no todas las debilidades presentan el mismo nivel de riesgo. Es necesario priorizar la corrección según el impacto potencial de cada una.

- **Gestión de debilidades:** mantener un registro de las vulnerabilidades y monitorearlas de manera continua permite gestionar los riesgos de forma proactiva.

- **Plan de remediación:** elaborar un plan de acción para corregir las fallas detectadas. Las medidas pueden incluir, por ejemplo, actualizaciones de software.

- **Capacitación de los empleados:** educar al equipo sobre las mejores prácticas de seguridad que se implementarán tras el pentest.

- **Pruebas de verificación:** después de aplicar las correcciones, realizar nuevas pruebas para asegurar que las medidas adoptadas son efectivas.

- **Revisión de políticas de seguridad:** actualizar las políticas internas de seguridad según sea necesario para prevenir futuras vulnerabilidades.

De esta manera, es posible fortalecer la postura de seguridad empresarial frente a los ciberataques, garantizando que las fallas detectadas durante el pentest sean gestionadas y corregidas de forma efectiva.

Pentest: los principales desafíos

Con el rápido ritmo de la innovación tecnológica y las constantes amenazas cibernéticas, el pentest se ha adaptado. Los profesionales de esta área enfrentan una creciente demanda de seguridad frente a nuevas metodologías de ataque, por lo que deben mantenerse actualizados con las últimas tendencias y desafíos en ciberseguridad. A continuación, se destacan algunas tendencias importantes:

- **Evolución de las amenazas cibernéticas.** Los métodos de ataque son cada vez más sofisticados, lo que obliga a los profesionales

de pentest a desarrollar técnicas avanzadas para identificar vulnerabilidades. La complejidad del código y la diversidad de plataformas amplían el espectro de puntos de falla, exigiendo una capacitación integral y adaptación constante.

- **Pentest en entornos de nube:** la migración a la nube presenta nuevos desafíos. La evaluación de vulnerabilidades en este contexto debe considerar la configuración de la infraestructura, el control de acceso y la separación de datos. La protección en entornos de nube requiere una visión integrada que combine el pentesting tradicional con conocimientos especializados en seguridad en la nube.

- **IoT y ciberseguridad:** con el aumento del número de dispositivos conectados a través del Internet de las Cosas (IoT), se generan nuevos puntos de ataque en la red. Cada dispositivo representa un vector de ataque potencial, lo que amplifica la necesidad de realizar pruebas de penetración sólidas y específicas para IoT, así como de abordar la seguridad durante toda la vida útil del dispositivo.

Futuro de pentest

Como indica la principal tendencia mundial, el futuro del pentest probablemente incluirá avances tecnológicos y la adopción de inteligencia artificial para mejorar la efectividad de las prácticas de seguridad.

- **Innovaciones tecnológicas en ciberseguridad**

  Los profesionales del área adoptan cada vez más herramientas innovadoras y tecnologías avanzadas para fortalecer sus estrategias de pentest. Se espera que la automatización permita realizar análisis de vulnerabilidades más eficientes y precisos. Estas innovaciones facilitarán la identificación y explotación de vulnerabilidades que actualmente podrían pasar desapercibidas durante las pruebas de penetración. Las principales tendencias en este sentido son las siguientes:

  - Capacidades avanzadas de reconocimiento.
  - Automatización en la identificación de fallas de seguridad.

- Iniciativas de prueba y planificación más adaptativas y contextuales.

Inteligencia artificial y aprendizaje automático

El uso de la inteligencia artificial (IA) y el aprendizaje automático está transformando la manera en que se realizan los pentests. Estas tecnologías no solo permiten simular ciberataques más complejos, sino que también proporcionan un análisis profundo y detallado, fundamental para elaborar un informe de pentest completo. En este ámbito se observan estas tendencias:

- Aplicación del aprendizaje automático para predecir y analizar comportamientos maliciosos.
- Mejora continua del proceso de pentest mediante aprendizaje y adaptación automáticos.
- Mayor capacidad de los profesionales de seguridad para interpretar datos y responder eficazmente a las amenazas.

Conclusión

Realizar un *pentest* es un paso crucial para **fortalecer la ciberseguridad,** ya que permite la identificación y remediación de vulnerabilidades, y actúa como catalizador para la mejora continua de las estrategias de defensa de una empresa.

1.2. Hallazgos, acciones correctivas y verificación

Durante la auditoría se recopila evidencia (registros, entrevistas, documentos) que se contrasta con los criterios establecidos (políticas, normas). Cualquier discrepancia se documenta como **hallazgo de auditoría**, entendido como cualquier evento, registro, documento o declaración identificado durante la auditoría que sirve para evaluar el cumplimiento.

Según la norma **ISO 9000:2015 (Sistemas de gestión de la calidad. Fundamentos y vocabulario)**, el concepto de hallazgo de auditoría se define como “resultados de la

evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría" (ISO, 2015, https://goo.su/INyr3).

Aunque esta definición puede resultar técnica y generar dudas, la norma incluye tres notas aclaratorias sobre el significado de un hallazgo de auditoría:

- **Nota 1.** Los hallazgos de auditoría indican conformidad o no conformidad.
- **Nota 2.** Los hallazgos de auditoría pueden conducir a la identificación de oportunidades de mejora o al registro de buenas prácticas.
- **Nota 3.** Si los criterios de auditoría se seleccionan a partir de requisitos legales o reglamentarios, los hallazgos pueden denominarse cumplimiento o no cumplimiento" (ISO, 2015, https://goo.su/INyr3).

Por lo tanto, un **hallazgo de auditoría** es cualquier evento, registro, documento o declaración; en definitiva, cualquier elemento que aparezca durante la auditoría y que sirva para

evaluar si se cumple o no lo que se está auditando. Por ejemplo:

- un registro es un hallazgo de auditoría;
- un procedimiento es un hallazgo de auditoría;
- una conversación del auditor con un trabajador para evaluar cierto proceso de la empresa es un hallazgo de auditoría.

Existe cierta confusión con este concepto entre los profesionales de la consultoría, quienes a veces creen que un **hallazgo de auditoría** es algo detectado durante la auditoría, pero que aún no ha sido evaluado como conforme o no conforme. Sin embargo, según la definición de la norma ISO **9000:2015,** un hallazgo de auditoría ya constituye evidencia evaluada como conformidad o no conformidad (nota1).

Durante la auditoría se registran hallazgos, es decir, discrepancias entre el estado real y lo esperado. Cada hallazgo debe describirse con claridad, sin juicios, e incluir la siguiente información:

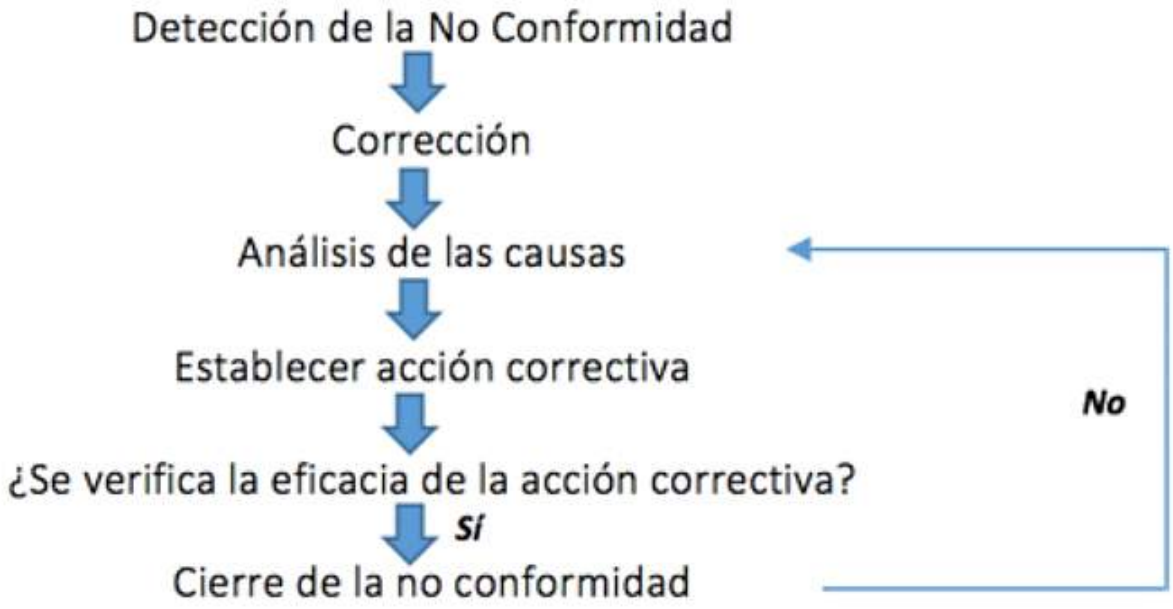
- **Criterio incumplido.** El requisito o control que no se cumple.
- **Evidencia objetiva:** registros, observaciones o documentos que demuestran el hecho.
- **Descripción precisa:** qué ocurrió y en qué contexto.

Los hallazgos se clasifican en **conformidades** y **no conformidades.** A su vez, las conformidades se dividen en **observación** y **oportunidad de mejora.**

- **No conformidad:** incumplimiento de un requisito. Ejemplo: falta de respaldo automático de datos.
- **Observación:** situación potencialmente riesgosa sin impacto inmediato. Ejemplo: plan de contingencia vencido, pero no implementado.
- **Oportunidad de mejora:** sugiere optimizar un proceso que ya es adecuado. Ejemplo: unificar formatos de reporte para ahorrar tiempo.

Ante una no conformidad, se planifican **acciones correctivas**, que son propuestas de mejora destinadas a eliminar la causa raíz del problema. Por ejemplo, si se detecta que faltan respaldos regulares, la acción correctiva podría ser implementar un procedimiento de respaldo automatizado.

Figura 2. Proceso de gestión de no conformidades y acciones correctivas



Fuente: IVE Consultores, s.f., https://goo.su/GIGBf

La **no conformidad** está clara en cuanto a su significado e implicaciones. En cambio, una conformidad puede tener

matices que se clasifican en **observaciones** y **oportunidades de mejora.**

Observación —

es un hallazgo en el que existe cumplimiento, pero que, debido a cómo se desarrolla una actividad, tarea o proceso concreto, podría convertirse en un incumplimiento en el futuro. En el siguiente apartado se presentarán ejemplos de este tipo.

Oportunidad de mejora —

es un hallazgo en el que también existe cumplimiento, pero que, aun así, se determina, bajo criterios objetivos, que hay margen para optimizar una actividad, tarea o proceso concreto.

Cada hallazgo debe registrarse en un reporte (o formato de no conformidad) y conducir a una acción correctiva o preventiva. El área afectada analiza el hallazgo, propone una acción (por ejemplo, actualizar un procedimiento o configurar una nueva regla de firewall) y asigna un responsable y un plazo de cierre. Posteriormente, el auditor o coordinador debe verificar que la acción se haya implementado efectivamente.

Este seguimiento se documenta, incluso mediante una simple hoja de cálculo, para cerrar el ciclo de mejora. Por ejemplo, si el hallazgo es “no existe autenticación multifactor (MFA) en accesos remotos”, la acción podría ser “implementar MFA en un plazo de 30 días”, y luego el auditor revisa los registros o configuraciones para confirmar su ejecución.

Es crucial verificar la eficacia de la corrección y cerrar la no conformidad. Este ciclo —**auditoría → hallazgo → acción correctiva**— garantiza mejoras sostenibles en la seguridad.

1.3. Evidencia y cadena de custodia

Todo **hallazgo de auditoría** se basa en evidencia confiable, como registros de accesos, archivos de configuración, bitácoras, reportes de escáneres, entrevistas, fotografías, entre otros.

Es crucial conservar esta evidencia de manera correcta. Para preservar la validez de la prueba se utiliza la **cadena de custodia**, un procedimiento riguroso y documentado que registra cada paso en el manejo de la evidencia, garantizando la integridad y autenticidad de las pruebas

digitales desde el momento de su recopilación hasta su presentación.

La cadena de custodia consta de un proceso documentado de decomiso, custodia y traslado de las evidencias

Comienza en el lugar donde se detecta la evidencia (por ejemplo, el servidor donde se halló un registro de incidente) y continúa hasta su análisis y almacenamiento. En la práctica, se documenta:

- cuándo se recolectó la prueba (fecha y hora) y quién la recolectó;
- quién recibió la evidencia y cómo se almacenó (físico o digital);
- quién tuvo acceso a la evidencia;
- en qué momento fue analizada.

De esta forma se evita la pérdida, alteración o manipulación indebida de la evidencia. Por ejemplo, si un auditor extrae logs de un servidor, debería firmar un acta indicando la fecha y hora; cualquier manipulación posterior rompe la cadena y puede invalidar el hallazgo.

En una pyme, este proceso puede simplificarse mediante firmas digitales o registros controlados en hojas de cálculo o documentos físicos, siempre dejando constancia clara de cualquier manipulación de la evidencia. En la práctica, se puede usar un formato sencillo donde se registre cada evidencia relevante, con la firma de quien la custodia. Por ejemplo, «archivo de logs del 12/03/2025 obtenido por auditor X, transferido a USB, verificado por auditor Y el 13/03/2025».

Mantener la cadena de custodia evita cuestionamientos legales y asegura que las evidencias de auditoría sean confiables. Si la auditoría interna se utiliza en un proceso legal o como respaldo para una certificación, este registro documentado resulta esencial.

1.4. Reporte ejecutivo de auditoría

Al finalizar, los resultados se plasman en un reporte (o informe) de auditoría interna. El reporte de auditoría es el documento oficial que resume y transmite los resultados, es decir, los hallazgos, conclusiones y recomendaciones derivados de la auditoría. Debe entregarse a la alta dirección y a los responsables de las áreas auditadas, con un lenguaje claro y orientado a la toma de decisiones. Un reporte claro y profesional facilita que la gerencia comprenda las debilidades y asigne recursos para corregirlas.

La estructura recomendada incluye los siguientes elementos:

- **Resumen ejecutivo.** Un informe claro inicia con un resumen para la dirección, donde se destacan los hallazgos críticos, los riesgos detectados y las recomendaciones más relevantes, sin profundizar en detalles técnicos.

- **Introducción:** fecha, alcance, objetivos y normas o políticas auditadas.
- **Procesos auditados:** resumen de las áreas revisadas.
- **Cuerpo del informe:** se detallan los hallazgos respaldados por evidencias y su impacto, seguidos de las acciones correctivas propuestas y los responsables asignados.
- **Hallazgos clasificados:** listado de no conformidades, observaciones y oportunidades de mejora, cada una con una breve descripción.
- **Conclusiones generales:** evaluación global de la eficacia del SGSI.
- **Recomendaciones:** sugerencias de acciones preventivas o de fortalecimiento de controles.

Además, se clasifica el nivel de riesgo asociado a cada hallazgo (alto, medio o bajo) para facilitar la priorización, y se incorpora una tabla de acciones correctivas pendientes con las medidas a implementar, los responsables asignados y las fechas límite.

El reporte debe ser concreto y visual; incluir tablas o gráficos sencillos facilita la comprensión. Por ejemplo, puede mostrarse el número de hallazgos por área o un gráfico de «cumplimiento de auditorías vs. planificado». El informe debe destacar que cada hallazgo ha de ser claro y estar respaldado por evidencia, evitando términos subjetivos.

Al finalizar, es necesario discutir el informe con la dirección y planificar el seguimiento de las acciones. Un auditor interno eficaz entrega resultados útiles, no solo documentos, y promueve que el proceso de auditoría sea percibido como un motor de mejora continua y no como un trámite burocrático.

Actividades prácticas – Unidad

1. **Diseñar un miniprograma anual.** Identificar 2 o 3 procesos críticos de una pyme ficticia (por ejemplo, acceso a sistemas, gestión de respaldos) y definir un cronograma anual para auditarlos.

2. **Simular un hallazgo.** Elegir un proceso (por ejemplo, registro de incidentes) e imaginar un

posible incumplimiento. Luego, describir las acciones correctivas necesarias, incluyendo cómo verificar su efectividad.

3 **Practicar el registro evidencia.** Crear un ejemplo de acta de toma de evidencia (cadena de custodia) para un registro de sistema extraído, detallando quién lo tomó y dónde se guarda.

CONTINUAR

Unidad 2. Métricas y mejora

2.1. KPI/ KRI: cobertura, incidentes, tiempos

Las métricas son indicadores medibles que permiten cuantificar la eficacia y el desempeño del SGSI y el impacto de la auditoría. Dentro de las métricas se encuentran los **KPI** y los **KRI**.

- **KPI (*key performance indicator*):** miden el desempeño actual o histórico del sistema. Por ejemplo, porcentaje de cumplimiento de políticas, tiempo promedio de respuesta a incidentes.

- **KRI (*key risk indicator*):** alertan sobre riesgos potenciales. Por ejemplo, tasa de incidentes, vulnerabilidades sin parchear, etc.

En una pyme, por ejemplo, un KPI útil podría ser «porcentaje de controles implementados según plan», y un KRI podría

ser «número de incidentes de seguridad en el trimestre».

Los KRI o indicadores claves de riesgo son herramientas que permiten anticipar y mitigar posibles amenazas, antes de que estas se materialicen, protegiendo los objetivos o recursos de las industrias.

Otras métricas habituales incluyen tiempos medios, por ejemplo, las siguientes:

- **MTTD (*mean time to detect*).** Mide cuán rápido se detecta un incidente.
- **MTTR (*mean time to respond*).** Mide cuán rápido se resuelve un incidente.

Monitorear estos valores es importante: los datos de incidentes y sus tiempos permiten evaluar la eficacia del equipo de seguridad. Un equipo ágil de una pyme debería fijar objetivos, como «resolver el 80 % de los incidentes en 24 h», y medir su cumplimiento mediante indicadores simples en hojas de cálculo o herramientas gratuitas.

Es importante alinear las métricas con los objetivos de la pyme. Veamos algunos ejemplos:

- **Cobertura de controles:** porcentaje de activos revisados o protegidos; por ejemplo, porcentaje de servidores con parches al día.
- **Incidentes:** número de incidentes de seguridad por trimestre, clasificados por gravedad; por ejemplo, número de accesos no autorizados detectados.
- **Tiempos de respuesta:** tiempo promedio de detección y de respuesta ante incidentes.
- **Cumplimiento de auditorías:** porcentaje de auditorías realizadas frente a las planificadas.
- **Cierre de no conformidades:** porcentaje de hallazgos cerrados dentro del plazo establecido.

KRI vs. KPI: ¿cuáles son las diferencias?

En síntesis, los KRI se diseñan para prever amenazas —¿existen señales tempranas de un riesgo?—, mientras que los

KPI muestran resultados ya obtenidos. La diferencia temporal puede resumirse así:

- Los KPI presentan datos históricos de desempeño.
- Los KRI alertan sobre factores que podrían desencadenar incidentes futuros.

De este modo, una pyme podría informar que, en el último semestre, redujo el tiempo medio de respuesta de 10 a 6 horas (KPI) y, al mismo tiempo, que su KRI «porcentaje de empleados con entrenamiento en phishing» es del 30 %, lo cual indica un riesgo que aún debe gestionarse.

2.2. Cuadros de mando y *storytelling*

De este modo, una pyme podría informar que, en el último semestre, redujo el tiempo medio de respuesta de 10 a 6 horas (KPI) y, al mismo tiempo, que su KRI «porcentaje de empleados con entrenamiento en phishing» es del 30 %, lo cual indica un riesgo que aún debe gestionarse.

Un cuadro de mando es una vista gráfica de los indicadores que ayuda a contar la «historia» del estado de la seguridad. Un dashboard agrupa gráficos y tablas relevantes en una sola vista, lo que facilita identificar tendencias y brechas. Al presentar métricas, conviene utilizar gráficos sencillos (barras, líneas o pastel) y resaltar la información esencial para ejecutivos.

Por ejemplo, puede mostrarse un gráfico de pastel con el porcentaje de controles críticos implementados o una línea de tiempo con los incidentes reportados mes a mes.

No obstante, estos paneles solo muestran datos; un buen storytelling transforma esos KPI en narrativas comprensibles y persuasivas. El storytelling consiste en contextualizar los datos desde la perspectiva del negocio: más allá de cifras técnicas, se explica cómo esos valores impactan objetivos organizacionales.

Por ejemplo, en un dashboard puede observarse la disminución de vulnerabilidades parcheadas durante el mes, pero el relato debe aclarar que «gracias a la inversión en actualizaciones, se ha reducido el riesgo de brechas».

Como señala la experiencia en business intelligence, los dashboards requieren interpretación y explicación para audiencias no técnicas. En la práctica, se pueden usar herramientas gratuitas, como Google Looker Studio, Grafana o Excel, para crear gráficos simples (barras, líneas) y acompañar cada reporte con conclusiones breves. De esta manera, la dirección comprende no solo qué números cambian, sino también por qué son relevantes.

Al diseñar un dashboard eficaz, conviene enfocarse en pocos KPI (entre tres y cinco) y actualizarlos con regularidad, por ejemplo, de manera mensual. Resulta útil incluir métricas como la superficie de ataque (número de activos conocidos), vulnerabilidades detectadas, incidentes atendidos y formación de empleados. A modo de ejemplo, un dashboard para gerencia podría incorporar:

- número de tickets de seguridad abiertos y cerrados;
- porcentaje de parches aplicados en plazo;
- nivel de concientización (encuestas de phishing).

Google Looker Studio es una herramienta gratuita adecuada para crear cuadros de mando, ya que puede conectarse a Google Sheets y generar reportes visuales dinámicos sin costo. Otras opciones libres incluyen Metabase o Redash, que permiten construir dashboards a partir de bases de datos internas.

En el caso de las pymes, resulta útil emplear plantillas sencillas o tableros prediseñados gratuitos —por ejemplo, para métricas de incidentes o parches aplicados— y generar informes periódicos que sean visualmente atractivos y fáciles de interpretar.

2.3. *Roadmap* trimestral de controles

La hoja de ruta trimestral (roadmap) es un plan dinámico que se actualiza cada tres meses para definir las acciones y controles de seguridad prioritarios. A partir de la evaluación de métricas y de hallazgos previos, se determinan los controles o mejoras que deberán abordarse en el siguiente trimestre. Por ejemplo, tras analizar los incidentes y KPI, una pyme podría decidir reforzar el firewall en el primer trimestre e implantar monitoreo de logs en el segundo.

Un roadmap trimestral funciona como un plan de acción por fases para mejorar el SGSI. Después de cada auditoría o revisión de incidentes, se identifican las áreas que necesitan fortalecerse y se distribuyen en los trimestres posteriores. A modo de ejemplo:

- el roadmap de Q1 puede incluir «implementar autenticación multifactor» y «configurar respaldo automático»;
- Q2:, «capacitación en seguridad para todo el personal»;
- Q3, «auditoría de proveedores de cloud»; y así sucesivamente.

Este plan se alinea con los hallazgos de auditoría interna y con los KPI definidos. La principal ventaja de un roadmap trimestral es su flexibilidad, ya que permite ajustar el foco según la evolución de los riesgos reales.

La ventaja de un roadmap trimestral es su flexibilidad, ya que ajusta el foco según la evolución de los riesgos reales.

A nivel práctico, basta con un documento o tablero, como Google Sheets o Trello, donde se enlisten las iniciativas de seguridad, sus responsables y las fechas proyectadas. Cada trimestre se revisa su ejecución y se incorporan nuevas lecciones, siguiendo el ciclo de mejora continua.

Al confeccionar el roadmap, se recomienda involucrar al equipo de TI y a la dirección para estimar tiempos y recursos. Por ejemplo, la pyme podría asignar parte del presupuesto anual a proyectos de seguridad significativos. En entornos con pocos recursos, muchas acciones son de bajo costo, como la capacitación interna, el uso de software libre o la actualización de políticas.

Aunque no existe un estándar que regule esta práctica, su enfoque ágil permite mantener al equipo alineado y anticipar problemas antes de la siguiente auditoría anual. Además, un roadmap trimestral ayuda a distribuir la carga de trabajo y a mostrar avances periódicos en el dashboard. Cada trimestre se revisa el progreso: si un control no se completó, se reprograma o se reasigna antes del período siguiente, lo que garantiza la mejora continua del SGSI.

2.4. Lecciones aprendidas. Cambio de control

Las auditorías internas y las métricas generan lecciones aprendidas que deben retroalimentar el SGSI. Estas lecciones cierran el ciclo de auditoría y mejora. Tras cada auditoría o incidente, el equipo analiza qué funcionó y qué no.

Si se repite un hallazgo —una incidencia recurrente— es señal de que algún control resultó insuficiente. En ese caso, corresponde cambiarlo o reforzarlo. Por ejemplo, si en varias auditorías se detecta la falta de respaldos frecuentes de bases de datos (incidente: pérdida de datos), la lección aprendida es actualizar la política y el sistema de backups con carácter urgente.

Otra lección puede referirse a mejorar la detección de incidentes. Si el KPI «tiempo de detección» es elevado, podría requerirse implementar sistemas de monitoreo en tiempo real.

Este análisis se documenta y se incorpora al SGSI. Por ejemplo, si un control se demuestra ineficaz —o excesivo—, se ajusta o se reemplaza.

El «cambio de control» se refiere justamente a modificar o añadir controles basándose en la experiencia. Por ejemplo, si

durante la auditoría se comprobó que la rotación de contraseñas era débil, se puede concluir que el control vigente —por ejemplo, un cambio anual— no resulta suficiente y reemplazarlo por otro más exigente, como el cambio cada seis meses con verificación técnica.

Este proceso de retroalimentación fortalece el SGSI. Aunque no siempre existe una fuente normativa específica, las guías de calidad promueven documentar las lecciones aprendidas y actualizar los procedimientos.

En pymes, este registro puede quedar en minutas de reunión o en un informe interno; lo importante es cerrar el ciclo: una vez detectado un problema en auditoría, se actualizan las políticas y los controles antes de la siguiente revisión.

En la práctica, después de cada ciclo de auditoría y reporte, el equipo de seguridad se reúne para analizar los hallazgos y el desempeño de los indicadores. Los controles obsoletos se sustituyen por otros más eficaces y se ajustan los objetivos de los KPI según la nueva realidad de la empresa.

Este círculo virtuoso —«auditoría ⇒ acción ⇒ medición ⇒ aprendizaje»— es fundamental para que el SGSI evolucione y responda a riesgos emergentes.

Actividades prácticas

A continuación, se proponen actividades orientadas a consolidar los conceptos trabajados:

- Definir tres KPI y dos KRI para una pyme de servicios de TI. Por ejemplo: «% de cumplimiento de parches mensuales» (KPI) o «número de usuarios con MFA» (KRI). Explique cómo medirlos y qué meta establecería.

- Crear un pequeño *dashboard* en una hoja de cálculo con gráficos que muestren la evolución trimestral de incidentes y tiempos de respuesta. Acompáñelo con un breve resumen de *storytelling* sobre la tendencia observada.

- Simular un *roadmap*: listar cuatro controles de seguridad por trimestre que una empresa ficticia de 20 empleados podría implementar, basándose en métricas hipotéticas actuales.

Otras actividades

- **Planificar auditorías.** Enunciar un programa anual de auditorías internas para una pyme ficticia. Definir qué procesos se auditarán en cada trimestre, con qué alcance y quién los realizará. Se puede usar Trello o Google Sheets para crear un calendario visual con columnas por trimestre y tarjetas por auditoría, indicando al responsable. También conviene integrar los criterios y los objetivos de cada auditoría (cumplimiento, seguimiento, mejora).

- **Redactar un hallazgo.** Describir un caso realista; por ejemplo, se detecta que no existe documentación de políticas de contraseñas. Clasificar el hallazgo, como «no conformidad» con el requisito 4.4 de ISO 27001, y proponer la acción correctiva, por ejemplo, «desarrollar e implementar la política de contraseñas en 30 días». Registrar evidencia —como capturas de pantalla de sistemas sin política— y asignar un responsable.

- **Crear una cadena de custodia simulada.** Crear un formato simple, como una tabla en Google Sheets, para registrar la cadena de custodia de una evidencia de auditoría. Definir columnas como «descripción de evidencia»,

«fecha/receptor/entregador» y «ubicación de almacenamiento». Simular datos —por ejemplo: evidencia «registro de logs del 01/2025», quién la custodió y cuándo— a fin de practicar la documentación.

- **Redactar un informe ejecutivo breve.** Redactar un informe dirigido a la gerencia a partir de los hallazgos anteriores. Incluir una introducción, un resumen de hallazgos clasificados y una recomendación destacada. Se pueden usar viñetas o tablas para presentar los hallazgos y las acciones pendientes.

- **Definir KPI.** Proponer al menos tres indicadores para la seguridad de la información en la pyme; por ejemplo, «% de sistemas parchados», «número de incidentes reportados» o «tiempo medio de respuesta». Para cada indicador, describir cómo se calcularía (fuentes de datos) y cuál sería el objetivo esperado.

- **Diseñar un tablero simple.** Crear un cuadro de mando básico con datos ficticios. Se puede usar Google Sheets para simular los datos y Google Looker Studio para conectarlos y

graficarlos (barras, líneas o pastel). Mostrar al menos dos métricas distintas.

- **Elaborar un roadmap trimestral.** Esquematizar un plan de mejoras para el primer año, listando controles o proyectos de seguridad para cada trimestre, como capacitación, implementaciones técnicas o revisiones de documentación. Priorizar en función de los hallazgos previos.

- **Analizar lecciones aprendidas.** A partir de un escenario —por ejemplo, incidentes recurrentes de phishing— describir qué control modificar o añadir. Explicar cómo el nuevo control, como la autenticación multifactor o el entrenamiento trimestral, cerraría la brecha identificada.

Laboratorio guiado

En este laboratorio práctico, los participantes aplicarán herramientas gratuitas para poner en práctica lo aprendido.

1. **Trello o Excel para el programa de auditoría**

- Crear un tablero en Trello (o una hoja de cálculo) llamado «Auditorías ISMS».
- Añadir tarjetas o filas con la descripción de cada auditoría planificada; por ejemplo, «auditoría Q1: accesos físicos y TI». Asignar fechas estimadas y un responsable.
- Adjuntar checklists o listas de verificación básicas en cada tarjeta, como «revisar ingreso de personal, llaves y credenciales».
- Como alternativa, se puede usar Google Calendar compartido para registrar los eventos de auditoría.

2 **Google Forms para la recolección de hallazgos**

- Crear un formulario en Google Forms titulado «Registro de hallazgos ISMS».
- Incluir preguntas como fecha, auditor, área auditada, tipo de hallazgo (no conformidad, observación u oportunidad de mejora), descripción, acción recomendada, responsable y fecha límite.
- Simular la carga de al menos tres hallazgos ficticios en el formulario. Los

resultados se guardarán automáticamente en Google Sheets.

- Observar cómo Google Sheets consolida los hallazgos; este archivo funcionará como el registro central de hallazgos de la pyme.

3

Dashboard con Google Looker Studio

- En Google Sheets (o en un archivo CSV), crear un conjunto de datos de ejemplo con columnas como nombre de métrica (por ejemplo, «% parcheo Q1»), valor y período.
- Ingresar datos ficticios para tres métricas, como «% parcheo: 75, 85, 95», «número de incidentes: 5, 3, 1» y «tiempo medio de respuesta: 10 h, 8 h, 5 h».
- Abrir Google Looker Studio, crear un reporte nuevo y conectar la hoja de Google Sheets como fuente de datos.
- Insertar gráficos; por ejemplo, un gráfico de barras para «% parcheo por trimestre» y un gráfico de líneas para «incidentes vs. tiempo». Personalizar los títulos según corresponda. De esta forma se genera un cuadro de mando interactivo sin costo.

4

Revisión y ajustes

- Revisar los datos del dashboard junto con los responsables; en el laboratorio puede simularse esta interacción con compañeros. Interpretar los resultados, como si mejoró el parcheo o si disminuyó el número de incidentes.
- Añadir una historia breve al dashboard en forma de texto o comentario que explique la tendencia; por ejemplo, «tras aplicar el plan de parches, los incidentes disminuyeron de 5 a 1».

5

Uso de Metabase o Redash (opcional avanzado)

- Si la pyme cuenta con conocimientos básicos de TI, se puede instalar la versión gratuita de Metabase o Redash en un servidor local o en un servicio ligero de nube.
- Cargar los mismos datos de ejemplo en su base de datos y replicar un dashboard. Esto permite demostrar el uso de soluciones de business intelligence de código abierto en una pyme.

- Este paso es optativo; como alternativa, puede mencionarse como una mejora futura, orientada a realizar analítica más profunda mediante estas herramientas.

6 **Revisión del roadmap**

- En una pizarra o en un documento compartido, listar los controles pendientes clasificados por trimestre. Por ejemplo, «Q1: implementar MFA; capacitación en contraseñas. Q2: actualizar antivirus; realizar backup externo».
- Cada integrante puede sugerir tareas adicionales basadas en el escenario. Es importante incluir acciones de corto plazo y visualizar su cronograma; esto puede hacerse en Trello mediante una lista por trimestre.

Este laboratorio demuestra que, con herramientas gratuitas como Trello, Google Workspace y Looker Studio, una pyme puede planificar auditorías, registrar hallazgos y visualizar métricas sin necesidad de invertir en software costoso.

Caso de estudio integrador 1

En este laboratorio se aplica lo aprendido mediante herramientas sin costo.

- **Planificación de auditoría.** Utilizar Google Sheets o Trello para crear un programa anual de auditorías con fechas, procesos y auditores. Este ejercicio permite priorizar áreas críticas según el tamaño y los riesgos de la empresa.

- **Gestión de hallazgos.** Con la misma herramienta (Sheets o Trello), modelar un registro de hallazgos. Por ejemplo, simular una no conformidad e ingresar la descripción, la acción correctiva asignada, el responsable y la fecha de verificación. Este ejercicio muestra cómo realizar el seguimiento de las acciones.

- **Evidencia digital.** Instalar y usar OSSEC/Wazuh (gratuito) o, en su defecto, revisar logs simples de Windows o de un servidor Linux. Practicar cómo extraer un log relevante y documentar su cadena de custodia en un acta sencilla, que puede elaborarse en un documento de texto indicando quién accedió al log, cuándo y con qué propósito.

- **Cuadro de mando.** Recolectar datos de ejemplo, como el número mensual de incidentes y los tiempos promedio de respuesta, y cargarlos en Google Looker Studio (gratuito) o Grafana (gratuito, requiere instalación). Crear gráficos de barras o de líneas. Luego, redactar un breve storytelling. Elaborar un informe simple, por ejemplo, en PowerPoint, que resuma lo visualizado e iniciar con una frase como «en el primer semestre observamos que...».

- **Roadmap y lecciones.** En Trello, crear un tablero tipo Kanban con las columnas «Q1», «Q2», «Q3» y «Q4». Añadir tarjetas con cada control planificado por trimestre. En cada tarjeta incluir la lección que motiva ese control; por ejemplo, «Q2: implementar MFA – lección: muchos accesos descubiertos con credenciales comprometidas en Q1».

Este laboratorio ejemplifica con herramientas asequibles cómo una PYME puede gestionar su SGSI sin software pago, aprovechando entornos colaborativos gratuitos (Google Workspace, Trello) y soluciones open source básicas.

Caso de estudio integrador 2

InnovaTextil S.A. es una empresa con 30 empleados dedicada a productos textiles que implementó un SGSI básico y ahora realizará su primer ciclo de auditoría interna.

1 Auditoría y hallazgos

El gerente de TI elabora un programa anual (Unidad 1) en el que planifica auditar los procesos de acceso lógico en febrero, el respaldo de información en mayo y los proveedores críticos en noviembre.

Durante la auditoría de respaldo —mayo— se detecta un hallazgo: «las copias de seguridad no se almacenan fuera del sitio», tal como exige la política interna. Se documenta la no conformidad y se propone como acción correctiva establecer un respaldo en nube y en medios físicos fuera de la oficina. Se asigna un responsable para implementarlo dentro de un plazo de dos meses.

Se crea un acta de evidencia, firmada por el auditor y por el responsable de TI, siguiendo la cadena de custodia. El informe de auditoría presenta este hallazgo en el resumen

ejecutivo, destaca su impacto —riesgo de pérdida de datos— y recomienda una acción urgente.

2

Métricas y dashboard

Con base en los incidentes del primer semestre, InnovaTextil define KPI como el porcentaje de respaldos realizados según plan y el tiempo medio de recuperación ante una prueba de fallo (MTTR). También mide KRI, como la cantidad de intentos de intrusión detectados en firewalls y el tiempo medio de respuesta ante cada alerta.

Se confecciona un cuadro de mando simple en Excel que muestra estos indicadores mensualmente. El reporte gráfico evidencia que, tras aplicar las acciones correctivas de respaldo, el cumplimiento pasó del 60 % al 100 % y el MTTR se redujo de 4 horas a 1 hora. Se acompaña con una narrativa dirigida a la gerencia: «gracias a la nueva estrategia de respaldos, hemos asegurado la continuidad del negocio y reducido a la cuarta parte el tiempo de recuperación ante incidentes críticos».

Las gráficas se presentan en la reunión de revisión gerencial junto con la justificación de las decisiones adoptadas.

3

Roadmap y lecciones

A partir de estos resultados, InnovaTextil elabora un roadmap para el siguiente trimestre. De sus lecciones aprendidas se determinan:

- Q3: implementar autenticación multifactor (aprendizaje: accesos inseguros).
- Q4: capacitar al personal en ciberhigiene (aprendizaje: repetición de contraseñas).

Cada control se documenta en un tablero —por ejemplo, en Trello— donde se registra la lección que motivó el cambio. De este modo, el SGSI evoluciona alineado con la experiencia práctica.

Este caso integra auditoría, correcciones y métricas en una pyme realista, mostrando cómo cerrar el ciclo de mejora continua.

Caso de estudio integrador 3

TecnoAgro S.R.L. es una empresa argentina de tecnología agrícola con 20 empleados. Su infraestructura es modesta: cuentan con un servidor local con información de clientes y un servicio de correo basado en la nube. No disponen de un departamento de TI dedicado; varias funciones son realizadas por un generalista. Tras un incidente reciente —un correo de phishing permitió el acceso no autorizado al sistema contable—, la gerencia decide fortalecer el SGSI. Se convoca a un auditor interno, un empleado de sistemas, para iniciar acciones de auditoría y métricas.

1

Programa anual de auditorías

El auditor interno, junto con la gerencia, define un programa con el siguiente esquema trimestral:

- **Q1.** Control de accesos (revisión de permisos de usuarios, contraseñas predeterminadas y controles de ingreso físico).
- **Q2:** gestión de vulnerabilidades (verificación de parches en servidores y estaciones de trabajo).

- **Q3:** políticas y procedimientos (existencia y aplicación de políticas de seguridad, registro de backups).
- **Q4:** concientización y respuesta (simulacros de phishing y revisión de planes de emergencia).

Para cada auditoría se asignan fechas tentativas y el auditor se declara responsable, reportando directamente al dueño de la empresa.

2 Hallazgos y acciones

En la primera auditoría (Q1), el hallazgo principal fue que ningún acceso remoto al servidor requería autenticación multifactor; se clasificó como no conformidad. Se documentó con evidencia obtenida desde la consola de administración, donde la opción de MFA no estaba activada. La acción correctiva propuesta fue implementar MFA en un plazo de 30 días.

Otro hallazgo, clasificado como observación, fue que el listado de acceso físico al edificio no se actualizaba desde hacía un año. Se recomendó mantener un control de visitas

actualizado. El auditor registra ambos hallazgos en el formato correspondiente —puede usar Google Forms, como en el laboratorio— y asigna responsables y fechas.

3 **Evidencia y custodia**

Cada hallazgo se acompaña de su evidencia: capturas de pantalla del servidor —por ejemplo, usuario «root» sin MFA— y copia del registro de accesos al edificio. Estas evidencias se guardan en una carpeta compartida con control de acceso, y se documenta en un registro quién las recolectó y dónde se almacenan, asegurando la cadena de custodia.

Por ejemplo, el auditor anota: «captura de pantalla del sistema (C:/evidencia/MFA_off_2025-03-10.png) – obtenida por auditor X el 10/03/2025 y guardada en el Drive de la empresa (verificado con firma digital)».

4 **Reporte ejecutivo**

Al finalizar la auditoría de Q1, el auditor elabora un reporte sintético para la dirección.

Incluye una introducción breve con el alcance y los objetivos, y un resumen de los hallazgos:

- **Hallazgos mayores:** falta de MFA en accesos remotos, sin impacto evidenciado aún.
- **Observaciones:** registro de ingreso físico desactualizado.

El informe incorpora recomendaciones —por ejemplo, «implementar MFA y revisar credenciales admin»— y una lista de acciones con sus responsables; por ejemplo: «jefe de sistemas: MFA en 30 días» y «gerente administrativo: actualizar listas en 15 días». Este reporte se entrega al CEO y al encargado administrativo.

5 **Definición de métricas**

Paralelamente, se eligen indicadores para realizar el seguimiento:

- **KPI1: porcentaje de dispositivos actualizados.** Se medirá como el porcentaje de computadoras y servidores con parches al día. El objetivo inicial es alcanzar el 90 %.

- **KPI2: número de incidentes mensuales.** Corresponde al conteo de incidentes de seguridad detectados. La meta es mantenerlos por debajo de dos por mes.
- **KRI1: porcentaje de usuarios con capacitación.** Mide el porcentaje de empleados que completaron la capacitación anual de seguridad. El valor inicial es 0 %, con el objetivo de llegar al 100 %.
- **KRI2: tasa de phishing detectado.** Número de correos de phishing capturados por la herramienta, lo que permite anticipar campañas maliciosas.

Estas métricas se registrarán trimestralmente. Se acuerda que el auditor presentará un informe cuantitativo en cada reunión de dirección, mostrando tendencias que indiquen mejoras o áreas que aún requieren atención.

6

Cuadro de mando

El auditor crea un tablero sencillo en Google Looker Studio, arrastrando los datos ingresados en Google Sheets. El tablero incluye un gráfico de barras para «% de

dispositivos parchados» por mes, un gráfico de líneas para «incidentes mensuales» y un medidor (gauge) para «capacitación (%) completada».

Este dashboard se presenta en la reunión trimestral de dirección. Su lectura visual permite identificar de inmediato la mejora —por ejemplo, la barra de parches aumenta del 60 % al 80 % tras las acciones implementadas— y comprender qué aspectos requieren atención, como la necesidad de que la línea de incidentes disminuya con el tiempo.

7

Roadmap y mejora continua

Con base en los hallazgos y las métricas, el auditor coordina un roadmap con la siguiente planificación trimestral:

- **Q2.** Habilitar MFA en todos los accesos, renovar el antivirus y capacitar al personal (pendiente del KRI de usuarios con entrenamiento).
- **Q3:** realizar pruebas de respaldo, implementar políticas formales de contraseñas y comenzar los registros de auditoría de la red.

- **Q4:** ejecutar un simulacro de phishing y actualizar el plan de continuidad.

Al finalizar cada trimestre, se revisan los objetivos y se valida la evidencia correspondiente; por ejemplo, confirmar que el MFA está activo y que los backups funcionan adecuadamente. La lección aprendida de Q1 fue que la seguridad de acceso resultaba insuficiente, por lo que se reforzará el control de identidad, constituyendo un cambio de control.

8

Resultados obtenidos

Tras un año, TecnoAgro S.R.L. alcanza un 100 % de cobertura de parches, completa el 50 % del entrenamiento —aún en curso— y reduce sus incidentes mensuales a uno. El CEO destaca que el SGSI dejó de ser «papel» y pasó a convertirse en un proceso vivo, gracias al uso coordinado de auditorías y métricas.

Este caso muestra cómo una pyme argentina puede integrar auditoría interna y métricas prácticas para mejorar su seguridad de manera ordenada y sin realizar una gran inversión.

CONTINUAR

Referencias

IVE Consultores, (s.f.). Cómo estudiar no conformidades según ISO 9001 y ayudar a que tu organización sea más robusta [método infalible]. https://iveconsultores.com/no-conformidad-iso-9001/

Laprovittera, C. (2025). Cómo Iniciarse como Pentester en 2025. https://achirou.com/como-iniciarse-como-pentester-en-2025/

National Institute of Standards and Technology [NIST]. (2008). Technical Guide to Information Security Testing and Assessment (NIST Special Publication 800-115). National Institute of Standards and Technology.

OWASP. (2014). OWASP Testing Guide (Version 4.0). The OWASP Foundation

CONTINUAR

Lección 4 de 4

Descarga en PDF