colgas Cinsa CoTranscol	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES	Versión	1
		Fecha Elaboración	04-05-2026
		Código	INS-PLT-ZZZ-0000

Elaborado por: Profesional de seguridad de la información.	Revisado por: CISO	Aprobado por: Gerente General Comité de Seguridad de la Información

Registro de Modificaciones			
Nº Versión	Fecha	Motivo de la modificación	Páginas elaboradas o modificadas
1	04-05-2026	Creación del documento.	Todas

1. INTRODUCCIÓN

En el entorno empresarial actual, caracterizado por la creciente digitalización de los procesos y la interconexión entre organizaciones, la seguridad de la información constituye un elemento fundamental para la continuidad del negocio, la protección de los activos estratégicos y el cumplimiento de las obligaciones legales y regulatorias.

Las organizaciones interactúan de manera permanente con proveedores, contratistas y terceros que, para el desarrollo de sus actividades, pueden tener acceso a información corporativa, sistemas tecnológicos o infraestructura crítica. Esta interacción genera riesgos que deben ser gestionados mediante la adopción de lineamientos claros y controles adecuados de seguridad de la información.

En este contexto, COLGAS, CINSA y/o COTRANSCOL establecen la presente política de seguridad de la Información para proveedores, con el propósito de definir los lineamientos mínimos que deberán observar los terceros que accedan, procesen o administren activos de información de la compañía.

Esta política se encuentra alineada con buenas prácticas internacionales en materia de ciberseguridad, incluyendo los lineamientos del National Institute of Standards and Technology (NIST) y estándares de gestión de seguridad de la información, así como con la normativa colombiana vigente en materia de protección de datos personales, en especial la Ley 1581 de 2012 y sus decretos reglamentarios.

2. OBJETIVO GENERAL

Establecer los lineamientos, principios y requisitos mínimos de seguridad de la información que deben observar los proveedores y terceros que, en el desarrollo de sus actividades o en el marco de relaciones comerciales con COLGAS, CINSA y/o COTRANSCOL, tengan acceso a activos de información, infraestructura tecnológica o datos de la compañía.

La presente política busca contribuir a la protección de la confidencialidad, integridad y disponibilidad de la información, así como prevenir incidentes de seguridad que puedan afectar la continuidad operativa, el cumplimiento normativo y la reputación corporativa.

Objetivos específicos

1. Establecer lineamientos y controles mínimos de seguridad de la información que deberán observar los proveedores y terceros que, en el desarrollo de sus actividades, tengan acceso a información, sistemas tecnológicos o activos digitales de COLGAS, CINSA y/o COTRANSCOL, con el fin de prevenir accesos no autorizados, pérdida, alteración o divulgación indebida de la información.
2. Fortalecer la gestión de riesgos asociados al acceso y tratamiento de información por parte de proveedores y terceros, promoviendo la adopción de buenas prácticas de seguridad que contribuyan a la protección de la confidencialidad, integridad y disponibilidad de los activos de información de la compañía.

3. APLICACIÓN Y ALCANCE

Esta política se aplica a todos los proveedores que, por la naturaleza de su servicio, requieran procesar, almacenar y/o acceder a información confidencial, crítica o activos de información de COLGAS, CINSA y/o COTRANSCOL.

4. DEFINICIONES

MFA (Autenticación de Multifactor): método complementario a la contraseña de la cuenta de usuario utilizando mecanismos de aplicación, código sms, correo, entre otros que validen la identidad del usuario.

Antivirus / EDR: programa informático cuyo objetivo es la detección y respuesta de amenazas avanzadas sobre equipos de cómputo.

Activo de información: son los datos, aplicaciones, sistemas y tecnología de información de COLGAS, CINSA y/o COTRANSCOL a los que los proveedores pueda acceder o utilizar en base al contrato del servicio.

Malware: hace referencia a cualquier tipo de software malicioso que trata de infectar un dispositivo.

Tercero/Proveedor: persona natural o jurídica que haya sido contratada por COLGAS, CINSA y/o COTRANSCOL con el fin de suministrar bienes y/o prestar servicios a favor de COLGAS, CINSA y/o COTRANSCOL.

Colaborador: persona que labora para COLGAS, CINSA y/o COTRANSCOL.

5. FECHA DE ENTRADA EN VIGENCIA

La presente política entrará en vigencia a partir de la fecha de su aprobación y publicación oficial.

6. CONTENIDO

Los proveedores y terceros que tengan acceso a activos de información de COLGAS, CINSA y/o CONTRANSCOL deberán adoptar controles de seguridad adecuados que permitan proteger la confidencialidad, integridad y disponibilidad de la información, conforme a los lineamientos establecidos en la presente política.

Estos lineamientos buscan asegurar que las actividades realizadas por terceros se desarrollen bajo estándares adecuados de protección de la información y gestión del riesgo tecnológico.

1. Responsabilidades del Personal y Capacitación

a) Los dispositivos utilizados por el personal que tenga acceso a la información o sistemas de la compañía deberán contar con:
   - Aplicación oportuna de actualizaciones y parches de seguridad para sistemas operativos y software.
   - Instalación y funcionamiento de software antimalware actualizado con la última firma.
   - Activación de firewall personal estándar de la industria.
   - Cifrado de disco y almacenamiento para proteger datos en caso de pérdida o robo.

b) Asegurar que todo el personal involucrado, incluyendo contratistas y subcontratistas, reciba capacitación profesional y sensibilización en ciberseguridad al inicio de la vinculación y al menos una vez al año.

c) Definir y documentar roles y responsabilidades en el ciclo de desarrollo seguro (SDL), incluyendo responsables para análisis de riesgos, modelado de amenazas, pruebas de seguridad y remediación. Este documento deberá estar disponible para auditoría cuando COLGAS, CINSA y/o COTRANSCOL lo solicite.

2. Control de Acceso Lógico y Autenticación

a) Proteger la confidencialidad de todas las contraseñas o claves de acceso asignadas a los proveedores por COLGAS, CINSA y/o COTRANSCOL.
b) Implementar autenticación multifactor (MFA) para el acceso a consolas de administración, usuarios con privilegios elevados y accesos remotos.
c) Establecer una política de contraseñas que cumpla con:

Usuarios Administradores

- Cambio cada 60 días.
- Longitud mínima 20 caracteres.
- Complejidad (mayúsculas, minúsculas, números y símbolos).
- Bloqueo tras 3 intentos fallidos.
- Historial mínimo de 24 contraseñas únicas si el sistema lo permite.
- Tiempo mínimo de vigencia de contraseña: 1 día

Cuentas de Servicio

- Longitud mínima 24 caracteres.
- Complejidad (mayúsculas, minúsculas, números y símbolos).
- Bloqueo tras 3 intentos fallidos.
- Historial mínimo de 6 contraseñas únicas.
- Tiempo mínimo de vigencia de contraseña 1 día.

Usuarios sin privilegios elevados

- Cambio cada 90 días.
- Longitud mínima 10 caracteres.
- Complejidad (mayúsculas, minúsculas, números y símbolos).
- Bloqueo tras 3 intentos fallidos.
- Historial mínimo de 6 contraseñas únicas.
- Tiempo mínimo de vigencia de contraseña: 1 día.

d) Retirar privilegios de acceso inmediatamente cuando el personal deje de estar involucrado en el procesamiento de información de COLGAS, CINSA y/o COTRANSCOL.
e) Asegurar un sistema de registro de actividades (logs de auditoría) que cumpla con:

- Registrar todas las altas y bajas de usuarios (usuario, fecha, hora, actividad)

- Registrar el inicio de sesión (logging on) y cierre de sesión (logging off) de todos los usuarios (hora, fecha, usuario, IP, MAC, - nombre de host)
- Registrar todos los cambios o modificaciones realizados en los perfiles/roles de usuarios (usuario, fecha, hora, actividad)
- Registrar todas las actividades realizadas por los usuarios, incluyendo transacciones ejecutadas y accesos a archivos, detallando para cada evento: usuario, fecha, hora, tipo de actividad y tipo de acceso (lectura, escritura, modificación, eliminación).
- Retención mínima de 12 meses y protección contra alteración.

f) Disponer de un módulo de MFA integrado en el aplicativo.

3. Seguridad en Redes y Comunicaciones

a) Instalar y mantener sistemas de protección contra intrusiones (IDS/IPS) y firewalls en servidores y puertas de enlace, configurados para excluir protocolos innecesarios, conforme a CIS Benchmarks.
b) Mantener registro de la actividad de firewalls y gateways por un período mínimo de 12 meses, asegurando su protección contra alteración y disponibilidad para auditoría.
c) Proteger datos en tránsito mediante TLS 1.3 (preferido) o 1.2, autenticación mutua de certificados y algoritmos seguros (AES-256, SHA-256). Protocolos inseguros (SSL, TLS <1.2) deberán estar deshabilitados.
d) Instalar y mantener un firewall de aplicación (WAF) capaz de detectar y bloquear amenazas basadas en OWASP Top 10, con reglas actualizadas y pruebas periódicas de efectividad.

4. Protección contra Malware y Código Malicioso

a) Instalar, configurar, activar y mantener actualizado software antimalware (antivirus, antispyware, protección contra ransomware) en todos los servidores, dispositivos, portátiles y estaciones de trabajo que procesen o almacenen datos de COLGAS, CINSA y/o COTRANSCOL.
b) Configurar el software para ejecución automática al arranque y protección continua, incluyendo bloqueo de ejecución de código no autorizado (whitelisting).
c) Generar reportes periódicos (mensuales) sobre estado de protección y detecciones, asegurando que los logs estén protegidos contra alteración y disponibles para auditoría.
d) Reportar incidentes de malware específicos de COLGAS, CINSA y/o COTRANSCOL que puedan afectar críticamente sus sistemas en un plazo máximo de 24 horas desde su confirmación.
e) Realizar pruebas periódicas de efectividad y mantener integración con sistemas de monitoreo (SIEM) cuando aplique.

5. Seguridad en servidores y plataformas

a) Asegurar la integridad, confidencialidad y disponibilidad de los servidores mediante controles físicos y lógicos.
b) Proteger el acceso a los servidores con autenticación segura y contraseñas robustas.
c) Cambiar contraseñas predeterminadas antes de la puesta en producción y renovarlas cada 90 días.
d) Ubicar los servidores en zonas físicamente seguras con control de acceso restringido.

e) Aplicar estándares de configuración segura (CIS Benchmarks, NIST) y realizar hardening completo.
f) Implementar herramientas de análisis de seguridad y monitoreo continuo para detectar cambios no autorizados.
g) Aplicar parches críticos en un plazo máximo de 4 días desde su publicación.
h) Implementar control de cambios formal y revisión periódica de configuraciones.
i) Registrar toda la actividad de acceso al servidor y conservar los logs por mínimo 12 meses, asegurando su protección contra alteración.
j) Realizar revisiones de seguridad trimestrales y auditorías completas al menos una vez al año para asegurar vigencia de los controles.
k) Los servidores deben usar cifrado en disco y comunicaciones internas.

6. Protección de datos y bases de datos

a) Mantener cifrada la información clasificada como confidencial en tránsito y reposo, utilizando algoritmos seguros (AES-256, RSA-2048) y protocolos TLS 1.3.
b) Restringir el acceso físico y lógico a las bases de datos y archivos bajo el principio de “necesidad de conocer”.
c) Implementar borrado seguro conforme a NIST SP 800-88 y revisar controles periódicamente.
d) Proteger accesos con autenticación robusta y contraseñas renovadas cada 90 días.
e) Mantener registros de acceso y transacciones por mínimo 12 meses o lo que indique la regulación colombiana, asegurando su protección contra alteración.
f) Contar con copias de respaldo bajo medidas equivalentes de seguridad y realizar pruebas de restauración trimestrales.
g) Implementar herramientas de análisis para revisar configuraciones y asegurar el cumplimiento de la línea base.
h) Realizar revisiones de seguridad trimestrales y auditorías completas anuales.
i) Asegurar que las jurisdicciones donde se procesan datos cumplan normas equivalentes o superiores a las aplicables en Colombia, entregando evidencia legal.
j) Asegurar independencia lógica o física de la información de COLGAS, CINSA y/o COTRANSCOL respecto a otras entidades en entornos cloud.

7. Prácticas de Desarrollo Seguro

a) Incorporar análisis estático (SAST), dinámico (DAST) y de composición de software (SCA) en el ciclo de desarrollo para identificar vulnerabilidades en código y dependencias.
b) Mitigar todas las vulnerabilidades críticas, altas y medias antes de pasar a producción.
c) Aplicar prácticas de desarrollo seguro conforme a estándares reconocidos (NIST SSDF, OWASP SAMM, ISO 27034), incluyendo análisis de riesgos y modelado de amenazas (ej. STRIDE, PASTA) en la fase de diseño. Documentar estas actividades y poner evidencias a disposición de COLGAS, CINSA y/o COTRANSCOL cuando sean requeridas.
d) Asegurar el uso de repositorios seguros con control de acceso (ej. Git con MFA), aplicar firmas digitales o verificación de integridad en el código antes del despliegue, e implementar controles para prevenir código malicioso (revisión de commits, análisis de integridad).
e) Entregar evidencias periódicas del cumplimiento del SDL (reportes por release) y realizar auditorías internas o externas al menos una vez al año sobre prácticas de desarrollo seguro.

f) Proporcionar un SBOM actualizado en cada release, incluyendo todas las dependencias y librerías utilizadas en la solución.

8. Gestión de Vulnerabilidades y Parches

a) Desarrollar e implementar un proceso documentado para la gestión de vulnerabilidades, incluyendo monitoreo continuo de fuentes confiables (NVD, CERT, OWASP, fabricantes).
b) Identificar vulnerabilidades específicas que puedan impactar los ambientes operativos o plataformas utilizados en nombre de COLGAS, CINSA y/o COTRANSCOL.
c) Evaluar la criticidad de las vulnerabilidades utilizando CVSS y contexto del negocio para priorización.
d) Remediar vulnerabilidades conforme a los siguientes SLA:
   - Críticas (CVSS ≥ 9.0): Corrección y despliegue en ≤ 4 días calendario.
   - Altas (CVSS 7.0–8.9): Corrección y despliegue en ≤ 15 días calendario.
   - Medias (CVSS 4.0–6.9): Corrección y despliegue en ≤ 30 días calendario.
- En ningún caso una vulnerabilidad podrá permanecer sin tratamiento por un período superior a noventa (90) días calendario.

Informar a COLGAS, CINSA y/o COTRANSCOL sobre vulnerabilidades críticas en un plazo máximo de 24 horas desde su detección.

e) Proporcionar evidencia del cierre (reportes, pruebas) y generar reportes periódicos sobre cumplimiento de SLA.
f) Incluir gestión de vulnerabilidades en librerías y dependencias del software.

9. Gestión y Respuesta a Incidentes

a) Notificar a COLGAS, CINSA y/o COTRANSCOL sobre incidentes de seguridad que afecten datos o sistemas críticos en un plazo máximo de 24 horas desde su detección (otros incidentes en ≤48 horas), enviando detalles al correo csirt@colgas.com.
b) Contar con un plan formal de respuesta a incidentes que incluya roles, responsabilidades, procedimientos y canales de comunicación, probado al menos una vez al año (preferiblemente semestral para sistemas críticos).
c) Investigar las causas del incidente y proporcionar a COLGAS, CINSA y/o COTRANSCOL un informe detallado con análisis de causa raíz y acciones correctivas.
d) Mantener un canal de atención 24/7 para incidentes críticos de seguridad.

10. Gestión de Cambios y Configuración

a) Desarrollar, probar y documentar cada cambio conforme a un proceso formal de gestión de cambios alineado con buenas prácticas (ITIL, ISO 20000), preservando la integridad lógica de datos, programas y rastros de auditoría.
b) Obtener aprobación formal antes de aplicar cualquier cambio en sistemas críticos.
c) Mantener una línea base de configuración y monitorear continuamente para detectar cambios no autorizados.
d) Registrar todos los cambios realizados, incluyendo quién, cuándo y qué se modificó, asegurando que los registros estén protegidos contra alteración y disponibles para auditoría.

e) Realizar revisiones periódicas (al menos trimestrales) para garantizar la vigencia de la configuración aprobada.

11. Respaldo y recuperación ante desastres

a) Implementar medidas de respaldo adecuadas, incluyendo almacenamiento seguro fuera del sitio de procesamiento, con cifrado y controles equivalentes a los datos principales.
b) Asegurar la reanudación de aplicaciones críticas y actividades de negocio en forma oportuna tras una emergencia o desastre.
c) Contar con un plan de recuperación ante desastres (DRP) documentado para cada sistema crítico y probarlo al menos una vez al año, complementado con pruebas parciales trimestrales.
d) Realizar pruebas de restauración de respaldos trimestralmente para asegurar su efectividad.
e) Asegurar disponibilidad anual de los servicios de 99.96% o superior, con RTO ≤ 24 horas y RPO ≤ 12 horas.
f) Entregar reportes de pruebas DRP y restauración cuando COLGAS, CINSA y/o COTRANSCOL lo solicite.

12. Propiedad y eliminación segura de datos

a) Reconocer que toda la información procesada es propiedad exclusiva de COLGAS, CINSA y/o COTRANSCOL y utilizarla únicamente conforme a lo establecido en el contrato.
b) Garantizar el borrado seguro de datos al finalizar el contrato, cuando lo solicite COLGAS, CINSA y/o COTRANSCOL, y/o cuando se eliminen o reemplacen medios de almacenamiento, utilizando métodos que cumplan con NIST SP 800-88 o estándares equivalentes.
c) Entregar a COLGAS, CINSA y/o COTRANSCOL un certificado de borrado seguro que incluya el método utilizado, fecha y alcance del proceso.
d) Asegurar que el borrado seguro se realice conforme a la legislación aplicable en materia de protección de datos personales (Ley 1581 de 2012 y normas equivalentes en otras jurisdicciones).

13. Auditoría y cumplimiento de controles

a) Permitir a COLGAS, CINSA y/o COTRANSCOL realizar auditorías de seguridad, previa notificación, sobre procesos, configuraciones, evidencias y registros relacionados con el cumplimiento de este anexo.
b) Facilitar acceso a logs, reportes y personal clave durante la auditoría.
c) Corregir hallazgos en los siguientes plazos:

- Críticos: ≤15 días.
- Altos: ≤30 días.
- Medios: ≤60 días.

d) COLGAS, CINSA y/o COTRANSCOL podrá realizar auditorías periódicas o extraordinarias, incluyendo aquellas derivadas de incidentes de seguridad.

14. Uso de Inteligencia Artificial

a) Los proveedores deberán declarar el uso de sistemas de Inteligencia Artificial y limitar su utilización exclusivamente a los fines autorizados contractualmente por la compañía.
b) Se prohíbe el uso de información de la compañía para entrenamiento, ajuste o mejora de sistemas de IA sin autorización expresa. Dicha información no deberá salir, quedar expuesta ni ser accesible en Internet o entornos públicos.
c) Los sistemas de IA no deberán procesar información personal, sensible o confidencial de la compañía sin controles de seguridad reforzados y sin cumplimiento de la normativa aplicable.
d) Los proveedores deberán asegurar la segregación y protección de los entornos de desarrollo, entrenamiento y operación de los sistemas de IA, evitando accesos no autorizados y fugas de información.
e) El proveedor deberá poder explicar, a nivel funcional, el funcionamiento de los sistemas de IA y su impacto en los servicios prestados a la compañía.

7. RESPONSABILIDADES Y ROLES

Los proveedores y terceros que interactúen con activos de información de la compañía deberán:

- Adoptar controles de seguridad acordes con los lineamientos establecidos en la presente política.
- Implementar medidas razonables para prevenir incidentes de seguridad de la información.
- Reportar oportunamente cualquier evento o incidente que pueda afectar la seguridad de la información de la compañía.
- Promover buenas prácticas de seguridad de la información entre el personal que participe en la prestación del servicio.

Con el fin de garantizar una adecuada gestión de la seguridad de la información en la interacción con terceros, COLGAS, CINSA y/o COTRANSCOL establecen los siguientes roles y responsabilidades para la implementación, seguimiento y cumplimiento de los lineamientos definidos en la presente política.

1. Gerencia general

La gerencia general es responsable de promover una cultura organizacional orientada a la protección de la información y de respaldar la implementación de controles adecuados de seguridad en las relaciones con proveedores y terceros.
En particular le corresponde:

- Aprobar la presente política y sus actualizaciones.
- Garantizar la asignación de recursos humanos, tecnológicos y financieros necesarios para la gestión de la seguridad de la información.
- Promover el cumplimiento de la normativa aplicable en materia de protección de datos personales y seguridad de la información.
- Impulsa la adopción de buenas prácticas internacionales en materia de ciberseguridad y gestión del riesgo tecnológico
- Supervisar que las relaciones con proveedores contemplen controles adecuados para la protección de la información corporativa.

2. Seguridad de la Información

El área responsable de seguridad de la información tendrá a su cargo la coordinación de los lineamientos y controles relacionados con la protección de los activos de información en la interacción con proveedores.
Sus responsabilidades incluyen:

- Diseñar, actualizar y divulgar la presente política.
- Definir los estándares técnicos y controles de seguridad aplicables a proveedores y terceros.
- Evaluar los riesgos asociados al acceso de terceros a sistemas o información de la compañía.
- Establecer lineamientos para la gestión de incidentes de seguridad relacionados con proveedores.
- Supervisar el cumplimiento de los controles de seguridad establecidos en esta política.
- Coordinar auditorias, revisiones o evaluaciones de seguridad de la información.

3. Proveedores, contratistas y terceros

Los proveedores y terceros que tengan acceso a activos de información de la compañía deberán adoptar medidas razonables de seguridad para proteger la información a la que tengan acceso durante la prestación de sus servicios.

En este sentido, deberán:

- Implementar controles técnicos y organizacionales que permitan proteger la confidencialidad, integridad y disponibilidad de la información.
- Utilizar la información de la compañía exclusivamente para los fines autorizados en el marco de la relación comercial.
- Proteger las credenciales de acceso a sistemas y evitar su divulgación a terceros no autorizados.
- Reportar oportunamente cualquier incidente de seguridad que pueda afectar los sistemas o la información de la compañía.
- Garantizar que el personal que participe en la presentación del servicio conozca y observe buenas prácticas de seguridad de la información.
- Adoptar medidas para prevenir accesos no autorizados, pérdida, alteración o divulgación indebida de la información.

4. Colaboradores de la compañía

Los colaboradores de COLGAS, CINSA y/o CONTRASCOL que interactúen con proveedores o gestionen información corporativa deberán contribuir activamente a la protección de los activos de información.
En particular deberán:

- Cumplir los lineamientos establecidos en la presente política.
- Utilizar de manera responsable los sistemas y recursos tecnológicos de la compañía.
- Evitar compartir información corporativa con terceros no autorizados.
- Reportar cualquier evento o situación que pueda representar un riesgo para la seguridad de la información.
- Participar en las actividades de capacitación y sensibilización en materia de seguridad de la información.

8. SANCIONES

El incumplimiento de los lineamientos establecidos en la presente política podrá dar lugar a la aplicación de las medidas administrativas, contractuales o legales que resulten aplicables, de conformidad con la normativa vigente y con las disposiciones establecidas en la relación contractual con cada proveedor o tercero.

9. APROBACIÓN Y MODIFICACIONES

La presente política ha sido aprobada por el Comité de Seguridad de la Información y cuenta con el visto bueno de la Gerencia General, en atención a su carácter corporativo y transversal. Este documento será revisado periódicamente, al menos una vez al año, o cuando se presenten cambios normativos tecnológicos o estratégicos que requieran su actualización, con el fin de asegurar su vigencia y eficacia.