Elévate Perú

SESIÓN 4

AUDITORÍA Y MEJORA CONTINUA

Sistema de Gestión de Seguridad de la Información — ISO/IEC 27001:2022

EXTRACTO · VISTA PREVIA

Gestión documental, indicadores, auditoría interna ISO 19011, no conformidades, acciones correctivas y mejora continua (PHVA)

Contenido

Presentación de la Sesión

La Sesión 4 del diplomado en Sistema de Gestión de Seguridad de la Información — ISO/IEC 27001:2022 aborda el cierre del ciclo de gestión: cómo se documenta la evidencia del SGSI, cómo se mide su desempeño, cómo se audita internamente conforme a la norma ISO 19011, y cómo las no conformidades detectadas se convierten en acciones correctivas que retroalimentan la mejora continua.

En el contexto peruano, estos procesos cobran especial relevancia: el Instituto Nacional de Calidad (INACAL) adopta la ISO/IEC 27001 como Norma Técnica Peruana (NTP-ISO/IEC 27001), y la Secretaría de Gobierno y Transformación Digital (SGTD) de la PCM exige a diversas entidades públicas la implementación de un SGSI certificable. Además, la Ley N.° 29733 de Protección de Datos Personales exige evidenciar controles documentados de seguridad ante la Autoridad Nacional de Protección de Datos Personales.

Gestión Documental

La información documentada es la evidencia de que el SGSI funciona como se planificó (Cláusula 7.5 de la ISO/IEC 27001:2022). Sin documentación controlada, no hay forma de demostrar ante un auditor —interno, de certificación, o incluso ante la SGTD en el caso de una entidad pública— que los controles del Anexo A realmente operan.

Jerarquía documental típica

1. **Política de Seguridad de la Información** — el documento de más alto nivel, aprobado por la Alta Dirección.
2. **Procedimientos** — describen cómo se ejecutan los procesos del SGSI (gestión de accesos, gestión de incidentes, etc.).
3. **Instrucciones de trabajo** — pasos operativos específicos para una tarea puntual.
4. **Registros** — evidencia objetiva de que algo ocurrió (bitácoras, actas, reportes).

Buenas prácticas (Cláusula 7.5)

- Control de versiones: identificación, fecha y responsable de cada cambio.
- Revisión y aprobación antes de publicar un documento.
- Control de acceso: quién puede leer, editar o distribuir.
- Retención y disposición: por cuánto tiempo se conservan los registros.
- Disponibilidad: el documento correcto, en el lugar y momento correcto.

> **Aplicación práctica**
> Una Política de Seguridad sin versión ni fecha de aprobación es la primera no conformidad típica que levanta un auditor de certificación en Perú. Verifica siempre el control de versiones antes de cualquier auditoría.

Indicadores del SGSI

Un SGSI sin indicadores es un sistema que no puede demostrar mejora ni eficacia (Cláusula 9.1). La norma ISO/IEC 27004:2016 ofrece la guía técnica para diseñar y gestionar estas mediciones.

% Incidentes en SLA

92%

Eficacia de respuesta ante incidentes

No conformidades recurrentes

3

Efectividad de acciones correctivas

Controles Anexo A implementados

87%

Cobertura de controles

Un buen indicador requiere meta clara, frecuencia de medición, fórmula definida, un dueño responsable de actuar sobre él, y una relación explícita con un objetivo o riesgo del SGSI. Reportar solo actividad (por ejemplo, «se realizaron 14 capacitaciones») sin meta ni resultado no constituye un indicador de eficacia.

Auditoría Interna y No Conformidades

La ISO 19011 orienta cómo se audita: con qué principios (integridad, presentación imparcial, debido cuidado profesional, confidencialidad, independencia, enfoque basado en evidencia y enfoque basado en riesgo) y qué proceso seguir en cinco etapas: iniciar la auditoría, preparar actividades, ejecutar la auditoría, preparar el informe y dar seguimiento.

Severidad	Definición
Mayor	Ausencia total o falla sistemática de un requisito. Riesgo alto.
Menor	Incumplimiento puntual que no compromete la eficacia del SGSI.
Observación	Oportunidad de mejora; aún no es incumplimiento.

Reflexión: *¿Cuál principio de la ISO 19011 es más difícil de sostener en tu organización, y por qué?*

Contenido completo en el Ebook

El Ebook desarrolla la metodología completa de acciones correctivas (5 Porqués, Ishikawa), el ciclo PHVA de mejora continua, un caso aplicado de análisis de causa raíz, un glosario técnico y el taller práctico de elaboración de un Plan de Auditoría.

Continúa tu aprendizaje

Este Extracto es una muestra del contenido completo de la Sesión 4. El Ebook completo (25 páginas) incluye el desarrollo íntegro de cada tema, casos aplicados con contexto normativo peruano, tablas de indicadores, checklists de auditoría, glosario y el taller práctico del Plan de Auditoría.

Accede al Ebook completo

Ingresa al Aula Virtual con tu usuario de estudiante en **www.institutoelevateperu.pe** o escríbenos por WhatsApp al **973 336 333** para obtener el material exclusivo de esta sesión.

Elévate Perú

MUCHAS GRACIAS

¿Preguntas, dudas o casos de su organización que quieran compartir?

973 336 333 | www.institutoelevateperu.pe