Directriz de Seguridad de la Información para la Gestión de Terceros

Ciberseguridad y Confianza Digital
Conexxión SURA, Suramericana S.A. Filiales y Subsidiarias
Vigencia: 2026

CONTENIDO

INTRODUCCIÓN

Esta directriz define los lineamientos de seguridad de la información para la gestión de proveedores y terceros involucrados en la cadena de suministro de Conexxión SURA, Suramericana S.A. Filiales y Subsidiarias. Hace parte integral de la Política general de Seguridad de la Información y Ciberseguridad como una especificación de sus lineamientos.

Contempla prácticas exitosas incorporadas a partir de estándares internacionales de seguridad[1] *que la organización ha seleccionado para su cumplimiento o referencia, así como lineamientos externos definidos por los diferentes entes de control que regulan nuestras actividades.*

1. OBJETIVOS

Definir lineamientos para salvaguardar la información gestionada por y para proveedores y terceros desde Conexxión SURA, Suramericana S.A. Filiales y Subsidiarias, que accedan a información y/o gestionen tanto las Tecnologías de la Información (TI), como las tecnologías de la Operación (TO).

Definir los lineamientos mínimos aplicables a la gestión de riesgos de Ciberseguridad en terceros de la cadena de suministro y/o abastecimiento.

2. ALCANCE

Los lineamientos definidos en esta directriz complementan las definiciones de Abastecimiento de Conexxión SURA, Suramericana S.A. Filiales y Subsidiarias en lo relacionado a la seguridad de la información. Los aspectos aquí definidos aplican para las áreas de seguridad de la información, los negociadores, proveedores y terceros con acceso a información en las tecnologías de la información (TI) y tecnologías de la operación (TO) de Sura.

En este documento cuando se hace referencia a las Compañías se habla de Conexxión SURA, Suramericana S.A., Filiales, subsidiarias.

[1] Estándares internacionales de Seguridad: Conjunto de Marcos de Referencia como COBIT5, ISO27001, ISO27002, ISO 27032, NIST.

3. GLOSARIO

- ✓ *En este documento se considera **proveedor**, aquella persona natural o jurídica que provee o suministra un determinado bien o servicio a las Compañías, y a cambio recibe una contraprestación económica. Se considera **tercero**, todo colaborador o empleado vinculado al proveedor.*
- ✓ ***Cadena de suministro/Abastecimiento:** La cadena de abastecimiento en ciberseguridad se refiere a todos los pasos necesarios para llevar un producto o servicio desde su origen hasta el consumidor final. Es crucial para la infraestructura de las organizaciones, ya que cualquier vulnerabilidad en uno de los eslabones puede comprometer a toda la infraestructura. La gestión efectiva de la cadena de abastecimiento implica evaluar los riesgos asociados a los proveedores, la tecnología utilizada y la información transferida, y es esencial para prevenir ataques cibernéticos y proteger la reputación y la economía de las organizaciones.*
- ✓ ***Tercero/proveedor crítico para la seguridad de la información:** es aquel que cumple como mínimo con una de las siguientes características.*
  - ✓ *Tiene acceso a crear, consultar y modificar información que se cataloga como: **confidencial o datos sensibles**, entre ellos y sin limitarse a: información de pólizas y datos personales privados, manejo de información que se considera "know How", datos sensibles de clientes, empleados, aliados de negocio o proveedores de Sura.*
  - ✓ *Todo aquel catalogado como proveedor relevante para SOX.*
  - ✓ *Tienen altos privilegios sobre aplicaciones o plataformas de tecnología de las Compañias, por ejemplo: usuarios administradores que puedan crear permisos en las aplicaciones y cambiar las configuraciones del sistema.*
  - ✓ *Todo aquel que realice desarrollos, integraciones, APIs, soporte de aplicaciones, hosting web, emisión de certificados, Servicios de pasarelas de pago, almacenamiento y cómputo en nube, servicios de soporte informático y servicios de pentest o hacking ético (Presencial o remoto), prestadores de servicios de telecomunicaciones, mensajería como SMS, Correo electrónico, whatsapp y similares, etc.*

- ✓ ***Tercero relevante o clave SOX:*** *un tercero relevante bajo SOX es cualquier entidad externa o interna que participa directa o indirectamente en procesos que impactan significativamente la información financiera, los controles internos sobre la información financiera (ICFR) , la preparación de los estados financieros, la ejecución de controles generales de TI que soportan elementos de TI o que administran aplicaciones alcanzadas, y sobre cuya actividad la compañía debe mantener control o supervisión.*
- ✓ ***Negociador:*** *Persona responsable de gestionar el proceso de contratación o relacionamiento con el proveedor.*
- ✓ ***Administrador de contrato:*** *Persona encargada de supervisar la ejecución del contrato y verificar el cumplimiento de las obligaciones pactadas.*
- ✓ ***Administrador de proveedor:*** *colaborador del tercero que se hace responsable de reportar evidencias de cumplimiento y riesgo cyber, novedades de acceso y ciberseguridad.*
- ✓ ***Seguridad de la información:*** *Conjunto de medidas orientadas a proteger la confidencialidad, integridad y disponibilidad de la información.*
- ✓ ***Ciberseguridad:*** *Prácticas y controles orientados a proteger sistemas, redes, aplicaciones, dispositivos e información frente a amenazas digitales.*
- ✓ ***Tecnologías de la Información (TI):*** *Recursos tecnológicos usados para procesar, almacenar, transmitir y proteger información, como aplicaciones, servidores, redes y equipos de cómputo.*
- ✓ ***Tecnologías de la Operación (TO):*** *Tecnologías que monitorean o controlan procesos operativos, industriales o de infraestructura.*
- ✓ ***Dato sensible:*** *Información cuyo uso indebido puede afectar la intimidad del titular o generar discriminación, como datos de salud, biométricos o financieros, entre otros.*
- ✓ ***Información confidencial:*** *Información de acceso restringido que, si se divulga sin autorización, puede generar afectaciones legales, reputacionales, operativas o económicas.*
- ✓ ***Know how:*** *Conocimiento especializado, metodologías, prácticas o experiencia propia de la compañía que le generan valor.*

- ✓ ***Clasificación de la información:*** *Proceso mediante el cual la información se organiza según su nivel de sensibilidad y las medidas de protección que requiere.*
- ✓ ***Fuente autoritativa de terceros (FAT):*** *Registro oficial definido por la organización para identificar y administrar terceros con acceso a información, sistemas o recursos corporativos.*
- ✓ ***Acceso:*** *Permiso otorgado a una persona para ingresar o utilizar información, aplicaciones, sistemas, redes, sedes o recursos de la organización.*
- ✓ ***Mínimo privilegio:*** *Principio según el cual una persona solo debe tener los accesos estrictamente necesarios para cumplir su función.*
- ✓ ***Segregación de funciones:*** *Distribución de responsabilidades entre diferentes personas para reducir errores, fraudes o usos indebidos.*
- ✓ ***Incidente de seguridad de la información:*** *Se entiende por un incidente de seguridad aquel evento o serie de eventos inesperado(s) o no deseado(s) de seguridad de la información, que comprometen la operación de la compañía, amenazan la seguridad de la información (CID), o corresponden a una violación o amenaza inminente de las definiciones de seguridad.*
- ✓ ***Debida diligencia:*** *Validación previa que se realiza a un tercero para identificar riesgos y verificar que cumple los requisitos exigidos por la organización.*
- ✓ ***Prueba de concepto:*** *Evaluación controlada de una herramienta, solución o servicio antes de su adopción definitiva.*
- ✓ ***Acuerdo de confidencialidad:*** *Compromiso formal mediante el cual una parte se obliga a proteger la información recibida y a no divulgarla sin autorización.*
- ✓ ***Servicio en la nube:*** *Servicio tecnológico prestado a través de internet para almacenamiento, procesamiento, software o infraestructura.*
- ✓ ***Plan de respuesta a incidentes:*** *Documento o procedimiento que define cómo detectar, contener, atender y recuperar la operación ante un incidente de ciberseguridad.*
- ✓ ***Pruebas de intrusión / hacking ético****: Evaluaciones controladas para identificar vulnerabilidades en sistemas, aplicaciones o infraestructuras.*

- ✓ ***Vulnerabilidad**: Debilidad en un sistema, proceso o control que puede ser explotada por una amenaza cibernética.*
- ✓ ***SOX:** Referencia a la Ley Sarbanes-Oxley y a los controles asociados al reporte financiero y al control interno.*
- ✓ ***ICFR:** Controles internos sobre el reporte financiero.*
- ✓ ***OWASP:** Comunidad y marco de referencia enfocado en seguridad de aplicaciones.*
- ✓ ***OWASP Top 10:** Lista de los principales riesgos de seguridad en aplicaciones.*
- ✓ ***NIST CSF 2.0:** Marco de referencia del National Institute of Standards and Technology para gestionar riesgos de ciberseguridad.*
- ✓ ***ISO 27001:** Norma internacional para sistemas de gestión de seguridad de la información.*
- ✓ ***ISA/IEC 62443:** Serie de estándares orientados a la ciberseguridad en entornos industriales y de tecnologías de operación.*
- ✓ ***HIPAA**: Norma de referencia relacionada con la protección de información de salud.*

- ✓ ***Niveles de clasificación de la información:***

Dominio público	*Es la información que ha sido declarada de conocimiento público por parte del responsable de la información basado en las políticas definidas.*
Uso Interno / Datos Generales	*Es la información que puede ser conocida por todos los empleados de la compañía, sin restricción y que no puede ser conocida por personas externas a la compañía.*
Confidencial Compañía	*Contiene información del saber hacer o información privada de la Compañía, esta información puede ser conocida sólo por un grupo de empleados y no contiene datos privados ni sensibles de los clientes, proveedores, empleados pertenecientes a la misma (contratados, subcontratados, asesores o intermediarios).*
Confidencial Datos Sensibles	*Información que contiene datos privados/sensibles de cualquier cliente, proveedor, empleado y/u otro grupo de interés de la compañía (contratados, subcontratados, asesores o intermediarios).*

4. LINEAMIENTOS

Todos los proveedores, terceros, negociadores, administradores de contratos, administradores de proveedores, deben dar cumplimiento a la política, directrices y lineamientos de seguridad, establecidos en el marco normativo de seguridad, para la protección de la información y no incurrir en conductas que generen riesgos o puedan ocasionar incidentes que afecten a la información y/o la reputación u operación de Las Compañías, su incumplimiento puede derivar en sanciones y repercusiones legales de acuerdo con lo contratado.

Consideración: *Las medidas de seguridad y su nivel de rigurosidad dependerán del tipo de información a la que tenga acceso el tercero, así como de si se trata de una persona natural o jurídica (empresa).*

4.1. Obligaciones del Negociador y/o Administrador de Contrato

4.1.1. El administrador de Contrato debe:

4.1.1.1. Gestionar tan pronto se detecte, los requerimientos de accesos para terceros, es decir, asignación, modificación o retiro de permisos de usuario en aplicaciones, herramientas o sedes de las Compañías. Para todos los eventos de retiro se deben generar las novedades oportunas mediante las herramientas de Gestión de requerimientos de Tecnología.

4.1.1.2. Asegurar que, si un tercero requiere acceso a aplicaciones o sistemas de información de la compañía, debe estar previamente registrado o inventariado en la Fuente Autoritativa de Terceros definida por el responsable de Ciberseguridad.

4.1.1.3. Asegurar que el proveedor/Tercero responde a las solicitudes de Ciberseguridad con relación a actividades de monitoreo y verificaciones de cumplimiento, entre ellas y sin limitarse, charlas de ciberseguridad, actividades de concientización, comunicaciones relevantes, revisiones periódicas de la vigencia de los accesos o permisos de usuario, cuestionarios de debida diligencia o cumplimiento en ciberseguridad.

4.1.2. El negociador debe:

4.1.2.1. Tener en cuenta que, cuando la contratación involucre aplicaciones o servicios en la nube, debe notificar al responsable de legal/Jurídico la ubicación geográfica de los datos o la información

con el fin de validar si es viable almacenar la información acorde con las definiciones de privacidad y tratamiento de datos personales, y en todo caso, se deberá establecer la obligación de notificar el traslado de los datos en caso de que esto ocurra.

4.1.2.2. Cuando se realicen pruebas de concepto para validar las funcionalidades de herramientas y soluciones tecnológicas que impliquen la entrega de información de uso interno, confidencial o sensible al tercero, el proveedor/tercero deberá firmar con la Compañía, un acuerdo de confidencialidad.

4.1.3. El negociador o Administrador de contrato, debe hacer saber al tercero los medios y canales disponibles para el manejo de la información en Office 365, Sharepoint y Microsoft teams, cuando sea requerido.

4.2. Obligaciones del tercero

4.2.1. El tercero debe definir y comunicar al responsable SURA, un Administrador de Proveedor (AP) que se encargue de administrar los permisos de acceso (Altas, bajas y modificaciones de sus colaboradores con acceso a información de Las Compañías), así como sus revisiones periódicas solicitadas por Las Compañías.

***Nota**: Cuando se trate de un tercero, persona natural, este debe asumir el rol de administrador de proveedor (AP).*

4.2.2. El Administrador de Proveedor en el tercero debe velar por:

*4.2.2.1. **Reportar cambios significativos en la prestación del servicio como:***

4.2.2.1.1. Cambio de ubicación de datos;

4.2.2.1.2. Cambio de subprocesadores o subcontratistas;

4.2.2.1.3. Cambio de plataforma tecnológica o controles tecnológicos críticos;

4.2.2.1.4. Incidentes relevantes;

4.2.2.1.5. Cambios en certificaciones de seguridad, si aplica;

4.2.2.1.6. Cambios societarios o de operación.

4.2.2.2. Gestionar y proveer las evidencias que le sean solicitadas por el área de ciberseguridad para la evaluación del riesgo de Cyber en el tercero.

4.2.2.3. *Revisar oportunamente la vigencia y continuidad de los permisos de accesos de sus colaboradores de acuerdo con los procesos internos de Las Compañías.*

4.2.2.4. *Asegurar que se realicen internamente capacitaciones y concientización en materia de ciberseguridad a sus colaboradores al menos una vez al año. Y en caso de que aplique, convocar a las iniciativas de concientización y capacitación en materia de seguridad de la información a los que sea invitados por parte de las Compañías.*

4.2.2.5. *Se reporten oportunamente los incidentes de seguridad que puedan comprometer la confidencialidad, integridad o disponibilidad de la información o notificar al correo:* ***IncidentesSeguridad@suramericana.com.co***

4.2.2.6. *Durante la negociación y vigencia del contrato, quien haga sus veces de responsable del proceso con el tercero, debe propender por utilizar los medios o recursos autorizados para compartir información, prevaleciendo el uso de herramientas de Microsoft Office 365 de las Compañías.*

4.2.3. *El tercero debe conectarse remotamente o en sitio a las aplicaciones o recursos de las Compañías, a través de los medios establecidos y aprobados por el área de Tecnología y ciberseguridad.*

4.2.4. *El tercero debe contar con un plan de respuesta a incidentes de ciberseguridad documentado y probado que incorpore desde la detección, contención, respuesta y recuperación de la operación.*

4.2.5. *Cumplir con los requisitos legales en seguridad, privacidad y tratamiento de datos personales exigidos en el país donde esté ubicado y donde opere.*

4.2.6. *Garantizar que las compañías contratadas por el tercero a las cuales se les delega actividades de manejo de información de las Compañías, cumplen con la política, directrices y lineamientos de seguridad, establecidos en el marco normativo de seguridad para la protección de la información y no incurrir en conductas que generen riesgos o puedan ocasionar incidentes que afecten a la información o la operación, su*

incumplimiento puede derivar en sanciones y repercusiones legales de acuerdo con lo contratado.

4.2.7. *El tercero deberá contar con equipos de cómputo seguros, debidamente identificados mediante una nomenclatura formal y documentada, que permita al responsable de ciberseguridad de Las Compañías, habilitar permisos de conectividad únicamente sobre aquellos recursos previamente validados. Estos equipos deberán cumplir, como mínimo, con los siguientes requisitos: legalidad del software instalado, protección de punto final (antimalware) y, cuando aplique, uso de canales de conectividad privada (VPN).*

4.2.8. *Cuando se tenga acceso a información confidencial y sensible, el tercero debe adoptar como buena práctica marcos de referencia para la gestión de la seguridad de la información, ciberseguridad de las TI y TO y sin limitarse a:*

- *ISO 27001, NIST CSF 2.0.*
- *Privacidad desde el diseño.*
- *Si manejan dispositivos o Tecnologías de la Operación, adoptar ISA IEC 62443, HIPAA.*
- *Regulaciones/marcos aplicables al país donde opera.*

4.2.9. *Todo proveedor/Tercero que preste un servicio donde trate información confidencial o sensible de las Compañías, a través de sus propias herramientas y/o aplicaciones, debe demostrar evidencia de las pruebas de intrusión o hacking ético mínimamente dos veces al año cuando le sea requerido por la compañía.*

4.2.10. *Mantener actualizadas las herramientas tecnológicas y el software de los computadores con los que presta un servicio a las Compañías.*

4.2.11. *Cuando aplique, tener evidencia de los resultados de auditorías de seguridad realizadas por terceros en los últimos dos años. En caso de que sea un proveedor relevante para SOX, se deben tener los resultados de auditoría del año actual o en curso.*

4.2.12. *Adoptar como buena práctica estándares internacionales o aquellos fijados por las Compañías cuando se desarrolle o mantenga soluciones de TI. Por ejemplo:*

i. *OWASP TOP 10 para aplicaciones*
ii. *OWASP Top 10 para Modelos LLM.*

iii. *OWASP API Security Top 10*

4.2.13. Disponer de mecanismos adecuados para cuidar la continuidad del negocio con los servicios que presta a las Compañías, entre ellos, backups, pruebas de restauración, aislamiento de datos, cuando aplique.

4.2.14. Monitorear y realizar una adecuada gestión de vulnerabilidades sobre el software de otros terceros o software propietario que utilice en sus servicios y equipos de cómputo.

4.2.15. El tercero debe garantizar al terminarse la relación contractual que se aplican controles como:

4.2.15.1. Revocación de accesos;

4.2.15.2. Devolución o destrucción segura de información;

4.2.15.3. Certificación de eliminación segura de la información;

4.2.15.4. Devolución de activos;

4.2.15.5. Conservación de evidencias cuando aplique por temas legales o SOX.

4.3. Uso de IA generativa en servicios de terceros

4.3.1. El tercero no debe cargar, procesar o compartir información de las Compañías en herramientas de inteligencia artificial generativa, públicas o privadas, sin autorización previa y evaluación de riesgos de seguridad, privacidad y legal.

4.4. **Derecho de auditoría o verificación**

4.4.1. Las Compañías pueden solicitar evidencias, certificaciones, reportes, auditorías o verificaciones sobre los controles de seguridad del tercero, especialmente cuando trate información confidencial, sensible, SOX o preste servicios críticos.

5. DIVULGACIÓN

La presente Directriz hace parte integral de la Política general de seguridad de la información y ciberseguridad como una especificación de sus lineamientos, la cual deberá ser publicada a todos los grupos de interés dentro de los sitios definidos por las Compañías.

El rol encargado de la Ciberseguridad en las Compañías será la responsable de la administración de esta directriz y en esa medida gestionará con las áreas involucradas en las Compañías para su divulgación, cumplimiento y actualización.

6. GOBERNABILIDAD

El rol encargado de la Ciberseguridad en las Compañías, será la instancia responsable del gobierno de esta directriz. Cualquier modificación o excepción deberá ser aprobada por éste mismo órgano, siguiendo los lineamientos establecidos.

CONTROL DE CAMBIOS		
N° REVISIÓN	AUTOR DE LA REVISIÓN	DESCRIPCIÓN DE LA REVISIÓN/CAMBIO
1	LEIDY TATIANA VÉLEZ ANIBAL ALEJANDRO ALVAREZ CIBERSEGURIDAD Y CONFIANZA DIGITAL	CREACIÓN DE LA DIRECTRIZ Y REVISIÓN DE PARTE DE ABASTECIMIENTO CONEXXIÓN 22/04/2026
1	CAROLINA ARANGO COORDINADOR GESTIÓN Y DESARROLLO DE PROVEEDORES LINA MARCELA PEREZ LÍDERES ASUNTOS LEGALES JUAN FELIPE GÓMEZ DIRECTOR DE CONTROL INTERNO Y RIESGO DE TI ANYI SULEIMA GAVIRIA VALENCIA COORDINADOR GESTIÓN DE ACCESOS E IDENTIDADES ANDRES FELIPE ARISTIZABAL ANALISTA DE INFRAESTRUCTURA – OPERACIÓN CIBERSEGURIDAD CARLOS RESTREPO MIRA	REVISIÓN DE LINEAMIENTOS Y PRÁCTICAS EM ALINEACIÓN CON EL PROCESO LEGAL, GESTIÓN DE ACCESOS, ABASTECIMIENTO 10/06/2026

	ANALISTA DE INFRAESTRUCTURA – GOBIERNO DE ACCESOS *CONEXXIÓN SURA*	
1	*JUAN DAVID RESTREPO* *LÍDER DE CIBERSEGURIDAD Y CONFIANZA DIGITAL* *CONEXXIÓN SURA*	*07/07/2026*

DOCUMENTOS RELACIONADOS

TÍTULO	*VERSIÓN*	*FECHA*
POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	*8*	*APROBACIÓN EN JUNTA DIRECTIVA DE SURAMERICANA S.A.* *19/03/2026*
POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	*1*	*APROBACIÓN ASAMBLEA GENERAL CONEXXION SURA* *ACTA #2* *25/03/2026*

CLASIFICACIÓN DE LA INFORMACIÓN

DATOS GENERALES - USO EXTERNO