

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Propósito

Establecer el marco de gobierno, controles, protocolos operativos y evidencias para proteger la confidencialidad, integridad y disponibilidad de la información propia y de terceros, cumpliendo con las exigencias contractuales de aliados y mejores prácticas ISO/IEC 27001:2022.

Alcance

Aplica a todo el personal, contratistas, proveedores y sistemas bajo control de la empresa, tanto on premise como en nube (SaaS, PaaS, IaaS), redes corporativas y dispositivos utilizados para acceder a activos de información.

Referencias normativas

- ISO/IEC 27001:2022 y 27002:2022.
- Guías internas de Aplicaciones e Infraestructura (seguridad de TI).
- Requisitos del aliado ENEL (SGL 08 – SaaS; SGL 10 – Infra; SGL 11 – IaaS).
- Ley de Protección de Datos Personales aplicable (p. ej., Ley 1581/2012 en Colombia) y normativa local vigente.
- NIST 800 88 (Saneamiento de medios).
- PCI DSS v3 (si aplica a datos de pago).

PRESENCIA Colombo Suiza, en su compromiso con la seguridad de la información, establece las siguientes reglas generales para el uso de los activos de información:

1. Uso Exclusivo para Fines Laborales

Los activos de información, incluidos dispositivos, aplicaciones y datos, deben utilizarse exclusivamente para fines laborales relacionados con las actividades de la organización.

2. Protección de Información Confidencial

Se debe proteger la información confidencial y sensible de la organización, evitando su divulgación no autorizada. Esto incluye el uso de contraseñas fuertes y el cifrado de datos cuando sea necesario.

3. Acceso y Autenticación

El acceso a los activos de información debe estar limitado a los empleados autorizados. Se deben utilizar métodos de autenticación adecuados (como contraseñas, autenticación de dos factores) para garantizar la seguridad.

4. Uso Responsable de Recursos

Los empleados deben utilizar los activos de información de manera responsable y eficiente, evitando el uso excesivo de recursos como ancho de banda, almacenamiento y tiempo de procesamiento.

5. Prohibición de Instalación de Software No Autorizado

Está prohibido instalar o utilizar software no autorizado en los dispositivos de la organización. Solo se deben utilizar aplicaciones y herramientas aprobadas por el departamento de TI.

6. Mantenimiento de la Integridad de los Datos

Los empleados son responsables de mantener la integridad y precisión de los datos. Cualquier error o inconsistencia debe reportarse de inmediato a la persona correspondiente.

7. Cumplimiento de Políticas y Normativas

Todos los empleados deben cumplir con las políticas de seguridad de la información y las normativas legales aplicables. Esto incluye regulaciones como GDPR, HIPAA u otras específicas del sector.

8. Responsabilidad en el Uso de Dispositivos Móviles

Los dispositivos móviles utilizados para acceder a información corporativa deben estar protegidos con contraseñas y mecanismos de seguridad. Se deben evitar conexiones a redes públicas no seguras.

9. Devolución de Activos de Información

Al finalizar la relación laboral o cuando se cambien de puesto, los empleados deben devolver todos los activos de información (dispositivos, documentos, credenciales, etc.) en su estado original, asegurándose de eliminar toda la información personal o no relacionada.

10. Reporte de Incidentes de Seguridad

Cualquier incidente de seguridad, como pérdida, robo o uso indebido de activos de información, debe ser reportado de inmediato al departamento de TI o al responsable de seguridad de la información para su gestión y mitigación.

11. Gobierno, roles y responsabilidades

- Dirección: aprueba la política; provee recursos.
- Comité de Seguridad: supervisa riesgos, cumplimiento y planes.
- CISO/Líder de Seguridad: implementa y mantiene el SGSI; gestiona SoA y evidencias.
- Dueños de Activo: definen requisitos de acceso y clasificación.
- Custodios (TI/DevOps): operan controles técnicos (logs, parches, respaldos, hardening, redes).
- Usuarios: cumplen políticas/procedimientos y reportan incidentes.

12. Gestión de riesgos

- Metodología basada en probabilidad/impacto; inventario y valoración de activos.
- Registro de riesgos; tratamiento (evitar, mitigar, transferir, aceptar) y SLA para acciones.
-> Anexo Matriz de riesgos.
- Revisión al menos anual o ante cambios significativos.

13. Clasificación y manejo de la información

- Niveles: Pública / Interna / Confidencial / Restringida.
- Rotulación y manejo por nivel (almacenamiento, transmisión, compartición y destrucción).
- Datos estrictamente confidenciales: cifrado en reposo y tránsito, controles reforzados y trazabilidad.

14. Gestión de activos

- Inventario actualizado (HW/SW/servicios nube), propietario, criticidad, RTO/RPO, ubicación.
- Control de medios (ingreso/egreso, transporte seguro, custodia, saneamiento NIST 800 88).

15. Control de acceso e identidad

- RBAC y principio de mínimo privilegio. Altas/Bajas/Cambios via ticket y aprobación del dueño de activo.
- MFA obligatorio en sistemas críticos y desde redes no seguras.
- Integración con EG_AD/EG_IDM cuando aplique (IaaS/EG_VPC).
- Política de contraseñas y bloqueo tras intentos fallidos; límites de sesión para cuentas interactivas.
- Cuentas predeterminadas deshabilitadas; cuentas administrativas separadas; naming conventions.

16. Criptografía

- Cifrado en tránsito (TLS 1.2+), en reposo según criticidad;
- Gestión de llaves: generación, rotación, custodia, revocación y registro;
- Certificados X.509 para autenticación fuerte basada en certificados cuando aplique.

17. Registro y monitoreo (Logging & Auditing)

- UTC en toda infraestructura crítica; sincronización NTP.
- Fuentes mínimas: SO/BD/Aplicación/Proxy/WAF/Firewall/IDS/EDR/Autenticación.
- Retención conforme a guías de Infra y ley local; protección de integridad; disponibilidad on line/off line.
- Integración de eventos de seguridad con SIEM (EG_SIEM cuando aplique).
- Alertas en tiempo real y casos de uso (accesos privilegiados, DoS, escalamiento, exfiltración).

18. RespalDOS y retención

- Política de respaldos por tipo de dato/servicio; cifrado y protección en almacenamiento y transmisión.
- Pruebas de restauración periódicas; retención acorde a requisitos contractuales/legales.

19. Gestión de vulnerabilidades y parchado

- Escaneo periódico (al menos mensual críticos/expuestos) y ante cambios mayores.
- Patching a nivel aplicativo e infraestructura según SLA;
- Si no hay parche aplicable, controles compensatorios acordados y aprobados.
- Evaluación del parche (impacto/regresión) y parchado extraordinario para incidentes severos.

20. Desarrollo, CICD y Gestión de cambios

- SDLC seguro: revisiones de código, SAST/DAST, gestión de secretos;
- CAB o flujo de cambios con plan de remediación y ventanas;
- Revisión de configuración de seguridad post despliegue.

21. Seguridad de endpoints y hardening

- Baselines de hardening (SO/BD/App) y enforcement centralizado.
- EDR/antimalware actualizado.
- Configuración avanzada/mission critical en servicios críticos.

22. Seguridad de red

- Segregación por capas: DMZ FE, DMZ BE, LAN; PCN segregadas.
- ADs separados por (sub)red cuando aplique.
- Firewall perimetral con inspección con estado; IDS/IPS; WAF para publicación "Full" en Internet.
- Conexiones seguras IPsec/TLS VPN; tráfico mínimo necesario entre redes públicas/no confiables y red privada.
- Proxies para salida a Internet; segregación de accesos de administración; HA de red.
- Seguridad de enrutamiento y DNS; Wi Fi conforme a directrices; 802.1X en puertos.
- Sin conexiones directas entre redes de diferentes cloud providers.
- Enlaces WAN asegurados a nivel de aplicación; si no es posible, asegurar a nivel inferior.
- Comunicación proveedor aliado controlada y registrada mediante tecnología de desacoplamiento.

23. Disponibilidad, Continuidad y DRP

- Arquitecturas de alta disponibilidad y monitoreo.
- Estrategias de BC/DRP por servicio; RTO/RPO definidos; pruebas periódicas.

24. Respuesta a incidentes

- Flujo: detección → triage → contención → erradicación → recuperación → lecciones aprendidas.
- Clasificación de severidad; contacto 24/7; coordinación con Aliado cuando aplique.
- Preservación de evidencias forenses.

25. Proveedores y cumplimiento

- Debida diligencia de seguridad; cláusulas mínimas; evaluaciones periódicas.
- SoA ISO 27001 expuesto y certificación ISO 27001 vigente.
- Informes SOC (ISAE 3402/SSAE 16) cuando aplique.
- PCI DSS v3 Nivel 1 si se gestionan datos de pago.
- Anexo de Seguridad en contratos con requisitos y penalidades de seguridad (SLA).

26. Privacidad y datos personales

- Cumplimiento con la Ley de Protección de Datos Personales aplicable (p. ej., Ley 1581/2012).
- Derechos de titulares (ARCO/Habeas Data), bases legales, retención y supresión.

27. Concientización y formación

- Inducción y formación anual obligatoria (>95% cobertura); campañas temáticas.

28. Control de documentos

- Control de versiones, historial de cambios, actas de aprobación; repositorio oficial.

29. Definiciones (extracto)

Activo de información, Dueño de activo, Registro/Log, SoA (Statement of Applicability), MFA, RBAC, SIEM, PCN, DMZ-FE/DMZ-BE, EG_AD (Active Directory aliado), EG_IDM (Gestión de identidades aliado), EG_SIEM.

Estas reglas proporcionan un marco claro para el uso responsable y seguro de los activos de información dentro de la organización, protegiendo tanto a la empresa como a sus empleados.

Protocolos operativos (PO)

PO 01 Altas, bajas y cambios de acceso

- Solicitud vía ticket con justificación y aprobación del dueño del activo.
- Alta con RBAC y MFA; cuentas admin separadas.
- Baja inmediata al terminar la relación; revocación de llaves/tokens.
- Revisión trimestral de accesos y accesos privilegiados; evidencias almacenadas.

PO 02 Gestión de credenciales y autenticación

- Parámetros de contraseñas (longitud, complejidad, rotación según riesgo).
- Bloqueo por intentos fallidos; límites de sesión; MFA desde redes no seguras.
- Uso de X.509 para autenticación fuerte cuando aplique.

PO 03 Logging y monitoreo

- Sincronización UTC y NTP.
- Fuentes, formatos, retención; protección de integridad; SIEM y casos de uso.
- Alertas en tiempo real; reporte y seguimiento.

PO 04 Respallos y restauración

- Frecuencia y tipo (completo/diferencial/incremental); cifrado en tránsito/reposo.
- Pruebas de restore (trimestral/semestral); métricas de éxito; conservación según tabla de retención.

PO 05 Parches y vulnerabilidades

- Ciclos: críticos ≤ 72 h; altos ≤ 7 días; medios ≤ 30 días (ajustable por riesgo/operación).
- Controles compensatorios documentados si no hay parche.
- Parchado extraordinario por incidentes severos; evaluación de impacto.

PO 06 Hardening y configuración segura

- Baselines por sistema/rol; enforcement centralizado.
- Eliminación de servicios innecesarios; bloqueo de puertos; deshabilitar cuentas por defecto.

- Revisión periódica de configuración y desviaciones.

PO 07 Seguridad de red

- Diseño de DMZ FE/DMZ BE/LAN; segmentación adicional; PCN segregadas.
- Firewall, IDS/IPS, WAF; VPN TLS/IPsec; proxy para salida.
- 802.1X, seguridad Wi Fi; enrutamiento y DNS seguros; HA.
- Prohibición de conexiones directas entre cloud providers; monitoreo de enlace con tecnología de desacoplamiento.

PO 08 Saneamiento de medios

- Procedimiento conforme NIST 800 88: limpiar, purgar, destruir según criticidad.
- Registro de cadena de custodia y certificación de destrucción.

PO 09 Continuidad y DRP

- Análisis de impacto (BIA); RTO/RPO por servicio; pruebas planificadas;
- Escenarios de interrupción mayor en sedes; comunicación con interesados.

PO 10 Respuesta a incidentes

- Playbook por tipo (malware, DoS, fuga de datos, credenciales, 3rd party).
- Enlaces con Assurance Check extraordinario cuando aplique;
- Cierre con lecciones aprendidas y mejoras del control.

PO 11 Assurance Check (pre producción y anual)

- Alcance y criterios; evidencia de controles activos y efectivos.
- Integración con CVE (identificadores) para intercambio de vulnerabilidades.
- Apertura temporal de controles perimetrales a IPs de prueba cuando sea requerido por ENEL.

PO 12 Gestión de proveedores y SLA

- Due diligence, clasificación por riesgo, requisitos mínimos.
- Anexo de Seguridad con requisitos concretos y penalidades por incumplimiento.
- Renovación anual de certificaciones (ISO 27001, SOC, PCI DSS si aplica) y entrega a la contraparte.

Anexos

Anexo A. Declaración de Aplicabilidad (SoA)

Listado de controles aplicables/no aplicables, justificación y estado (implementado / en progreso / planificado).

Anexo B. Matriz de retención de logs y datos

Tabla por sistema: fuente, tipo, retención, ubicación, responsable, evidencia.

Anexo C. Tabla de respaldo y restauración

Frecuencias, ventanas, cifrado, pruebas y resultados.

Anexo D. Plantillas

- Acta de aprobación de política.
- Checklist de revisión de accesos (trimestral).
- Formato de Parcheo extraordinario.

- Registro de saneamiento de medios.
- Plan de pruebas DRP.
- Reporte de Incidente.

Anexo E. Mapa de cumplimiento en desarrollo de sistemas de información con ALIADOS (SGL 08/10/11)

- SGL 08 SaaS:
 - R1 (Identificación/Autenticación/Autorización): Secciones 9 y PO 01/02.
 - R2 (Logs forenses): Sec. 11 y Anexo B.
 - R3–R7 (Segregación/EG_PC): Sec. 16 y PO 07.
 - R8–R11 (WAN/decoupling/monitoring): Sec. 16 y PO 07.
 - R12 (Disponibilidad): Sec. 17 y PO 09.
 - R13 (Devolución de datos): Sec. 19/20; contrato y Anexo de Seguridad.
 - R14–R15 (Eliminación de medios/Política 33): Sec. 8 y PO 08.
 - R16–R17 (Cifrado y gestión): Sec. 10 y PO 02/08.
 - R18–R20 (Malware/Hardening): Sec. 15 y PO 06.
 - R21–R24 (Assurance Check/CVE/extraordinario): Sec. 18 y PO 11.
 - R25–R29 (Parches): Sec. 13 y PO 05.
 - R30 (Riesgo/incidentes): Sec. 6 y 18.
 - R31 (Seguridad de código): Sec. 14.
 - R32–R34 (Cumplimiento/Plan Seguridad/Certificación): Sec. 19.
 - R35–R36 (SLA/penalizaciones): PO 12 (Anexo de Seguridad).
- SGL 10 Infra: Hardening, autenticación fuerte/MFA, RBAC, cuentas admin separadas, UTC/Logs/SIEM, HA, respaldos/BC DRP, centralización de gestión, VA periódica, y checklist de red (DMZ FE/DMZ BE, IDS/IPS, WAF, proxys, IPsec/TLS VPN, 802.1X, DNS/route security). Referencias: Sec. 11, 15, 16, 17 y PO 03/05/06/07.
- SGL 11 IaaS: Cumplimiento PDPL/Política 33, SoA/ISO 27001, SOC, PCI DSS; integración EG_AD/EG_IDM/EG_SIEM; segmentación EG_VPC; sincronización UTC; saneamiento de medios NIST 800 88; Assurance Check pre prod/anual y extraordinario. Referencias: Sec. 9–11–16–18–19–20 y PO 03/07/08/11/12.

Anexo F. Inventarios de Activos y Configuraciones (CMDB)

Objetivo. Mantener un inventario íntegro y actualizado de activos y elementos de configuración (CI) para habilitar control de cambios, gestión de vulnerabilidades, respuesta a incidentes y continuidad.

Alcance. Hardware (servidores, endpoints, redes), software (sistemas, aplicaciones, librerías), servicios en nube (SaaS/PaaS/IaaS), datos (BD/almacenamientos), identidades (usuarios/roles/grupos), contratos/licencias y componentes de red (routers, switches, firewalls, WAF, balanceadores, VPN, IDS/IPS).

Campos mínimos por tipo.

- HW/Endpoint/Servidor: Etiqueta/ID, serie, modelo, dueño de activo y custodio, ubicación, IP/MAC, SO/versión, baseline de hardening, EDR/antimalware, cifrado, fecha alta/baja, criticidad (C I D), RTO/RPO, clasificación de la info, dependencias/servicios.
- SW/Aplicación: Nombre y versión, proveedor, licencia y vigencia, ambientes (dev/test/prod), dueño funcional, repositorio/origen, dependencias, controles (SAST/DAST), criticidad.
- Nube (IaaS/PaaS/SaaS): Cuenta/tenant/proyecto, región, VPC/VNET y subredes, SG/NSG/ACL, objetos (VM, contenedores, DBaaS, buckets), cifrado, roles/IAM, claves/secretos, integración EG_AD/EG_IDM cuando aplique.

- Datos/BD: Motor/versión, esquema, clasificación (Pública/Interna/Confidencial/Restringida), dueño, ubicación, cifrado en reposo/tránsito, retención/backup.
- Identidades: Usuario/rol/grupo, sistema origen (AD/IdP), privilegios, fecha alta/baja, último acceso, MFA, recertificación.
- Red/Seguridad: Dispositivo, versión/firmware, topología/ubicación, interfaces/VLAN/VRF, reglas/ACL/objetos, políticas (NAT, VPN), respaldo de configuración y fecha de última copia.
- Procesos. Altas/cambios/bajas con ticket; descubrimiento (agente/agentless) y reconciliación; auditorías trimestrales de exactitud; relación CI↔cambios/incidentes/problemas; exportos para evidencias.
- Evidencias y KPIs. Informe de cobertura (>95%), exactitud (>98%), antigüedad de registros (<30 días), trazabilidad CI↔cambio, conciliación con AD/EG_AD y cuentas en nube, reporte de hallazgos y remediaciones.

Anexo G. Protocolos de Infraestructura y Redes

Diseño y segmentación. Capas DMZ FE, DMZ BE, LAN, PCN segregadas, VLAN/VRF, micro segmentación cuando aplique. Sin conexiones directas entre redes de distintos cloud providers.

Perímetro y publicación. Firewalls con inspección con estado, IDS/IPS, WAF para publicación en Internet "Full"; protección contra DoS a nivel de aplicación cuando aplique; tecnología de desacoplamiento para enlace con Enel.

Gestión y plano de control. Acceso administrativo por bastion/jump y VLAN de gestión; RBAC/MFA y PAM para privilegios; registros de cambios; ventanas de mantenimiento y CAB. Respaldo de configuraciones cifrado y versionado; pruebas de restauración.

Transporte y acceso. IPsec/TLS VPN, 802.1X/NAC en acceso cableado/inalámbrico; Wi Fi seguro conforme a guías; DNS y enrutamiento seguros; NTP/UTC corporativo.

Monitoreo y logging. Syslog/SNMPv3/NetFlow/sFlow hacia SIEM; alertas de disponibilidad, cambios de config, eventos de seguridad y saturación.

HA y continuidad. Redundancia (HSRP/VRRP/MC LAG), failover de enlaces, pruebas periódicas, planes de contingencia.

Firmware/parcheo. Calendario por criticidad y exposición; evaluación de impacto; controles compensatorios si aplica.

Evidencias. Diagramas actualizados, running/startup configs, exportos de SIEM, bitácoras de cambios y respaldos.

Anexo H. Protocolos de Soporte (Mesa de Ayuda / ITSM)

Alcance. Gestión de Incidentes, Requerimientos, Cambios, Problemas y Conocimiento; integración con inventarios/CMDB.

Canales y registro. Portal, correo y teléfono únicos; plantillas por categoría/servicio; vínculo obligatorio a CI y ambiente (dev/test/prod).

Priorización (Urgencia × Impacto). P1 crítico (respuesta ≤15 min, resolución objetivo ≤4 h); P2 alto (≤30 min / ≤8 h); P3 medio (≤4 h / ≤2 días); P4 bajo (≤1 día / ≤5 días). Ajustable por servicio/SLA.

Escalamiento. Funcional (resolver) y jerárquico (decidir); Mayor Incidente: sala puente, comunicaciones a interesados, post mortem con acciones correctivas.

Cambios. Normal/Estandar/Emergencia; evaluación de riesgo y plan de reversa; aprobación CAB; verificación post cambio.

Conocimiento. Base de conocimiento con artículos validados; Known Error Database para problemas recurrentes.

Métricas. Cumplimiento de SLA/OLA, MTTA/MTTR, tickets reabiertos, satisfacción de usuario, FCR.

Evidencias. Reportes mensuales, tableros, registros de comunicaciones, actas de post mortem.

Historial de cambios

- v01: Emisión inicial.
- v02: Redacción integral, anexos y protocolos operativos; alineación con SGL 08/10/11; inclusión de SoA y Anexo de Seguridad.