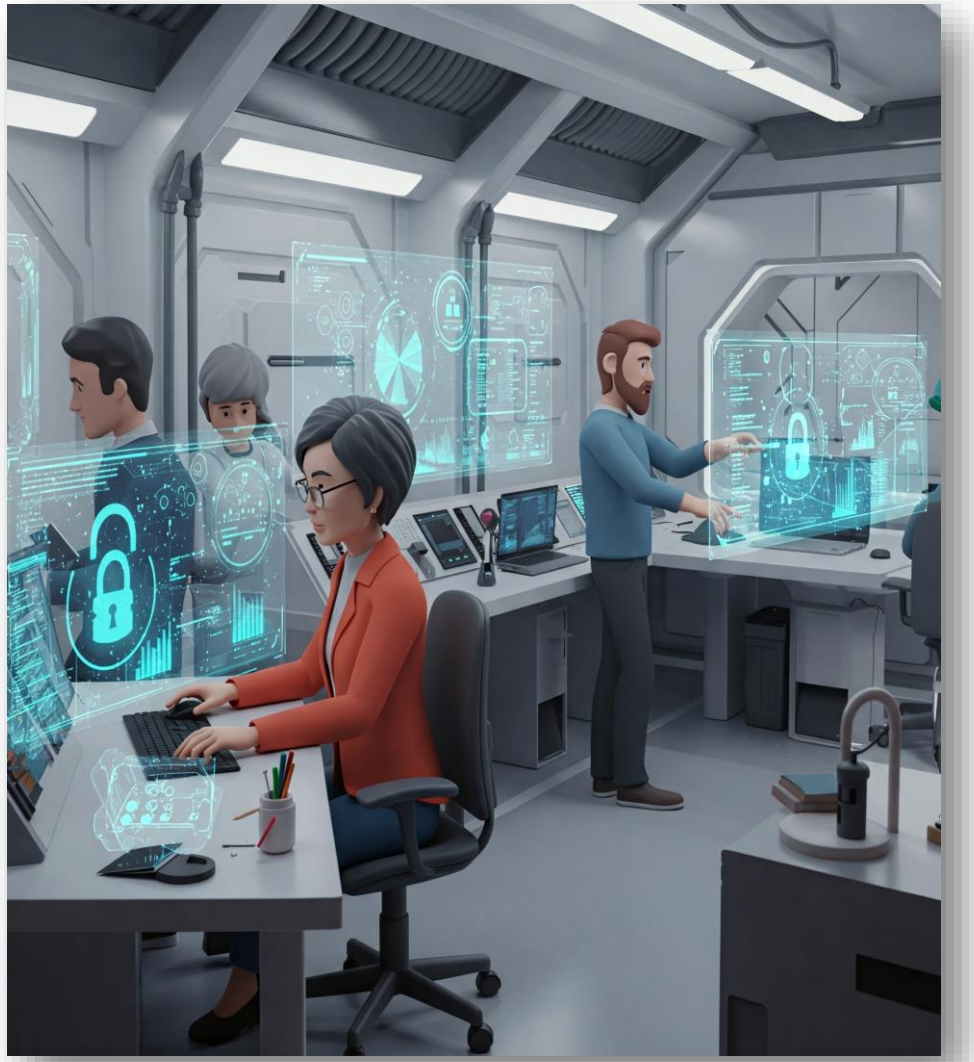
FORTALECIENDO LA SEGURIDAD Y EL CONTROL: AUDITORÍA DE TI Y CIBERSEGURIDAD PARA ENTIDADES DE LA SEPS

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

Importancia de la Auditoría de TI y la Ciberseguridad en el contexto actual



CONTENIDO SFPS

- 1. Marco Regulatorio y Riesgos
- 2. Auditoría de TI: Conceptos y elementos clave
- 3. Controles de ciberseguridad esenciales
- 4. Cultura de ciberseguridad y buenas prácticas
- 5. Preguntas y respuestas

1. Marco Regulatorio y Riesgos

Disposiciones de la Superintendencia de Economía Popular y Solidaria (SEPS), sobre gestión de riesgos tecnológicos y ciberseguridad

- La **SEPS, r**egula a entidades del sector financiero y no financiero que forman parte del sistema de economía popular y solidaria. Dada la transformación digital, ha emitido normativas específicas para proteger la infraestructura tecnológica y la información.

  La gestión de riesgos tecnológicos y la ciberseguridad se han vuelto esenciales para proteger tanto a las instituciones como a las personas que confían en ellas. No se trata solo de instalar antivirus o tener contraseñas seguras, sino de entender que detrás de cada sistema, cada archivo y cada transacción, tenemos información valiosa que puede ser vulnerable.

  Las amenazas digitales como los virus, el robo de datos o los fraudes en línea pueden afectar gravemente a una institución, especialmente si no está preparada. Por eso, es fundamental identificar los riesgos, prevenirlos y saber cómo responder si ocurre un incidente.

Principales normativas:

- RESOLUCIÓN Nro. SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 --- Seguridad de la información.
- RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-2023-0270 --- Seguridades en el Uso de canales electrónicos.
- RESOLUCIÓN Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-IGJ-0116 --- Administración de riesgo operativo.

Estas regulaciones obligan a las entidades a:

- Implementar políticas de ciberseguridad.
- Gestionar activos de información.
- Evaluar continuamente los riesgos tecnológicos.
- Establecer planes de respuesta ante incidentes.

Tipos de entidades bajo control de la SEPS y sus particularidades en cuanto a riesgos de TI

Entidades Financiera

- **Régimen general:** las cooperativas de ahorro y crédito de los segmentos 1 y 2; a las asociaciones mutualistas de ahorro y crédito para la vivienda y a la CONAFIPS
- **Régimen especial**: a las cooperativas de ahorro y crédito del segmento 3
- **Régimen simplificado:** las cooperativas de ahorro y crédito de los segmentos 4 y 5

Organizaciones no financieras:

- Asociaciones, fundaciones, comunas

Particularidades en cuanto a riesgos de TI:

- Limitado presupuesto para ciberseguridad.
- Falta de separación de funciones tecnológicas.
- Uso de software obsoleto o sin soporte.
- Escasa cultura de gestión de riesgo

La SEPS promueve la adopción escalonada de controles según cada organización

Principales riesgos de TI y ciberseguridad

- Malware (ransomware, virus)
- Phishing y ataques de ingeniería social.
- Ataques a la infraestructura (DDoS)
- Fugas de información y brechas de seguridad.
- Amenazas internas.
- Riesgos relacionados con terceros (proveedores de servicios en la nube).

La **ciberseguridad ya no es opcional**. El marco normativo de la SEPS obliga a todas las entidades supervisadas a tomar medidas activas para identificar, prevenir y responder a los riesgos tecnológicos.

Se debe implementar una **cultura de gestión de riesgos** basada en normativa, buenas prácticas y auditorías continuas.

2. Auditoría de TI

Es un proceso sistemático que evalúa los controles, sistemas y procesos tecnológicos de una organización para garantizar su seguridad, eficiencia y cumplimiento normativo. Analiza infraestructura, políticas y riesgos, identificando vulnerabilidades y proponiendo mejoras. Su objetivo es proteger datos, optimizar recursos y alinear la tecnología con los objetivos del negocio.

Objetivos Principales

- *Evaluar controles:* Verificar que los sistemas de TI tengan controles adecuados para mitigar riesgos.
- *Cumplimiento normativo:* Asegurar que la organización cumpla con regulaciones.
- *Identificar vulnerabilidades:* Detectar fallos de seguridad, ineficiencias o riesgos operativos.
- *Optimizar procesos:* Recomendar mejoras en la gestión de TI.
- *Garantizar continuidad:* Asegurar que los sistemas soporten la operación del negocio.

Diferencia entre Auditoría Interna y Externa de TI

Aspecto	Auditoría Interna	Auditoría Externa
Realizada por	Empleados de la organización o área interna.	Consultores o firmas independientes.
Enfoque	Preventivo, continuo y de mejora interna.	Validación independiente para terceros.
Objetivo principal	Mejorar procesos y cumplimiento interno.	Certificar el cumplimiento para stakeholders.
Frecuencia	Periódica (mensual/trimestral/anual).	Eventual (ej. para certificaciones o auditorías legales).

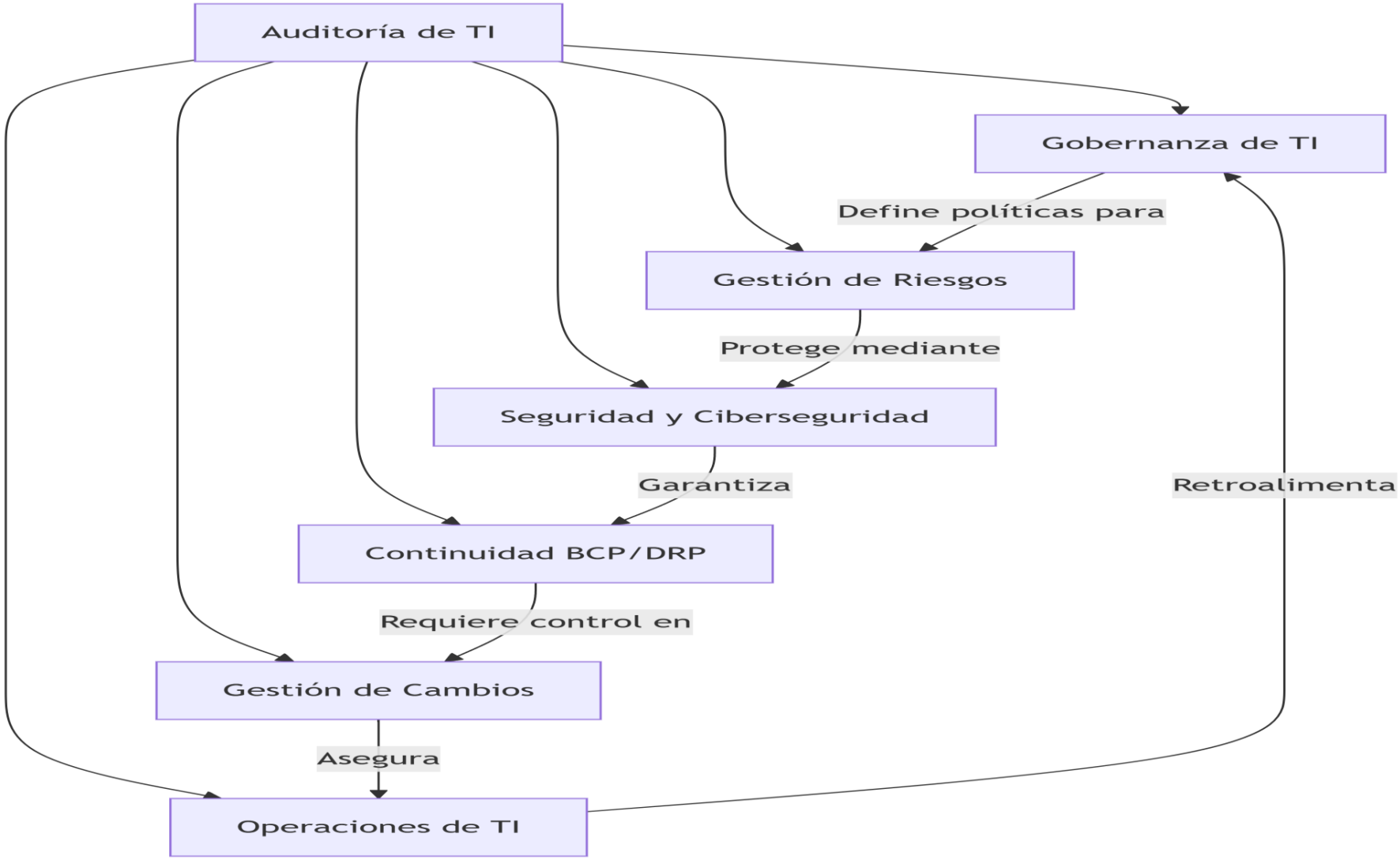
Fases de una Auditoria de TI

Fase	Actividades Clave	Entregables / Resultados	Stakeholders Involucrados
1. Planificación	Definir **alcance y objetivos**. Seleccionar **normativas de referencia** (ISO 27001, COBIT, NIST). Identificar **riesgos preliminares**. Elaborar **cronograma y asignar recursos**.	**Plan de Auditoría**: - Alcance documentado. - Matriz de riesgos inicial. - Cronograma firmado.	Alta dirección, Equipo de TI, Auditores.
2. Ejecución	Recolectar **evidencias** (entrevistas, documentos, pruebas técnicas). Aplicar **pruebas de controles** (ej: pentesting, revisión de logs). Documentar **hallazgos preliminares**.	**Registro de Evidencias**: - Grabaciones/actas de entrevistas. - Resultados de pruebas. - Lista de hallazgos sin clasificar.	Equipo de TI, Usuarios clave, Auditores.
3. Evaluación	Analizar evidencias vs. **estándares**. Clasificar hallazgos por **criticidad** (Crítico, Mayor, Menor). Validar hallazgos con el área auditada.	**Matriz de Hallazgos**: - Hallazgos categorizados. - Brechas de cumplimiento. - Impacto/Probabilidad evaluada.	Auditores, Responsables de TI.

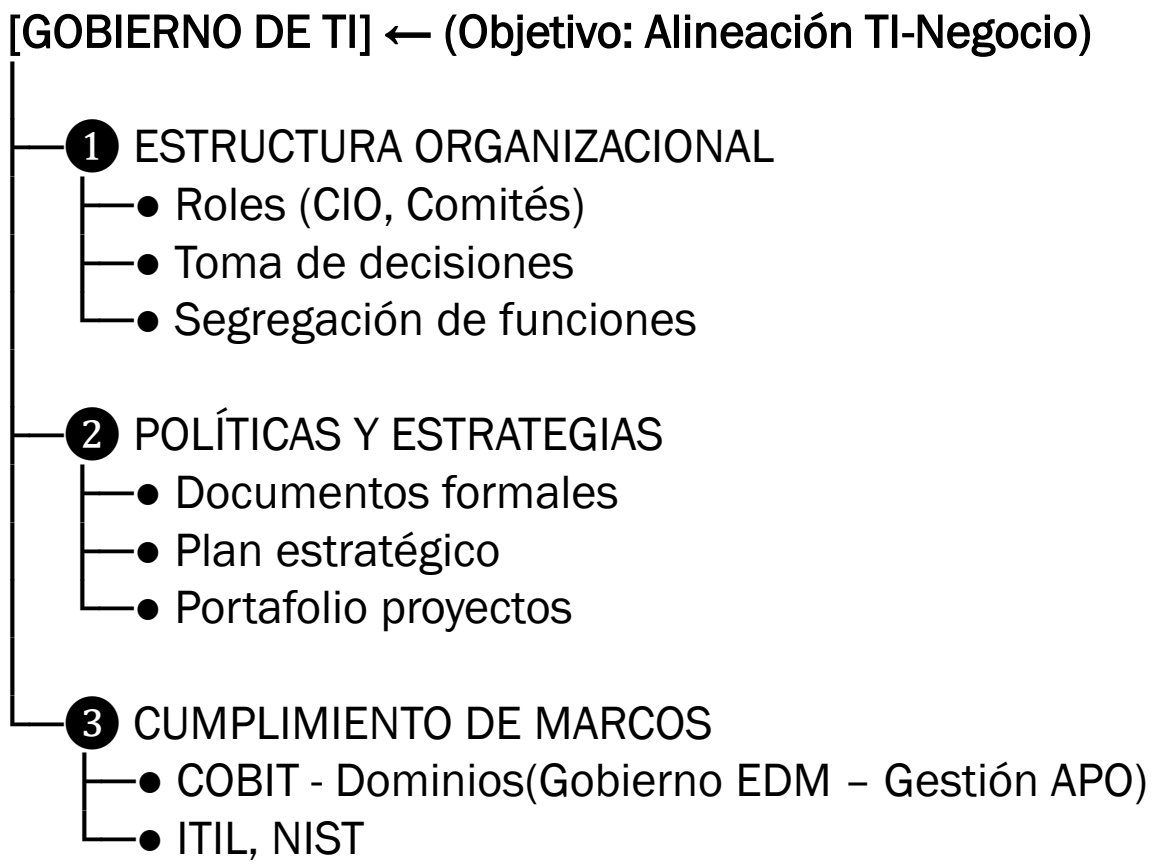
Fases de una Auditoria de TI

4. Informe	Redactar **informe ejecutivo y técnico**. Priorizar **recomendaciones** (corto/mediano/largo plazo). Presentar resultados a la **alta dirección**.	**Informe Final**: - Resumen ejecutivo. - Hallazgos con evidencias. - Plan de acción correctiva.	Alta dirección, Comité de Auditoría, TI.
5. Seguimiento	Monitorear **implementación de correcciones**. Realizar **auditorías de seguimiento** (si aplica). Cerrar **hallazgos solucionados**.	**Reporte de Cierre**: - Estado de acciones. - Evidencias de remediación. - Lecciones aprendidas.	Equipo de TI, Auditores, Cumplimiento.

Áreas clave de la Auditoría de TI



Áreas clave de la Auditoría de TI

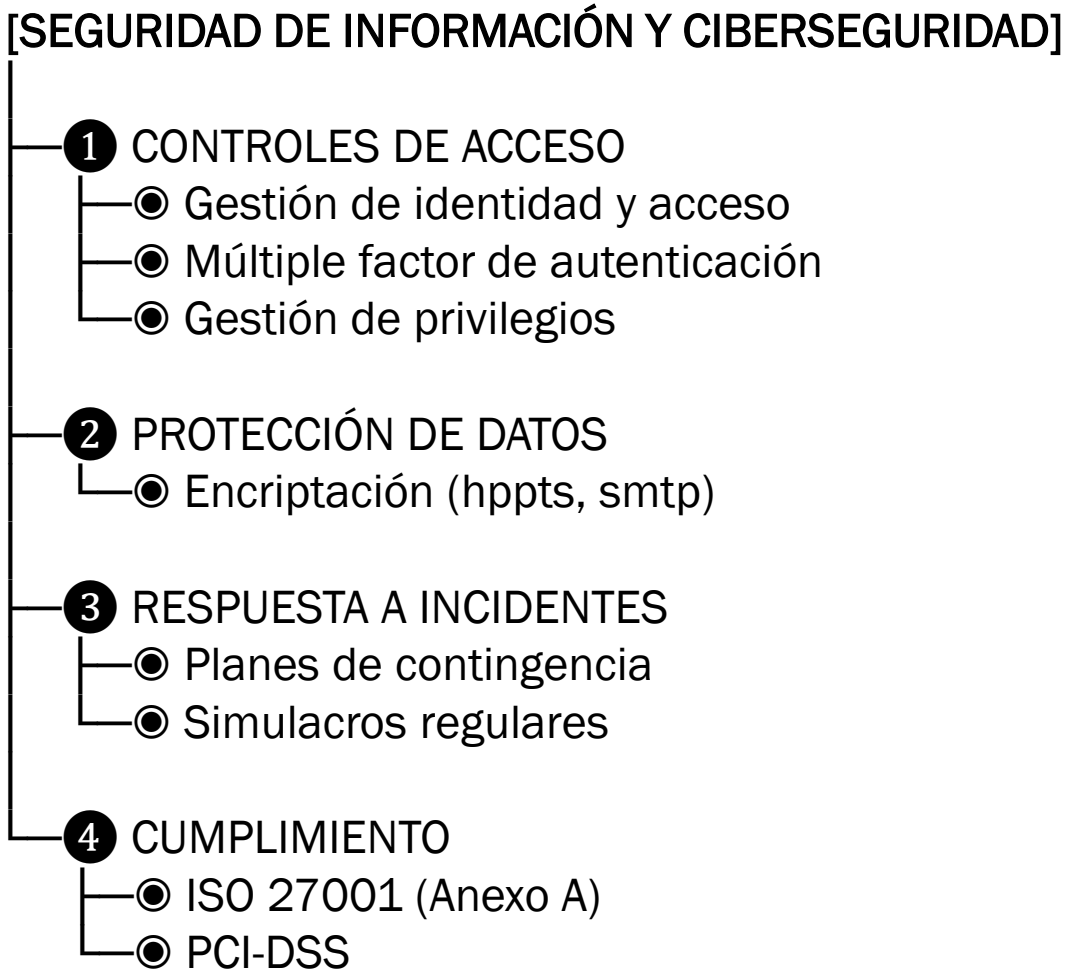


Áreas clave de la Auditoría de TI

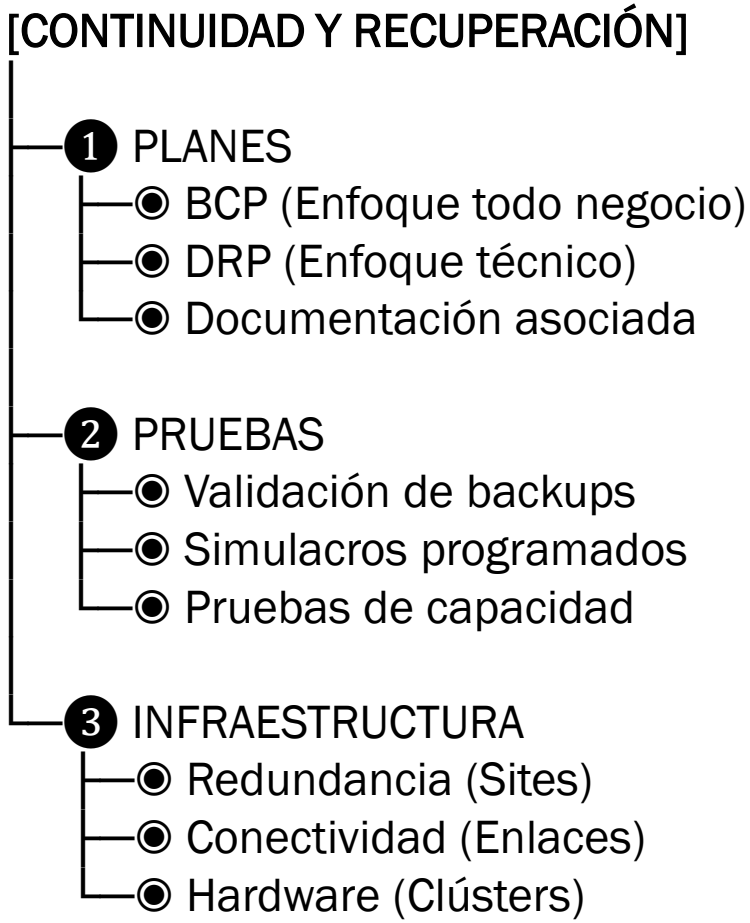
[GESTIÓN DE RIESGOS TI]

1. PROCESOS
   - Identificación (activos, amenazas)
   - Evaluación
   - Monitoreo (Número de intentos de acceso fallidos → >5 en 1 hora → Bloquear IP e investigar)
2. CONTROLES
   - Preventivos (firewalls, Gestión de Identidad y Accesos)
   - Correctivos (backups, Plan para recuperar sistemas críticos-DRP)
   - Detectivos (SIEM → OSSIM , pentesting)
3. ESTÁNDARES
   - ISO 31000 (enfoque proceso)
   - NIST CSF (5 funciones)
   - COBIT RISK (gobernanza)

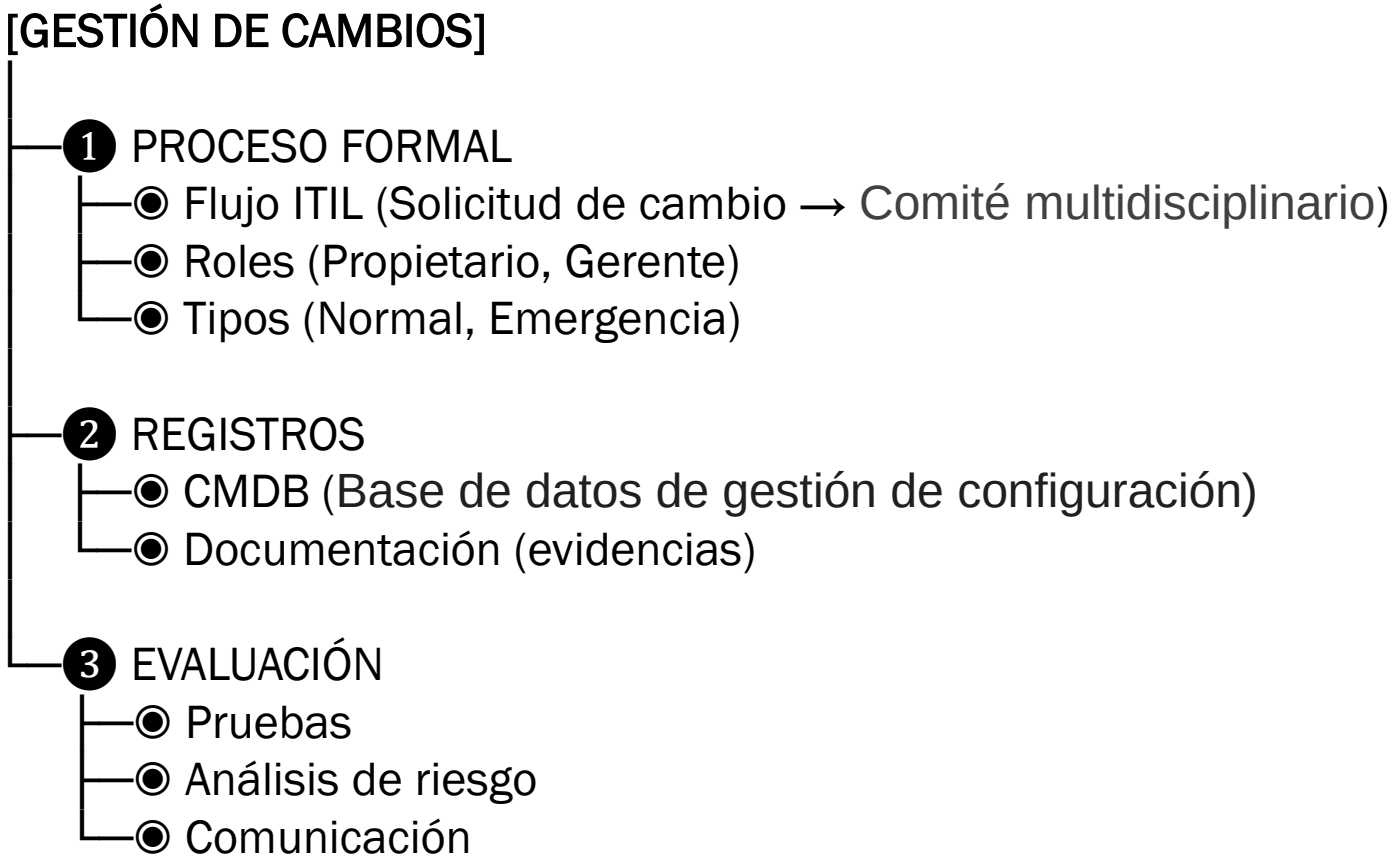
Áreas clave de la Auditoría de TI



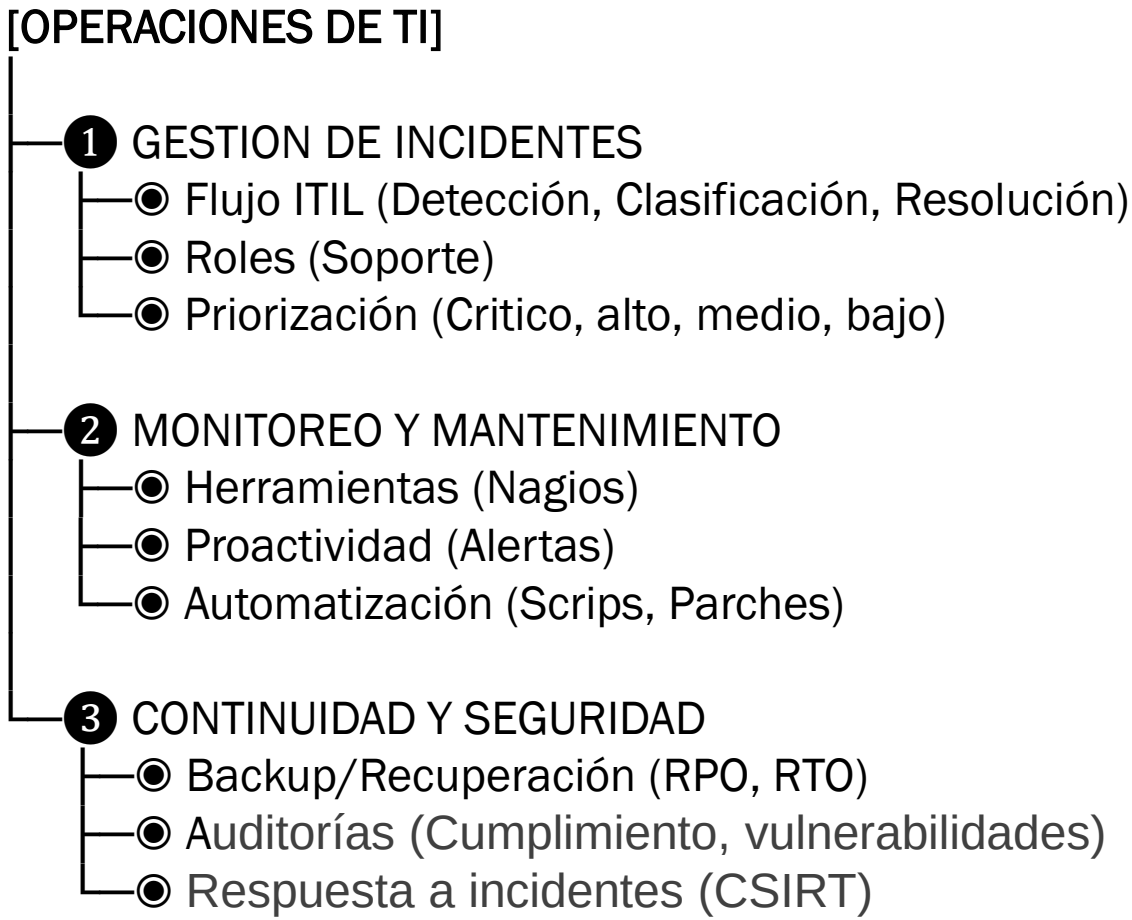
Áreas clave de la Auditoría de TI



Áreas clave de la Auditoría de TI



Áreas clave de la Auditoría de TI



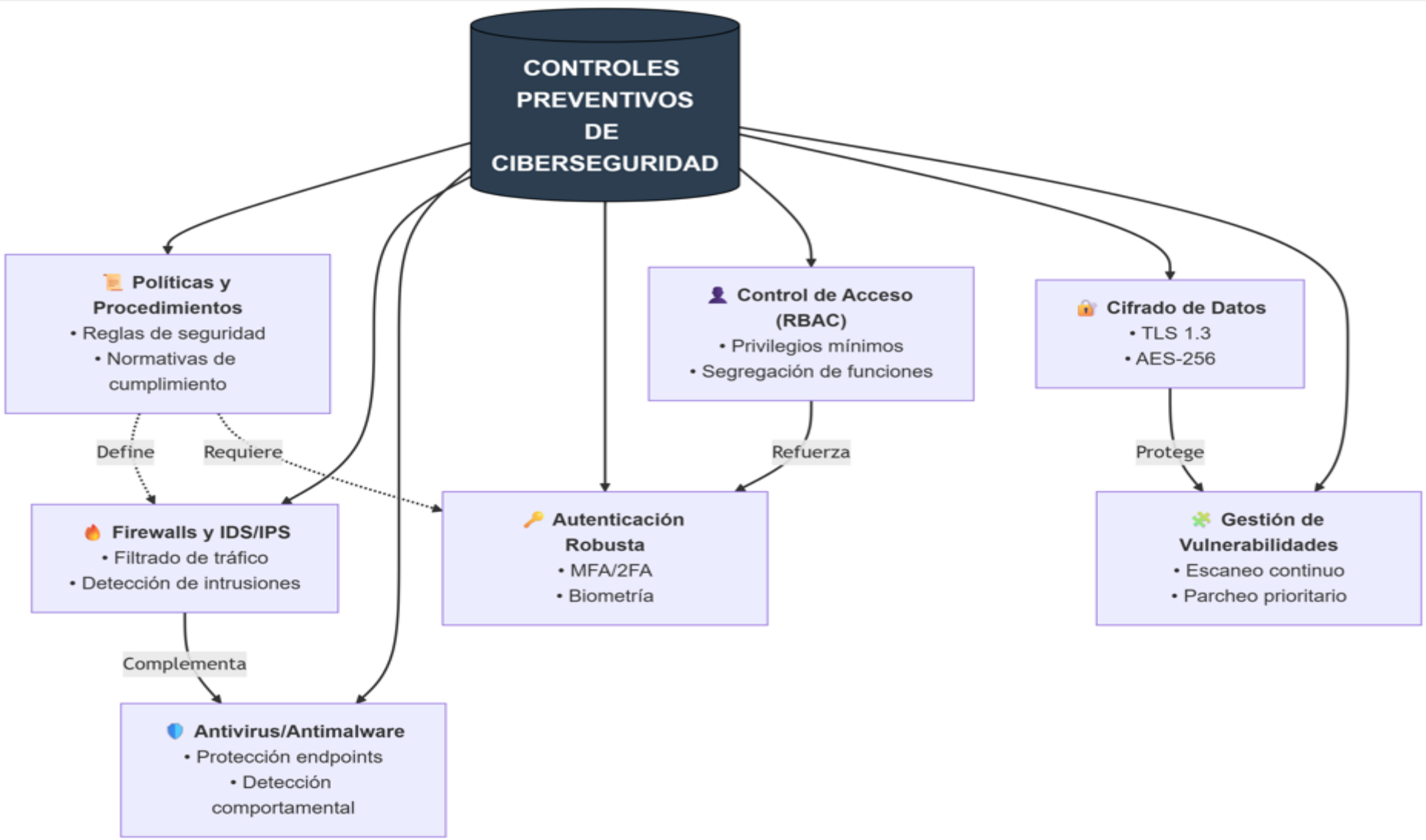
3. Controles esenciales de ciberseguridad

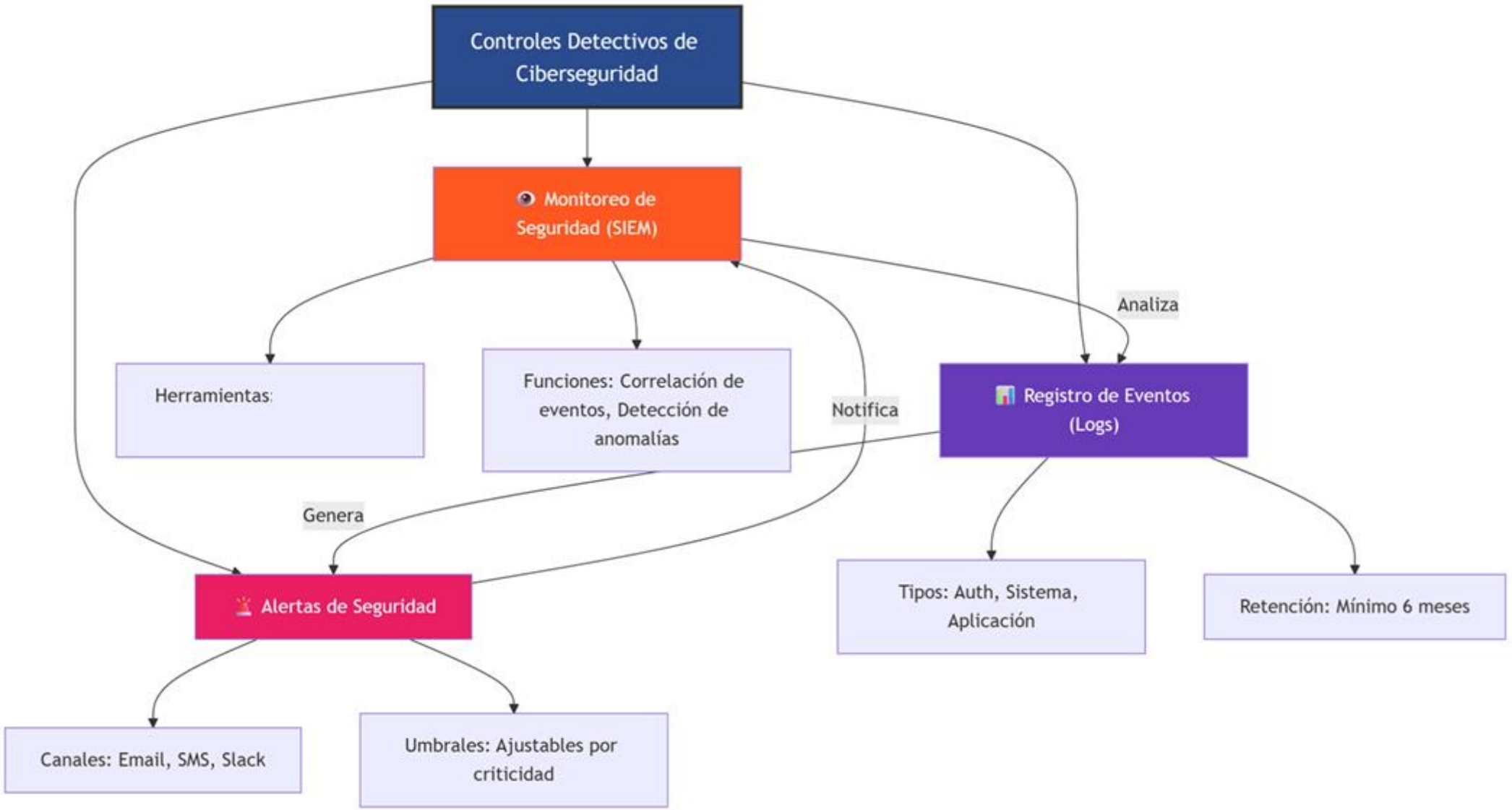
Son medidas básicas pero fundamentales que toda organización debe implementar para proteger su información y sistemas frente a amenazas digitales.

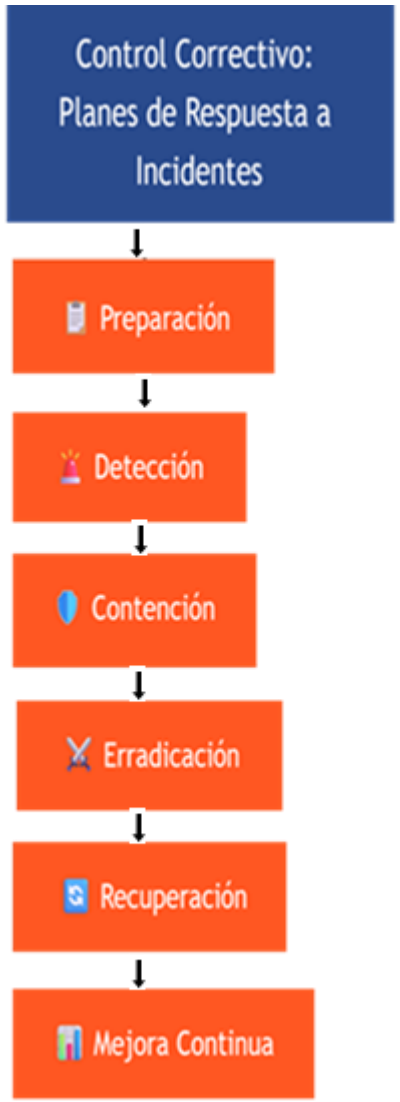
Se dividen en tres tipos:

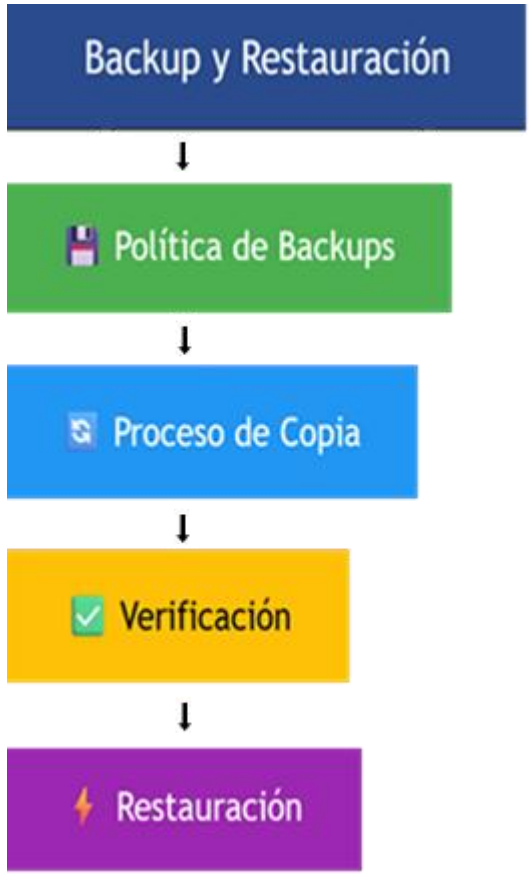
- *Preventivos*, buscan evitar ataques.
- *Detectivos,* identifican actividades sospechosas.
- *Correctivos,* ayudan a mitigar daños y recuperarse tras un incidente.

“Estos controles no son opcionales”


CONTROLES PREVENTIVOS DE CIBERSEGURIDAD
📜 Políticas y Procedimientos
• Reglas de seguridad
• Normativas de cumplimiento
👤 Control de Acceso (RBAC)
• Privilegios mínimos
• Segregación de funciones
🔐 Cifrado de Datos
• TLS 1.3
• AES-256
Define
Requiere
Refuerza
Protege
🔥 Firewalls y IDS/IPS
• Filtrado de tráfico
• Detección de intrusiones
🔑 Autenticación Robusta
• MFA/2FA
• Biometría
🧩 Gestión de Vulnerabilidades
• Escaneo continuo
• Parcheo prioritario
Complementa
🛡️ Antivirus/Antimalware
• Protección endpoints
• Detección comportamental


Controles Detectivos de Ciberseguridad
Monitoreo de Seguridad (SIEM)
Herramientas:
Funciones: Correlación de eventos, Detección de anomalías
Analiza
Notifica
Registro de Eventos (Logs)
Genera
Alertas de Seguridad
Tipos: Auth, Sistema, Aplicación
Retención: Mínimo 6 meses
Canales: Email, SMS, Slack
Umbrales: Ajustables por criticidad


Control Correctivo: Planes de Respuesta a Incidentes
Preparación
Detección
Contención
Erradicación
Recuperación
Mejora Continua


Backup y Restauración
Política de Backups
Proceso de Copia
Verificación
Restauración


BCP/DRP
Plan de Continuidad (BCP)
Proceso Integral
Plan de Recuperación (DRP)

4. Cultura de ciberseguridad y buenas práctica

Es el conjunto de valores, comportamientos y prácticas que una organización promueve para proteger sus activos digitales, con la finalidad de reducir riesgos y fomentar la responsabilidad compartida entre todos los colaboradores.

Buenas practicas para la prevención de incidentes

- Reconocimiento de correos electrónicos sospechosos (phishing).
- Uso de contraseñas seguras y su gestión.
- Navegación segura por internet.
- Protección de dispositivos móviles.
- Reporte de incidentes de seguridad.

5. Preguntas y respuestas

Contacto:

Gerardo Cajamarca Méndez
0995341444
gerardocim@softwaresystem-gc.com

SUPERINTENDENCIA
DE ECONOMÍA POPULAR Y SOLIDARIA

GRACIAS POR SU ATENCIÓN

www.seps.gob.ec