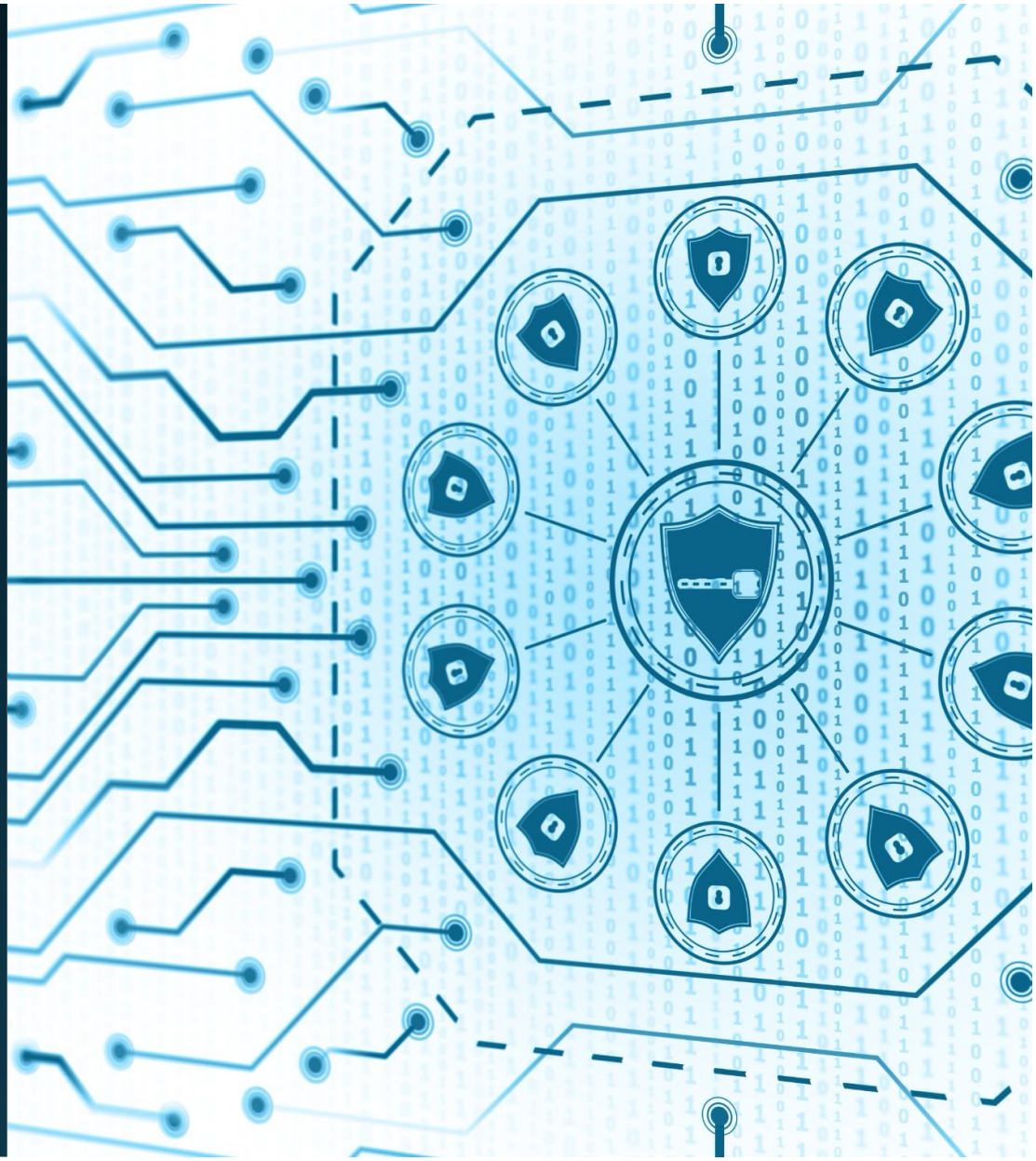
Ciberseguridad y Gobernanza

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Fortaleciendo el Sector Popular y Solidario

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Ciberseguridad y Gobernanza



Edgar Ramiro Sánchez Meza
Asesor Indepentiente en Gestión Estratégica de
Seguridad de la Información y Ciberseguridad

Agenda

01	REVISIÓN INICIAL – Análisis y diagnóstico
02	ORGANIZACIÓN – Alineación estratégica
03	GOBERNANZA – Hoja de ruta

01

REVISIÓN INICIAL

Análisis y diagnóstico

Revisión Inicial

Conceptos

01

📌 *“Los términos seguridad de la información y ciberseguridad suelen usarse indistintamente; sin embargo, la ciberseguridad es un subconjunto de la seguridad de la información. La seguridad de la información se ocupa de la información, independientemente de su formato....*

La ciberseguridad se ocupa de la protección de los activos digitales: todos los recursos incluidos en el hardware, el software y la información electrónica de red que se procesa, almacena en sistemas aislados o se transporta mediante entornos de información interconectados.

A diferencia de la seguridad de la información, la ciberseguridad no se ocupa de riesgos naturales, errores personales o seguridad física.”

Fuente: COBIT FOCUS AREA: Information Security Using COBIT 2019

Revisión Inicial

Conceptos

01

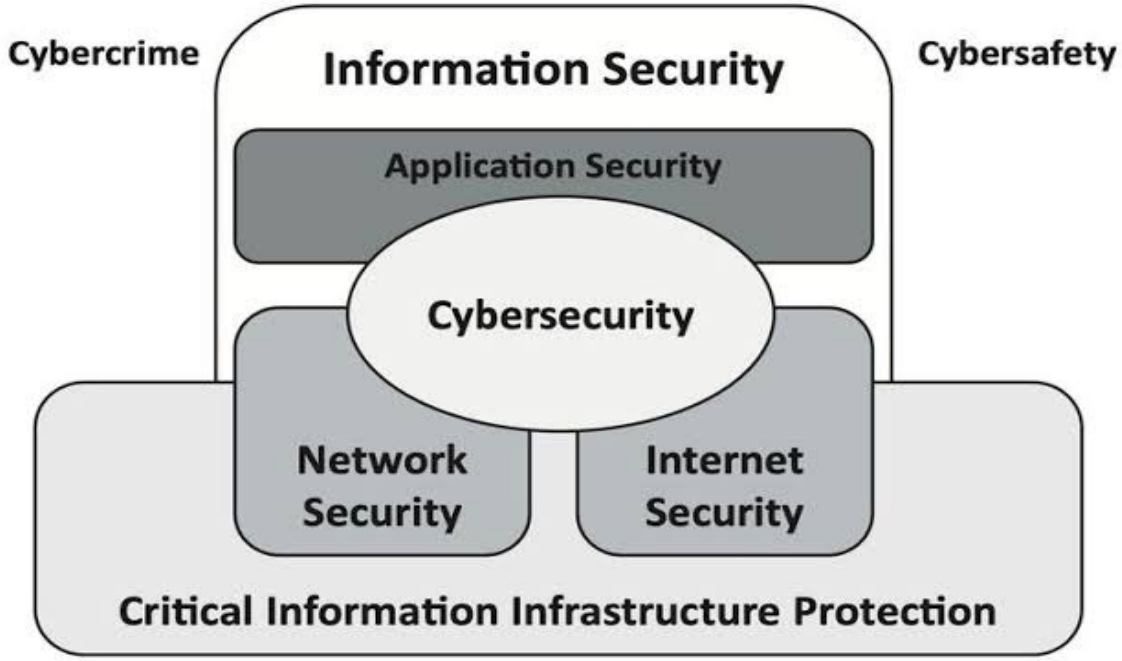


Figure 1 — Relationship between Cybersecurity and other security domains

ISO/IEC 27032 Ciberseguridad: Directrices para la seguridad en Internet

Revisión Inicial

Conceptos

01

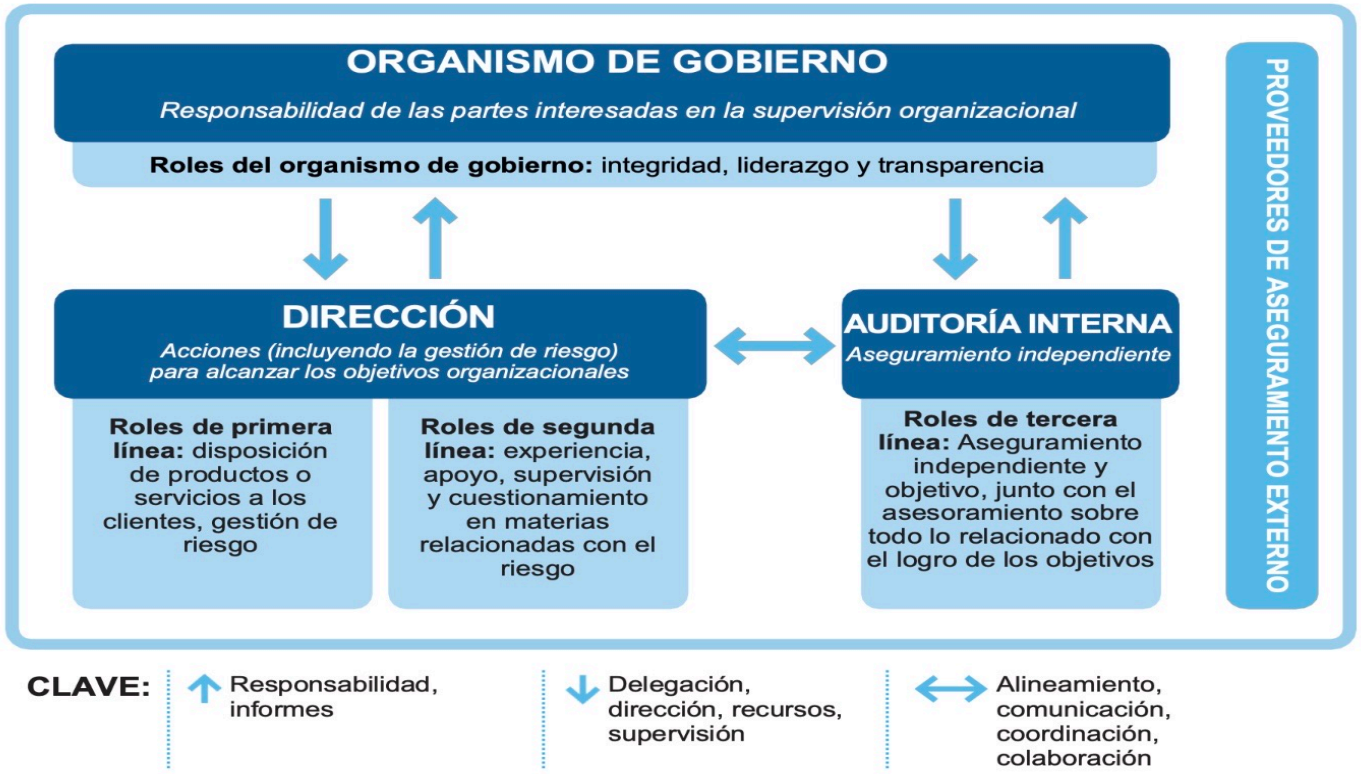
📌 *“Esta habilidad establece y mantiene un marco de gobernanza de seguridad de la información y procesos de apoyo para garantizar que la estrategia de seguridad de la información esté alineada con las metas y objetivos de la organización, que el riesgo de la información se gestione adecuadamente y que los recursos del programa se gestionen de manera responsable.”*

Fuente: COBIT FOCUS AREA: Information Security Using COBIT 2019

Revisión Inicial

El modelo de las tres líneas del IIA

01



PRIMERA LÍNEA
Opera · Ejecuta · Es dueña del riesgo

SEGUNDA LÍNEA
Supervisa · Define política · Monitorea

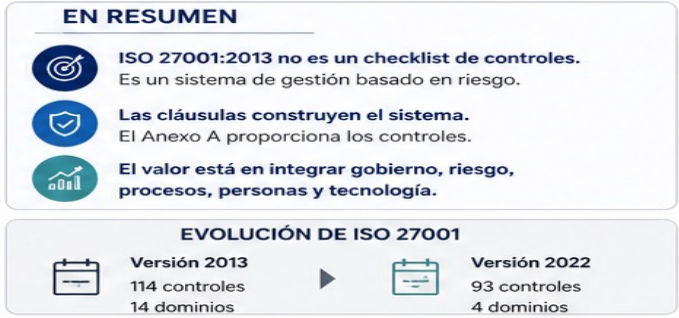
TERCERA LÍNEA
Asegura · Es independiente · Reporta al gobierno

Fuente: FLAI – Fundación Latinoamericana de Auditores Internos

Revisión Inicial

01

ISO/IEC 27001:2013 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información




INDICADORES CLAVE SGSI - REUNIÓN TRIMESTRAL DEL COMITÉ
Cumplimiento General ISO/IEC 27001
88%
Incidentes de Seguridad Reportados
Tiempo Promedio de Respuesta a Incidentes
Resultados de las Pruebas de Phishing
Entrenamiento de Concientización - Cobertura del Personal
94%
Comité de Seguridad de la Información

Revisión Inicial

01

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información

¿Qué contiene el Informe de Evaluación?

01 — Resultados de Auditoría Interna — ISO 9.2 · COBIT MEA04

- Hallazgos con evidencia
- Observaciones y oportunidades de mejora
- Estado de hallazgos de períodos anteriores
- No conformidades clasificadas C/M/m

02 — Métricas de Desempeño (KPIs) — ISO 9.1 · COBIT MEA02

- Cobertura SIEM sobre activos críticos
- Tiempo medio de detección (MTTD)
- % parches aplicados en plazo
- Incidentes por categoría y severidad

03 — Estado de Controles Annexo A — ISO 6.1.3 · SoA

- Controles implementados vs. declarados
- Controles excluidos con justificación
- Controles en proceso de implementación
- Brechas entre SoA y realidad operativa

04 — No Conformidades y Acciones — ISO 10.1 · APO12

- Análisis de causa raíz por NC
- Plazos de remediación y estado
- Acciones correctivas con responsable
- Recurrencia y tendencias

05 — Cumplimiento Regulatorio SEPS — MEA03 · Res. SEPS

- Cumplimiento de resoluciones SEPS
- Estado de obligaciones de reporte
- Notificaciones de incidentes enviadas
- Sanciones o alertas recibidas

ISO 27001:2022 Cláusula 9.3 — Revisión por la Dirección · El informe de evaluación es la base de toda decisión estratégica

Cómo leer el informe

1. **¿Qué es urgente?**
   Identificar las NCs críticas (C) y los KRIs en rojo. Son tu prioridad inmediata.
2. **¿Qué es importante?**
   Revisar el estado de los controles del Anexo A con mayor impacto en riesgo residual.
3. **¿Qué es estratégico?**
   Analizar tendencias: ¿qué métricas empeoran? ¿qué riesgos emergen?
4. **¿Qué va al Consejo?**
   Seleccionar los 3-5 ítems que requieren decisión o presupuesto del Consejo.
5. **¿Qué es para TI?**
   Separar las acciones técnicas que la 1ª línea puede ejecutar sin aprobación.

Revisión Inicial

01

ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información

	**PLANIFICAR**	4. Contexto de la Organización 5. Liderazgo 6. Planificación 7. Soporte	4. Incluye ciberespacio, grupos de interes relacionados con privacidad y la ciberseguridad. 5. Política de Seguridad de la información, ciberseguridad y proteccion de la privacidad. 6. Gestión de riesgos toma en cuenta activos del ciber espacio. 7. Incluye ciberseguridad y privacidad
	**HACER**	8. Operación Anexo A	- Planificación y Control Operacional - Evaluación y Tratamiento de riesgos y el uso del Anexo A. - Implementación de controles. - Controles de SI.
	**VERIFICAR**	9. Evaluación de Desempeño	- Planes de acción - Indicadores - Seguimientos de Auditoría (interna y externa) - Riesgos
	**ACTUAR**	10. Mejora	- Varias fuentes para la mejora continua (cambios reglamentarios, ciberespacio) - No conformidades y acciones correctivas

02

ORGANIZACIÓN

Alineación estratégica

Diagnóstico de Madurez

02

Análisis de los resultados del SGSI

Revisión de hallazgos, KPI, Planes de Acción, Riesgos

Identificación de activos críticos del negocio

Protección basada en el impacto financiero

Assessment de Madurez

Evaluación NIST

Alineación Estratégica

02

Definición del apetito del riesgo

Establecer formalmente cuanto está dispuesto a aceptar la Gerencia

Indicadores de riesgo

KPIs – KRIs.

Pasar de medir cuantos parches aplicamos, a “Cual es el riesgo residual de perdida financiera por ciberataques”

Actualización del Comité de Seguridad de la Información

Evolucionar el Comité de Seguridad hacia un rol consultivo de riesgos de negocio, no solo técnico

Operatividad Productiva y Resiliencia 02

Inteligencia de Amenazas

Anticipar ataques basados en el perfil de la empresa

Automatización

Respuesta a incidentes

Plan de continuidad de ciberseguridad

Recuperación ante desastres con un enfoque específico.

Cultura y mejora continua estratégica 02

Programa de Capacitación

Capacitación a líderes no técnicos y a terceros. (Scribd)

Simulacros de crisis

Toma de desiciones de Directorio

Auditoría

Servicios digitales seguros

Alineación Estratégica

02

NIVEL	RELACIÓN
Objetivo estratégico	Continuidad del negocio
Riesgo	Interrupción de banca digital
KPI	Exposición a vulnerabilidades críticas
Decisión	Priorizar

Alineamiento

02

Objetivo	NIST
Actualizar conjunto de políticas	Gobernar
Crear un comité de gestión de riesgos cibernéticos	Identificar
Programa para mejorar la cultura y el comportamiento	Proteger
Elabore un programa de gestión de amenazas.	Detectar
Mejorar el plan de respuesta ante incidentes	Responder
Actualizar el plan de continuidad del negocio	Recuperar

Gobierno – Actualización de Políticas

Actividades Gartner → Control ISO

- Afinar Políticas→ 5.01 Políticas de seguridad
- Afinar Métricas→ 5.35 Revisión independiente
- Retroalimentación → 5.36 Cumplimiento de políticas

5.01

Políticas de seguridad

Marco normativo base — incluye política sobre IA generativa y emergentes

5.02

Roles y responsabilidades

Define quién actualiza y aprueba el policy suite (CISO, propietarios)

5.35

Revisión independiente

Auditorías externas para capturar feedback y validar el policy suite

5.36

Cumplimiento de políticas

Verifica adherencia — cierra el loop de definir métricas.

5.31

Requisitos legales/regulatorios

Base para políticas que cubran cumplimiento normativo e IA

5.37

Procedimientos documentados

Operacionaliza las políticas — sin procedimientos quedan en papel

Identificar · Crear un Comité de Ciber Riesgos

Actividades

- Identificar los principals riesgos → 5.09 Inventario + 5.07 CTI
- Alinear los controles de soporte → 5.12 Clasificación

5.09

Inventario de activos

Sin inventario completo no se pueden identificar los top risks

5.12

Clasificación de información

Prioriza qué activos tienen mayor impacto al ser comprometidos

5.07

Inteligencia de amenazas (CTI)

Alimenta identificación de top risks con inteligencia actualizada

5.21

Cadena de suministro TIC

Alinea controles con riesgos heredados de terceros proveedores

5.19

Seguridad con proveedores

El comité debe cubrir riesgos de terceros — 60% de incidentes graves

5.02

Estructura del comité

Formaliza el cyber risk committee con roles y autoridad formal

Proteger · Programa para mejorar la cultura y el comportamiento

Actividades

- Alcance del programa → 6.03 Concienciación + 6.07 Teletrabajo
- Crear champions → rol de embajadores
- Herramientas de entrenamiento de IA → formación adaptada por rol

6.03

Concienciación y formación

Núcleo del programa — phishing simulado, formación por rol.

6.07

Trabajo remoto

El alcance incluye comportamiento seguro fuera de oficina.

8.05

Autenticación segura (MFA)

El programa incluye adopción de MFA — cambio cultural, no solo técnico

5.15

Control de acceso

Mínimo privilegio — requiere cambio de comportamiento en usuarios

8.07

Protección contra malware (EDR)

Complementa el programa de comportamiento con controles técnicos

8.23

Filtrado web (proxy/DNS)

Bloquea phishing — refuerza técnicamente el comportamiento Seguro.

Detectar · Elabore un programa de gestión de amenazas.

Actividades

- Mejorar el seguimiento → 8.16 SIEM + 8.15 Logging
- Actualizar el SOC → 8.20 IDS/IPS + 8.08 Vuln mgmt
- Inteligencia de amenazas → 5.07 CTI

8.16

Monitorización continua (SIEM)

Corazón del SOC — detección en tiempo real de comportamiento malicioso

8.15

Logging y registros

Sin logs completos no hay detección — alimenta el SIEM

5.07

Inteligencia de amenazas (CTI)

Integra feeds IOCs/TTPs al SOC — 'Integrate threat intelligence'

8.08

Gestión de vulnerabilidades

Scanning continuo — visibilidad de exposiciones activas

8.20

Seguridad en redes (IDS/IPS)

Sensor de detección en la red — complementa visibilidad del endpoint

8.17

Sincronización de relojes (NTP)

Correlación en SIEM requiere timestamps precisos

Responder · Mejorar el plan de respuesta ante incidentes

Actividades

- Actualizar los playbooks → 5.24 IRP + 5.26 Respuesta
- Implementar postmortem → 5.27 Lecciones aprendidas

5.24

Planificación IRP

Define estructura, roles, escalación y playbooks por tipo de incidente

5.25

Evaluación y triage de eventos

Proceso de triage para decidir si un evento es incidente

5.26

Respuesta a incidentes

Playbooks de contención y erradicación — el corazón del roadmap

5.27

Lecciones aprendidas

Formaliza el postmortem — mejora continua del IRP tras cada incidente

5.28

Recopilación de evidencias

Preservación forense — requisito para investigaciones y litigios

6.08

Reporte de eventos

El IRP empieza cuando alguien reporta — el canal debe estar en el playbook

Recuperar · Actualizar el plan de continuidad del negocio

Actividades

- Realizar BIA → 5.30 Continuidad TIC (RTO/RPO)
- Diseñar Plan → 8.13 Backups + 8.14 Redundancia
- Implementar plan → pruebas BCP documentadas

5.29

Seguridad durante interrupción

Mantiene controles activos durante crisis — el BCP preserva la seguridad

5.30

Continuidad TIC (RTO/RPO)

Define RTO/RPO para sistemas críticos — el BIA requiere este análisis

8.13

Copias de seguridad

Backups probados y aislados — pilar de recuperación ante ransomware

8.14

Redundancia de sistemas

Alta disponibilidad — diseño del BCP para cubrir gaps del BIA

5.23

Continuidad en cloud

El BCP moderno incluye recuperación de cargas cloud — nuevo 2022

5.35

Pruebas del BCP

Simulacros y pruebas de recuperación documentadas y revisadas

Alineamiento

02

1. EXPOSICIÓN DE RIESGO (MAPA DE CALOR)

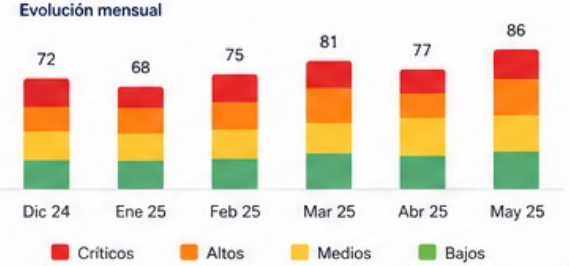
TOP 8 RIESGOS

1. Ransomware / Malware
2. Fuga de información
3. Interrupción de servicios TI
4. Accesos no autorizados
5. Fraude digital
6. Fallas en aplicaciones críticas
7. Errores humanos
8. Vulnerabilidades sin parchear

2. INCIDENTES (ÚLTIMOS 6 MESES)

Total incidentes	Críticos	Altos
86	9	18

Evolución mensual



3. VULNERABILIDADES

Críticas	312 (13%)
Altas	681 (28%)
Medias	1,021 (42%)
Bajas	404 (17%)

Variación vs. mes anterior	Críticas abiertas >30 días
-7%	48

4. CUMPLIMIENTO DE CONTROLES (ISO 27001)

Cumplimiento global

Control de Acceso	85%
Gestión de Activos	76%
Seguridad en Operaciones	72%
Protección de Datos	80%
Gestión de Incidentes	75%
Continuidad del Negocio	79%

5. ESTADO DE INICIATIVAS ESTRATÉGICAS

8	En ejecución
9	En planificación
4	En revisión
2	En riesgo / retraso

% avance promedio general 64%

6. RIESGO DE TERCEROS

Bajo	62 (40%)
Medio	58 (27%)
Alto	28 (18%)
Crítico	8 (5%)

Evaluaciones recientes (últ. 90 días)	Proveedones críticos sin evaluación
32	5

El problema de la terminología es real y documentado académicamente
https://www.researchgate.net/publication/366716821_Cybersecurity_vs_Information_Security

Los directorios entienden el riesgo, pero no saben cómo articularlo
https://news.mit.edu/2024/now-corporate-boards-have-responsibility-cybersecurity-too-0429

Solo el 39% de los directorios tiene comprensión proactiva del tema
https://hbr.org/2025/05/boards-need-a-more-active-approach-to-cybersecurity

Solo el 12% de las empresas del S&P 500 tiene un experto real en ciberseguridad en su directorio
https://corpgov.law.harvard.edu/2023/10/10/state-of-cyber-awareness-in-the-boardroom/

Alineamiento - Comunicación

02

EL PROBLEMA

- ✓ Desconexión entre lenguaje técnico y negocio
- ✓ Impacto: decisiones reactivas y baja inversión

PERSPECTIVA DEL DIRECTORIO

- ✓ Interés en riesgo, impacto financiero y continuidad
- ✓ No en herramientas ni detalles técnicos
- ✓ Hablar en impacto económico
- ✓ Presentar riesgos críticos
- ✓ Proponer decisiones claras

ALINEACIÓN PREVIA

- ✓ Coordinar con CIO, Riesgos y Legal
- ✓ Definir 3 mensajes clave
- ✓ Llegar con decisión solicitada

Alineamiento - Comunicación

02

TRADUCCIÓN DEL RIESGO

- ✓ Vulnerabilidad → Exposición
- ✓ Incidente → Impacto financiero
- ✓ Control → Reducción de riesgo

GOBERNANZA

- ✓ ISO 27001, COBIT, NIST como referencia
- ✓ Comunicar nivel de madurez vs industria

MÉTRICAS CLAVE

- ✓ Riesgo residual
- ✓ Tendencia
- ✓ Tiempo de respuesta
- ✓ Impacto económico

03

GOBERNANZA

Hoja de ruta

Enfoque

03

SGSI	CIBERSEGURIDAD
Cumplimiento	Riesgo
Controles	Amenazas
Auditoría	Operación
Interno	Impacto al cliente

Resumen

03

	EVALUACIÓN DE DESEMPEÑO	CIBERSEGURIDAD ESTRATÉGICA
Enfoque	Cumplimiento (Checklist)	Resiliencia y Continuidad
Prioridad	Control de Procesos	Protección de activos críticos
Rol de TI	Ejecutor Técnico	Socio estratégico del negocio
Métrica	% de Cumplimiento de controles	Reducción del impacto financiero

Gobernanza Ciberseguridad

03

Alineación Estratégica

Comité de Seguridad de la Información.

Liderazgo y compromiso de la Alta Dirección.

Definición de apetito del riesgo.

Marco Normativo y Estándares

ISO 27001:2022

NIST CSF 2.0

COBIT

Gestión de riesgos Cibernéticos

Servicios digitales seguros

Magerit o ISO 31000

BIA

PHVA

Monitoreo y reportes

Gestión de Terceros

Evaluación de seguridad de proveedores

Acuerdos contractuales

Monitoreo continuo

Gestión de desempeño

Cuadro de mando integral de ciberseguridad.

Optimización de recursos

Supervisión y Cumplimiento

Implementación del modelo de tres lineas

Mapeo de requisitos

Auditorías internas y externas

Reportes

Marco de Políticas y Procedimientos

Políticas, Estándares, Guías, Procedimientos – Politica y Estrategia Nacional de Ciberseguridad

Decisiones informadas al más alto nivel	Reducción de riesgos cibernéticos y operativos	Cumplimiento regulatorio	Mayor resiliencia, confianza y continuidad de negocio	Cultura de Seguridad en la organización

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

GRACIAS POR SU ATENCIÓN

www.seps.gob.ec