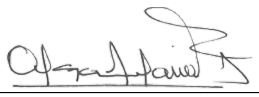
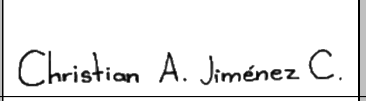
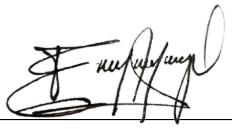
proindesa Ingeniería & Desarrollos	MATRIZ DE EQUIVALENCIA FUNCIONAL	**Código:** F-1168
		Fecha: 01/09/2025
		Versión: 01

INFORMACIÓN GENERAL DEL DOCUMENTO			
Código:	PNDS-PO-GRC-01	**Nombre del documento:**	Política de Ciberseguridad y S.I
Versión	8	**Fecha de Vigencia**	27/03/2026
Descripción del lineamiento	De conformidad con lo establecido en el memorando PD-MEN-PR-058-2025, el cual complementa las instrucciones previamente impartidas por Proindesa S.A.S. mediante el memorando PD-MEN-PR-038-2025, se adopta el documento PNDS-PO-GRC-01 Política de Ciberseguridad y S.I		
Proceso(s) Alcanzado(s) con la Política	Todos los procedimientos de Concesionaria Panamericana relacionados con Seguridad de la Información y Ciberseguridad		

INFORMACIÓN DE EQUIVALENCIA		
Cargo relacionados en el documento	**Equivalencia funcional interna**	**Justificación de la equivalencia**
Área de Riesgo y Cumplimiento	Área de Gobierno, Riesgo y Cumplimiento	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Líder de Riesgo y Cumplimiento	Coordinador GRC	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Presidente	Gerente General	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Vicepresidencia ejecutiva y de sostenibilidad	Gerente General Director de Sistemas Coordinación GRC	Para efectos de velar por el complimiento de la presente política se homologa a estos cargos
Comité de Auditoría	Auditoría	Auditoría de Proindesa, Corficolombiana y Grupo Aval.
Comité de cambios	Comité de Riesgos	En Panamericana el comité de riesgos es el encargado de evaluar los temas se seguridad de la información y ciberseguridad entre otros, asi mismo, el control de cambios en las aplicaciones.
Gerencía de auditoría Interna / Auditoría interna	Auditoría	Función que tiene Proindesa, Corficolombiana y Grupo Aval.

Coordinador de Ciberseguridad y S.I / Líderes de Ciberseguridad y S.I.	Coordinador GRC	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Gerencia Financiera	Director Financiero	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Gerencia T.I	Director de Sistemas	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Jefatura Jurídica Corporativa Gerencia de Litigios Jefatura Jurídica Corporativa	Director de Jurídico	Estructura organizacional aprobada para Concesionaria Panamericana S.A.S.
Comité de Ciberseguridad y S.I	Comité de Riesgos	En Panamericana el comité de riesgos es el encargado de evaluar los temas se seguridad de la información y ciberseguridad conforme a las responsabilidades establecidas en la Política de Comités.

RESPONSABLES DE LA VALIDACIÓN					
Área de Gobierno, Riesgos y Cumplimiento		**Área de Calidad, Procesos o equivalente**		**Área con mayor injerencia procesal**	
Firma:		**Firma:**		**Firma:**	
Nombre:	OLGA LUCIA AFANADOR MARIN	**Nombre:**	CHRISTIAN ALEJANDRO JIMÉNEZ CORTÉS	**Nombre:**	ERWILENIN CARVAJAL RAMIREZ
Cargo:	COORDINADORA GRC	**Cargo:**	LIDER DE DESARROLLO ORGANIZACIONAL	**Cargo:**	DIRECTOR DE SISTEMAS

proindesa® Ingeniería & Desarrollos	DECLARACIÓN DE EXCEPCIONES Y NO APLICABILIDAD DE POLÍTICAS CORPORATIVAS	**Código:** F-1169
		Fecha: 01/09/2025
		Versión: 01

INFORMACIÓN GENERAL DEL DOCUMENTO			
Código:	PNDS-PO-GRC-01	**Nombre del documento:**	Política de Ciberseguridad y S.I
Versión	8	**Fecha de Vigencia**	27/03/2026
Descripción del lineamiento	De conformidad con lo establecido en el memorando PD-MEN-PR-058-2025, el cual complementa las instrucciones previamente impartidas por Proindesa S.A.S. mediante el memorando PD-MEN-PR-038-2025, se adopta el documento PNDS-PO-GRC-01 Política de Ciberseguridad y S.I		

INFORMACIÓN DE NO APLICABILIDAD POLÍTICA O LINEAMIENTO		
Numeral	**Descripción**	**Justificación de no aplicabilidad**
7.1	Notas al pie - 1 Roles y Responsabilidades definidos en el Procedimiento de Monitoreo de Seguridad de la Información PNDS-PR-GRC-14. 2 Se descargará el MFA Authenticator de Microsoft, según el documento Línea Base de Software Corporativo PNDS-DG-TEC-08 cuyo propósito sea desarrollar la gestión operativa de accesos corporativos, promoviendo las buenas prácticas de seguridad a través de la autenticación multifactor.	Se aplican los procedimientos, instructivos y formatos propios de Panamericana.
7.1.	Asegurar la protección de la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información. Para el caso puntual del "MFA Authenticator" de Microsoft, en caso que el funcionario no consienta su descarga e instalación en un dispositivo propio, no podrá acceder a la VPN, por lo que se deberán establecer otros métodos para la autenticación multifactor o de acceso a la información, aplicativos y/o desarrollos, tales como trabajo presencial permanente (sin acceso a Home Office o trabajo en casa).	Actualmente Panamericana implementó la herramienta corporativa Netskope y su servicio de VPN ZTNA, la cual NO exige multifactor de autenticación.

IDENTIFICACIÓN DE CONTROLES NO APLICABLES		
Control	**Numeral de ubicación**	**Justificación de no aplicación**
N/A	N/A	N/A

PROCESOS ALCANZADOS SOX NO APLICABLES O NORMATIVAS NO APLICABLES	
Proceso o Normativa	**Justificación de no aplicación**
N/A	N/A

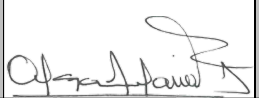
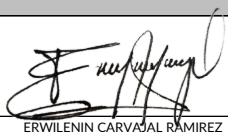
RESPONSABLES DE LA VALIDACIÓN					
Área de Gobierno, Riesgos y Cumplimiento		**Área de Calidad, Procesos o equivalente**		**Área con mayor injerencia procesal**	
Firma:		**Firma:**		**Firma:**	
Nombre:	OLGA LUCIA AFANADOR MARIN	**Nombre:**	CHRISTIAN ALEJANDRO JIMÉNEZ CORTÉS	**Nombre:**	ERWILENIN CARVAJAL RAMIREZ
Cargo:	COORDINADORA GRC	**Cargo:**	LIDER DE DESARROLLO ORGANIZACIONAL	**Cargo:**	DIRECTOR DE SISTEMAS

Tabla de contenido

1. OBJETIVO

Definir los lineamientos para proteger la información de la Proindesa, Sociedades Administradas, Concesionarias y Constructoras (en adelante la Organización), incluyendo la identificación de activos críticos y la gestión de los riesgos de Ciberseguridad y S.I. Este marco se ajusta a las directrices de Grupo Aval y Corficolombiana, incluyendo buenas prácticas, controles, roles y canales de comunicación que mantengan informada a la Alta Dirección, asegurando la continuidad de las operaciones críticas con el fin de dar cumplimiento a los compromisos contractuales ante eventos imprevistos.

2. ALCANCE

Aplica a miembros de Alta Dirección y funcionarios de la Organización que utilicen información o servicios tecnológicos; asimismo, se extiende a los proveedores que mantengan relación con el desarrollo del objeto del negocio.

3. MARCOS DE REFERENCIA Y REGULACIÓN

- **NTC-ISO/IEC 27001-2022:** Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI).
- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios.
- **Ley 1581 de 2012 (Habeas Data):** Por la cual se dictan disposiciones generales para el tratamiento y la protección de datos personales.
- **Ley 1273 de 2009:** Protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones
- **Framework de Ciberseguridad NIST:** Marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo de ciberseguridad.

4. DECLARACIÓN DE COMPROMISO

La Organización se compromete en promover una cultura de cumplimiento y control de acuerdo con los pilares establecidos por el sistema de Administración de Riesgos de Ciberseguridad y Seguridad de la Información, por lo anterior gestiona actividades encaminadas a:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la Política de Ciberseguridad y S.I.
- Promover continuamente una cultura de Ciberseguridad y S.I.

- Gestionar de manera estructurada y estratégica los riesgos de Ciberseguridad y S.I asociados al negocio y su relacionamiento con terceros.
- No hay excepciones a la presente Política.

Todos los miembros de la Organización son responsables de aplicar los criterios definidos en esta política y ajustar sus actuaciones de acuerdo con los lineamientos establecidos en Ciberseguridad y S.I; de igual forma son responsables de reportar los incidentes de los que pudiera a tener conocimiento a través de los canales de comunicación establecidos.

5. POLÍTICA DE CIBERSEGURIDAD Y S.I

La Organización reconoce la importancia de proteger la información frente a amenazas que puedan afectar la continuidad del negocio.

Por ello, establece acciones orientadas a la protección de los activos de información, la gestión de riesgos de Ciberseguridad y S.I, la protección de datos personales y el fortalecimiento de la cultura de seguridad.

Las acciones de cumplimiento de la política se fundamentan en los principios de **Confidencialidad, Integridad, Disponibilidad y Privacidad** de la información; por lo anterior, la Organización garantiza:

1. Cumplir requisitos y principios de Ciberseguridad y S.I.
2. Proteger los activos de información y tecnológicos.
3. Gestionar y mitigar los riesgos asociados a Ciberseguridad y S.I. en los procesos Organizacionales.
4. Definir y divulgar directrices, políticas, normas, estándares y procedimientos que generen compromiso en todas las áreas.
5. Fortalecer la cultura de Ciberseguridad y S.I. de los funcionarios y proveedores, que administren activos de información.
6. Incorporar requisitos de Ciberseguridad y S.I. en el plan de continuidad del negocio frente a incidentes.
7. Mantener vigente la Política mediante revisiones anuales o cuando se presenten cambios estructurales que impacten a la Organización.
8. Permitir que cualquier miembro de la Organización proponga ajustes a la Política, comunicando las inquietudes al correo: seguridad.informacion@proindesa.com.co.

Con base en lo anterior, la Organización adopta políticas que estructuran el Sistema de Ciberseguridad y S.I. como expresión de la Alta Dirección para garantizar una gestión transparente y eficaz de los riesgos, así como la, identificación de controles que los mitiguen razonablemente.

5.1. Protección de la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información

Todos los miembros de la Organización y terceros independientes que tengan acceso a información deben asegurar, la confidencialidad, integridad, disponibilidad y privacidad de la información, de tal manera que la información:

- Solo sea accedida por el personal autorizado.
- Sea concisa, precisa, incidiendo en la exactitud y completitud.
- Este disponible en el momento que sea requerida.
- Sea accedida legítimamente y utilizada para lo que se autorizó.

Para esto, quienes accedan a través de cualquier dispositivo tecnológico (propio o de la Organización), o a través de cualquier aplicación (app), a información de la Organización, su correo electrónico corporativo, y cualquier sitio repositorio o de aplicación tecnológica y/o digital de la Organización, deberán contar de manera previa con autorización y aprobación del acceso correspondiente por las instancias definidas[1], y debe estar acorde con el rol que desempeñe dentro de la Organización.

La Organización podrá instalar en el dispositivo móvil (propio o de la Organización) cualquier software o app que considere necesaria, como, por ejemplo, MFA Authenticator de Microsoft[2], o una app de antivirus, con el fin de propender la confidencialidad, integridad, disponibilidad y privacidad de la información de la Organización.

En este sentido quienes no otorguen su consentimiento para la instalación del software o app requerida por la Organización, en su dispositivo propio no podrá acceder a la información de la Organización (ej. Email corporativo / Microsoft 365). El Área de Riesgo y Cumplimiento, en conjunto con la Vicepresidencia Ejecutiva y de Sostenibilidad o quien haga sus veces y el jefe directo, establecerán alternativas para viabilizar el cumplimiento íntegro de la presente Política, que primará sobre cualquier acuerdo puntual con el funcionario.

Para el caso puntual de la solución tecnológica que defina implementar la Organización para validar la identidad de los usuarios a través del múltiple factor de autenticación, en caso de que el funcionario no consienta su descarga e instalación en un dispositivo propio, no podrá acceder los recursos internos de la Organización , por lo que se deberán establecer otros métodos para la autenticación multifactor o de acceso a la información, aplicativos y/o desarrollos, tales como trabajo presencial permanente (sin acceso a Home Office o trabajo en casa).

Las sociedades del portafolio de infraestructura podrán descargar o instalar software o apps en los dispositivos propios frente a la evidencia de uso para fines Corporativos, así sea de manera ocasional, negarse a esta acción se considerará un incumplimiento a la presente Política.

---

[1] Roles y Responsabilidades definidos en el *Procedimiento de Monitoreo de Seguridad de la Información PNDS-PR-GRC-14.*

[2] Se descargará el MFA Authenticator de Microsoft, según el documento *Línea Base de Software Corporativo PNDS-DG-TEC-08* cuyo propósito sea desarrollar la gestión operativa de accesos corporativos, promoviendo las buenas prácticas de seguridad a través de la autenticación multifactor.

5.2. Cultura de Ciberseguridad y S.I.

La administración del sistema de Gestión de Riesgos de Ciberseguridad y S.I. se gestiona a través una cultura de roles y responsabilidades y que se materializa a través de 3 líneas:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en Ciberseguridad y S.I, en el cumplimiento de políticas y procedimientos organizacionales definidos.
- La segunda línea debe definir y ejecutar actividades de concienciación y cultura sobre las políticas y procedimientos organizacionales de Ciberseguridad y S.I., que abarquen a todos los funcionarios de la Organización.
- La tercera línea debe monitorear la ejecución y el cumplimiento de la cultura y concienciación de Ciberseguridad y S.I.

5.3. Determinar el apetito de riesgo, el nivel de tolerancia y la capacidad de riesgo.

La Alta Dirección y la segunda línea deberán alinearse con la definición y alcance del Modelo Corporativo de Gestión de Riesgos de Ciberseguridad y S.I. del Grupo Aval para definir el apetito de riesgo, el nivel de tolerancia y la capacidad máxima al riesgo, considerando el efecto de la naturaleza de sus operaciones y líneas de negocio, así como los tipos y niveles de Ciberseguridad y S.I.

5.4. Gestionar el cambio

La Alta Dirección y la segunda línea aseguran la implementación del proceso de aprobación que evalúa plenamente los riesgos de Ciberseguridad y S.I. en todos los nuevos procesos, actividades, productos y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realizan cambios sobre alguna aplicación que impacte el negocio, se lleva a un comité de cambios donde se evalúan los posibles riesgos que traería la implementación de dicho cambio. Adicionalmente la Organización implementa y gestiona los riesgos, las normativas, tendencias, definiciones y actualización de estrategias a través de las reuniones periódicas del Comité de Ciberseguridad y S.I., según los lineamientos establecidos en el *Reglamento del Comité de Ciberseguridad y S.I PNDS-DG-GRC-31*.

5.5. Realizar Seguimiento y Presentar Informes

La segunda línea de la Organización asegura la ejecución de actividades necesarias para asegurar el correcto funcionamiento de los monitoreos implementados a nivel de Ciberseguridad y S.I, , según lo establecido en el *procedimiento de Monitoreos de Ciberseguridad y S.I. PNDS-PR-GRC-14*, adicionalmente realiza diagnósticos de Seguridad de la Información ISO 27001 y Ciberseguridad Framework de Ciberseguridad NIST con el fin de calcular el nivel de seguridad y madurez en el que se encuentra la Organización, indicadores corporativos, Evolución de Riesgos y Evolución de controles. De manera específica deberán trabajarse en este mismo sentido los riesgos de Ciberseguridad y S.I. basados en directrices corporativas que apoyen su desarrollo.

5.6. Identificar, Evaluar, Controlar y mitigar los Riesgos de Ciberseguridad y S.I.

La Organización cuenta con procesos que permiten identificar, evaluar, documentar, gestionar y mitigar los riesgos de Ciberseguridad y S.I. Esta valoración al sistema se realiza por lo menos una vez al año o cuando circunstancias especiales ocurran, identificando riesgos y evaluando su probabilidad e impacto, el cual debe estar alineado con la metodología corporativa AVAL de Gestión de Riesgos de Ciberseguridad y S.I. El resultado de estas actividades será registrado en la matriz ITRM de la Organización.

La primera y segunda línea de la Organización mantiene un “ambiente de control”, estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de los riesgos lo cual será reflejado en la madurez del sistema siguiendo los componentes y metodología corporativa establecidos a través de las metas anuales del S.G.S.I.

Con lo anterior, la primera línea debe contar con controles generales de accesos, privilegios, actualizaciones en los siguientes aspectos mínimos:

- Supervisión de controles de accesos físicos.
- Supervisión de controles de accesos lógicos.
- Supervisión y protección de contraseñas.
- Supervisión protección de los puertos de configuración y acceso remoto.
- Restricción de la instalación de aplicaciones por parte del usuario final.
- Asegurar que los sistemas operativos estén “parchados” con las actualizaciones o en su defecto que los controles implementados mitiguen la posibilidad de materialización de un incidente.
- Asegurar que las aplicaciones de software se actualicen regularmente.
- Restricción de los privilegios administrativos (es decir la capacidad de instalar software o cambiar los ajustes de configuración de la computadora).

5.7. Asegurar el sistema de Ciberseguridad y S.I. en situaciones de contingencia

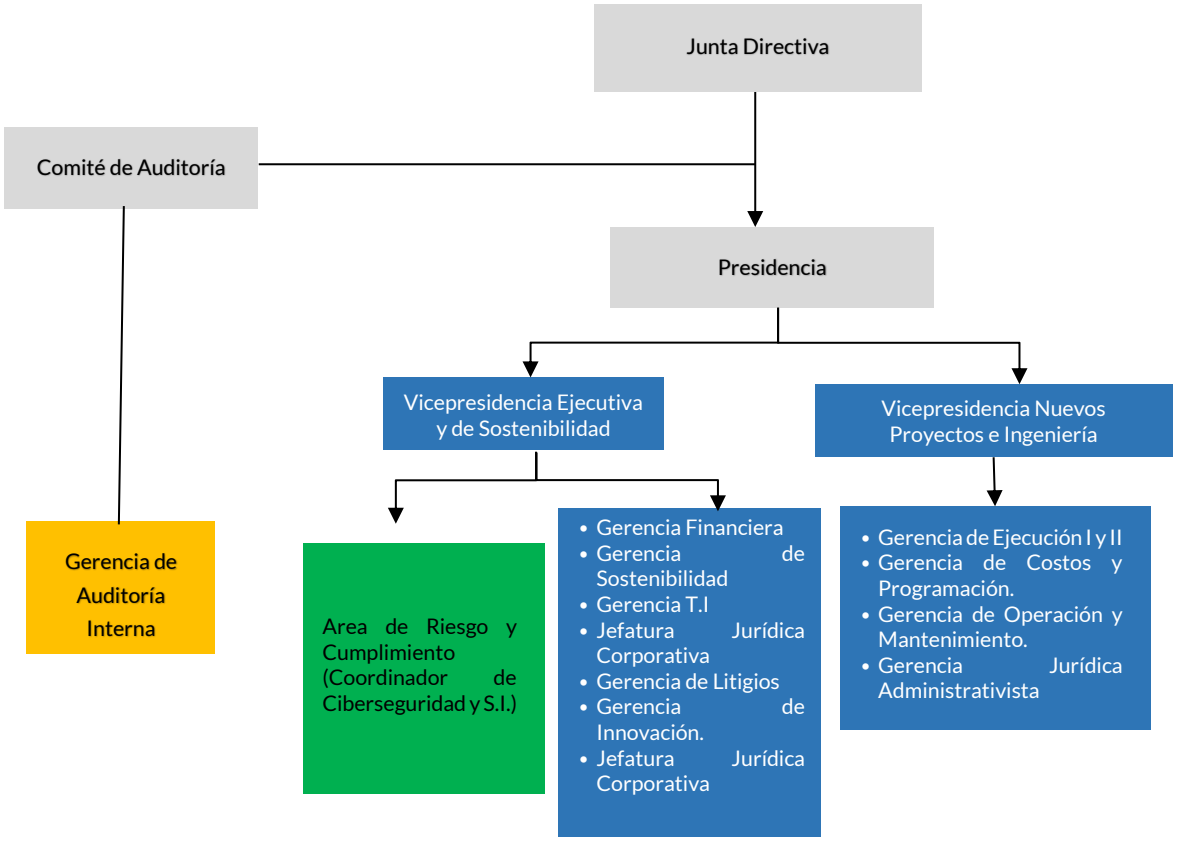
La segunda línea o el responsable de la Ciberseguridad y S.I. de la Organización, debe velar porque en los planes de continuidad del negocio se incluyan y garanticen los pilares de la Ciberseguridad y S.I.

5.8. Garantizar el cumplimiento de la Ley vigente aplicable

Es obligación de las tres líneas de la Organización dar cumplimiento a todas las normas de los reguladores vigentes que le aplique a cada sociedad.

6. GOBIERNO PARA LA GESTIÓN DE CIBERSEGURIDAD Y S.I.

La Organización cuenta con la siguiente estructura Organizacional que garantiza la administración y funcionamiento del sistema de gestión de riesgos en Ciberseguridad y S.I.:



Convenciones Líneas:

Nota: El anterior diagrama representa los cargos que se involucran en la gestión del sistema de Ciberseguridad y S.I., por lo cual no modifica ni resume el organigrama vigente de la Organización.

6.1. Primera Línea

La primera línea la constituyen los responsables de Seguridad Informática (Gerencia T.I) y todos los funcionarios de la Organización. La Política de Ciberseguridad y S.I. reconoce a estos como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de Ciberseguridad y S.I. inherentes a los productos, actividades y procesos, y disponer de los recursos suficientes para realizar eficazmente sus tareas.

Así mismo deben cumplir con políticas y procedimientos definidos por la Organización contribuyendo a una sólida cultura en Ciberseguridad y S.I.

6.2. Segunda Línea

Esta línea está conformada por el Área de Riesgo y Cumplimiento, responsable de la gestión de Ciberseguridad y S.I., la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Ciberseguridad y S.I.

El Área de Riesgo y Cumplimiento, como responsable debe presentar los resultados de gestión directamente a la Alta Dirección o al Comité de Auditoría. Así mismo, debe contar con recursos suficientes para realizar eficazmente todas sus funciones y desempeñar un papel central y proactivo en el Sistema de Gestión de Ciberseguridad y S.I. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos derivados del negocio, incluyendo temas específicos de Ciberseguridad y S.I.

6.3. Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de Ciberseguridad y S.I., así como las políticas, estándares y procedimientos de los sistemas, rindiendo cuentas al Comité de Auditoría. Las personas encargadas de auditorías internas que deben realizar estas revisiones deben ser competentes y estar debidamente capacitadas y no participar en el desarrollo, implementación y operación de la estructura de riesgo/control. Esta revisión puede ser realizada por el área de auditoría interna en la Organización o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

7. ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos de la Política de Ciberseguridad y S.I., se han definido los siguientes actores clave en la Gestión:

Actor	Actividades	
	De ejecución	**De Supervisión**
Comité Corporativo de Ciberseguridad y S.I. de Grupo Aval y Corficolombiana	• Proveer principios, directrices y lineamientos Corporativos de Ciberseguridad y S.I., tomar las acciones preventivas y correctivas pertinentes para las Entidades del Grupo Aval. • Identificar, evaluar e incluir los requerimientos de Ciberseguridad y S.I. en las iniciativas corporativas realizadas para las entidades. • Tomar decisiones relacionadas con la Ciberseguridad y S.I de las entidades. • Socializar actividades y proyectos que sean de interés común y/o impacten a las entidades. • Generar retroalimentación de las jornadas de seguridad y diagnósticos de los SGSI realizados y contribuir a la mejora continua de la postura de Seguridad de la Información. • Definir principios, directrices y lineamientos Corporativos de Ciberseguridad y S.I. • Definir requerimientos de Ciberseguridad y S.I en las iniciativas corporativas realizadas para las entidades. • Socializar actividades y proyectos que sean de interés común y/o impacten a las Empresas del servicio.	• Monitorear el cumplimiento a nivel corporativo de las políticas del Sistema de gestión de Ciberseguridad y S.I. en cada entidad. • Monitorear el cumplimiento a nivel internos de las políticas del Sistema de Ciberseguridad y S.I. en cada entidad.
Junta Directiva o quien haga sus veces	• Aprobar la Política de la Ciberseguridad y S.I. y dar cumplimiento en los requisitos aplicables a estos. • Estudiar y aprobar el apetito de riesgo. • Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la Ciberseguridad y S.I. • Exigir el cumplimiento de las normas y regulaciones gubernamentales de Ciberseguridad y S.I. • Participar en programas de concienciación y capacitación en temas de Ciberseguridad y S.I.	• Supervisar la Ciberseguridad y S.I. en la Organización, comprendiendo los riesgos y asegurando que estos sean gestionados.

Actor	Actividades	
	De ejecución	**De Supervisión**
Alta Dirección	• Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de Gestión de Ciberseguridad y S.I. • Evaluar los informes que le presente el área de Riesgo y Cumplimiento, sobre los resultados de la evaluación de efectividad del programa de Ciberseguridad y S.I., propuestas de mejora en materia de Ciberseguridad y S.I. y resumen de los incidentes que afectaron a la Organización. • Promover la aplicación y apropiación de buenas prácticas de Ciberseguridad y S.I. • Asegurar la evaluación de Ciberseguridad y S.I de todos sus activos de información sin excepción. • Fortalecer la cultura de Ciberseguridad y S.I de los funcionarios de la Organización, proveedores y terceras partes, que administren activos de información de la Organización.	• Supervisar la Ciberseguridad y S.I. en la Organización, comprendiendo los riesgos y asegurando que estos sean gestionados.

Actor	Actividades	
	De ejecución	**De Supervisión**
Comité de Ciberseguridad y S.I.	• Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Ciberseguridad y S.I. • Evaluar y coordinar la implementación de controles específicos de Ciberseguridad para los sistemas o servicios. • Promover la difusión, sensibilización y apoyo a la Ciberseguridad y S.I. • Velar por la actualización continúa de la documentación del sistema de Ciberseguridad y S.I. • Velar porque que las actividades de control definidas frente a los riesgos de Ciberseguridad y S.I. identificados a la fecha, se tenga en cuenta en todos los proyectos de Tecnología, desde su especificación inicial hasta su puesta en producción. • Validar y presentar oportunidades de mejora al Sistema de Gestión de Ciberseguridad y S.I. • Revisar los resultados obtenidos por la función de Ciberseguridad y S.I.	• Monitorear la gestión realizada por medio de los reportes consolidados que le presente periódicamente el área de Riesgo y Cumplimiento, Como resultado de esta revisión, el Comité puede proponer la generación o modificación de lineamientos corporativos que pueden afectar a una o a todas las entidades del sector de infraestructura, según se requiera. De presentarse este tipo de situaciones, el Coordinador de Ciberseguridad y S.I. o el Líder de Riesgo y Cumplimiento, o quienes hagan sus veces, escalaran el tema para validación por parte de los responsables en Corficolombiana como casa matriz de la Organización. • Conocer los Incidentes de Ciberseguridad y S.I. y presentados en las entidades y que hayan tenido impacto significativo, reportados por la Organización, así como de los planes de acción definidos para la mitigación de estos. • Revisar los avances de implementación de herramientas de Ciberseguridad y S.I. dentro de la infraestructura de la Organización.
Líder de Riesgo y Cumplimiento, o quien haga sus veces	• Validar las directrices para el mejoramiento de la gestión de Ciberseguridad y S.I., de acuerdo con el Modelo Corporativo de Ciberseguridad y S.I. y las mejores prácticas en materia. • Planificar el presupuesto financiero y los recursos suficientes para desarrollar las funciones de Ciberseguridad y S.I. • Preparar reportes de Ciberseguridad y S.I. para la Alta Dirección. • Definir los lineamientos de mejora en los procesos del Sistema de Gestión de Ciberseguridad y S.I., en consenso con Corficolombiana y/o Grupo Aval.	• Mantener actualizados los lineamientos de Ciberseguridad y S.I. de acuerdo con las instrucciones corporativas emitidas por Grupo Aval y comunicadas por Corficolombiana. • Apoyar y aprobar los lineamientos de mejora en los procesos del Sistema de Gestión de Ciberseguridad y S.I. • Presentar al Comité de Ciberseguridad y S.I. los avances de implementación de herramientas de Ciberseguridad y S.I. dentro de la infraestructura.

Actor	Actividades	
	De ejecución	**De Supervisión**
	Cumplir con las demás responsabilidades que sean definidas para la Alta Dirección. • Definir lineamientos para la implementación y configuración de herramientas de seguridad T.I y Ciberseguridad, con base en las características de cada herramienta.	
Coordinador de Ciberseguridad y S.I o quien haga sus veces	• Definir e implementar un Sistema de Ciberseguridad y SI, alineado con la estrategia corporativa, el cumplimiento legal, normativo y contractual, con las mejores prácticas internacionales, que apoye los procesos de la Organización y la continuidad del negocio. • Preparar el informe de gestión definido por casa matriz, referente a la gestión de Riesgos de Ciberseguridad y S.I. • Participar en el Comité de Ciberseguridad y S.I. de la Organización. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Propiciar la actualización del inventario de riesgos de Ciberseguridad y S.I. • Mantener actualizada la matriz de riesgos de Ciberseguridad y S.I de la Organización • Adaptar y adoptar los lineamientos que, en materia, sean establecidos por casa matriz. • Apoyar a la primera línea en el proceso de identificación de riesgos y controles, la determinación de su criticidad y verificación del cumplimiento de los planes de acción establecidos en la gestión de incidentes de Ciberseguridad y S.I. • Mantener actualizados los lineamientos de Ciberseguridad y S.I. de la Organización. • Capacitar periódicamente a los funcionarios de la Organización, con el fin de fortalecer la cultura de prevención de riesgos de Ciberseguridad y S.I. • Divulgar en la Organización las instrucciones corporativas que, en materia, remita Corficolombiana y/o Grupo Aval. • Recibir y consolidar información de Ciberseguridad y S.I. de la Organización con el fin de generar reportes de monitoreo	• Verificar la protección de la información, preservando la debida confidencialidad, integridad, disponibilidad y privacidad de la información y mantener la imagen de la Organización. • Conocer los incidentes de Ciberseguridad y S.I. y las medidas que se han implementado para mitigarlas. • Monitorear el resultado de evaluación de Riesgos de la Organización y sus filiales directas. • Definir y monitorear indicadores clave de desempeño sobre la gestión de Ciberseguridad y S.I. • Monitorear el cumplimiento de reportes y de indicadores del sistema de gestión de Ciberseguridad y S.I. de la Organización. • Realizar recomendaciones a las definiciones de controles en los proyectos de la Organización con el fin de garantizar que sean pertinentes para velar por la Ciberseguridad y S.I. en los mismos. • Velar porque se realicen las pruebas de Ciberseguridad y S.I. a la infraestructura tecnológica de la Organización. • Verificar la correcta implementación de herramientas de Ciberseguridad y S.I. con relación a la arquitectura definida.

Actor	Actividades	
	De ejecución	**De Supervisión**
	periódicos, de acuerdo con el protocolo de comunicaciones corporativo. • Definir una arquitectura de seguridad para la Organización y facilitar la incorporación de prácticas de Ciberseguridad y S.I. en todas las áreas.	
Gerencia T. I	• Participar en el Comité de Ciberseguridad y S.I. de la Organización cuando sea necesario. • Adoptar y socializar las mejores prácticas sugeridas en por Comité, Casa matriz y/o Grupo Aval. • Adoptar los lineamientos establecidos por el Coordinador de Ciberseguridad y S.I. o quien haga sus veces. • Informar al Coordinador de Ciberseguridad y S.I o quien haga sus veces sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad y S.I. • Apoyar a la segunda línea en el proceso de identificación de riesgos y controles, así como en su evaluación. • Implementar y operar las herramientas de Seguridad T.I y Ciberseguridad con base en la arquitectura definida por el Área de Riesgo y Cumplimiento, y las características de las herramientas.	• Velar por que se adopten medidas para responder a los incidentes presentados y para prevenir futuros incidentes. • Verificar se adopten las mejores prácticas vigentes en el mercado con respecto a la administración de infraestructura y apoyo en la respuesta a incidentes al Coordinador de Ciberseguridad y S.I. o quien haga sus veces. • Apoyar la definición y medición de indicadores clave de desempeño sobre la gestión de Ciberseguridad y S.I.

Actor	Actividades	
	De ejecución	**De Supervisión**
Responsables de la Información de la Organización	• Identificar, clasificar y proteger la información bajo su responsabilidad, conocer los riesgos a los que podría estar expuesta y velar porque se provean los mecanismos necesarios para que estos riesgos se mitiguen a niveles aceptables, considerando costo-beneficio para los procesos a su cargo. • Con el apoyo de la segunda línea, identificar los controles clave para mitigar los riesgos identificados. • Llevar a cabo la ejecución de los controles para mitigar los riesgos (Autocontrol). • Definir y ejecutar los planes de acción para mitigar los riesgos de seguridad de la información a su cargo. • Reportar al área de Riesgo y Cumplimiento, cualquier incidente de Ciberseguridad y S.I. y de manera particular cualquier evento material de Ciberseguridad y S.I.	• Vigilar y velar que su equipo de trabajo dé cumplimiento a la Política de Ciberseguridad y S.I.
Auditoría Interna	• Adelantar las pruebas de auditoría que considere apropiadas de acuerdo con el plan de trabajo anual probado por el Comité de auditoría de la Organización.	Evaluar y vigilar el cumplimiento de la Política de Ciberseguridad y S.I.

8. SEGURIDAD EN NUEVAS TECNOLOGÍAS Y RIESGOS EMERGENTES

La Organización ha implementado normas y lineamientos de Ciberseguridad y S.I., con relación a los servicios de infraestructura de la Organización, con el fin de articular capacidades como integración de datos, digitalización, automatización de procesos, seguridad en la nube, entre otros, alineando esfuerzos para monitorear, desarrollar e implementar estrategias de remediación de los riesgos emergentes, donde se describen las actividades para:

- Definir políticas de Ciberseguridad y S.I. para nuevas tecnologías implementadas.
- Aplicar procedimientos para clasificar información, gestionar usuarios y asignar responsables, asegurando controles adecuados en las nuevas tecnologías.
- Documentar procesos de muestreo, generación de reportes, flujos de automatización, codificación y pruebas de las tecnologías utilizadas.
- Gestionar y monitorear riesgos cibernéticos y de terceros derivados de nuevas tecnologías, incluyendo riesgos operativos, financieros, regulatorios y tecnológicos.

- Incorporar requisitos de Ciberseguridad y S.I. en el plan de continuidad del negocio para sistemas automatizados y servicios digitales.
- Supervisar el desempeño de sistemas automatizados, garantizando cumplimiento regulatorio y alineación con políticas internas.

9. MODELO DE EVALUACIÓN DEL SISTEMA DE GESTIÓN DE CIBERSEGURIDAD Y S.I.

Para la identificación de riesgos y la aplicación de controles, la Organización adopta y da a conocer el Modelo de Evaluación de Ciberseguridad y S.I. emitido por Grupo Aval. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión e identificar las oportunidades de mejora que permitan fortalecerlo, basado en los dominios y controles propuestos en la norma NTC-ISO 27001:2022 y en el Framework de Ciberseguridad NIST.

10. COMUNICACIÓN DE LINEAMIENTOS CORPORATIVOS

Para propender por la estandarización de la aplicación del cumplimiento de los lineamientos corporativos en todas las entidades del Grupo Aval, se establece como mecanismo de información oficial los siguientes:

- **Instrucciones Generales**, donde incluirá actividades, por lo general metodológicas, previa evaluación, análisis y acuerdo con los especialistas competentes de cada una de las entidades el Equipo de Ciberseguridad y S.I. Corporativo (Grupo Aval) emite instrucción general a Presidentes, Líderes de Ciberseguridad y S.I. y cuando aplique dueños de proceso de los cuatro Bancos y Corficolombiana y sus inversiones. Estos a su vez divulgan la instrucción general a sus pares de las filiales respectivas y algunas veces a otras áreas de interés según se indique en la Instrucción. Lo anterior en cumplimiento del Protocolo de Comunicación definido por la Vicepresidencia Senior Corporativa de Riesgos y Cumplimiento del Grupo Aval.
- **Conceptos,** son aclaraciones o ampliación de información, útiles para dar cumplimiento las instrucciones generales, generalmente comunicaciones por medio de correo electrónico institucional. El Equipo de Ciberseguridad y S.I. Corporativo emite Conceptos a los Líderes de Seguridad de la Información de los cuatro Bancos y Corficolombiana y sus inversiones, así como filiales adicionales en casos especiales, y éstos a su vez divulgan los Conceptos a los Líderes de Ciberseguridad y S.I. de las filiales respectivas siguiendo el protocolo de comunicación.

La comunicación de estos lineamientos deber ser trasmitida desde Proindesa S.A.S hasta la última de las filiales directas de sus sociedades administradas y empresas pertenecientes al portafolio de inversiones del sector infraestructura.

11. REPORTES

Con el fin de facilitar el monitoreo de cumplimiento, Corficolombiana o Grupo Aval solicita diferentes reportes de gestión que constituye un efectivo apoyo para la administración; estos deberán ser veraces, comprensibles, completos y oportunos.

Así mismo, la Organización deberá informar a Corficolombiana, aquellos incidentes Ciberseguridad y S.I. que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de las sociedades pertenecientes al portafolio de inversión del sector infraestructura en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos a través de Proindesa como Holding y líder del sector.

Adicionalmente, la Organización deberá tener una base de datos consolidada de incidentes de Ciberseguridad y S.I clasificada en tipo de incidente, impacto y plan de remediación, así como, que este reporte se encuentre protegido dada la sensibilidad de esta información.

12. CAPACITACIÓN Y ENTRENAMIENTO

Los funcionarios y terceros deben tener conocimiento de las políticas y procedimientos de Ciberseguridad y S.I. que deben aplicar, adicionales a los que se requieren para ejecutar sus actividades. Como parte del programa de capacitación, el personal nuevo que ingrese a las sociedades de la Organización debe asistir durante el periodo de inducción, a una charla sobre los requerimientos del sistema en la Organización.

Así mismo, anualmente para la totalidad de los funcionarios el área de Riesgo y Cumplimiento programa la realización de una capacitación y/o actualización sobre Ciberseguridad y S.I. La capacitación y entrenamiento se puede brindar en forma continua, virtual o presencial, con el propósito de fortalecer los conceptos y asegurar la continuidad y sostenibilidad del Sistema.

13. INVESTIGACIÓN Y SANCIONES

El cumplimiento de la Política de Ciberseguridad y S.I. con sus respectivas normas es de obligatorio cumplimiento para todos los funcionarios, de tal manera que cada funcionario debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en Ciberseguridad y S.I., así como de la protección de los activos de información de la Organización.

La Organización reconoce que en el evento de incumplimiento de esta política y demás actividades que se deriven de ella, los funcionarios encargados de su aplicación y/o cumplimiento deberán someterse a sanciones administrativas y legales. Dicho proceso se realizará de acuerdo con las políticas internas de la Organización relacionadas con el manejo de faltas.

14. DOCUMENTOS Y REGISTROS REFERENCIADOS

- PNDS-MN-GRC-03 Normas de Seguridad de la Información y Ciberseguridad
- PNDS-PR-GRC-14 Monitoreos de Ciberseguridad y S.I.
- PNDS-DG-GRC-31 Reglamento Comité Ciberseguridad y S.I.

15. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	22/06/2017	Creación del documento
2	25/09/2020	Actualización general del documento con base en el documento M-AR-SI-01 Política Corporativa de Seguridad de la Información y Ciberseguridad de Grupo Aval Versión No 1.
3	26/08/2021	Actualización general del documento con base en el documento M-AR-SI-01 Política Corporativa de Seguridad de la Información y Ciberseguridad FinalV2. Recibida mediante Instrucción Seguridad de la Información y Ciberseguridad N°23. Se actualizan los cargos en el esquema de líneas de defensa de acuerdo con el organigrama vigente. Se incluye periodicidad de revisión de la Política de Seguridad de la Información y Ciberseguridad.
4	29/09/2023	Se ajusta la política de acuerdo con la instrucción de seguridad de la información y ciberseguridad No. 29 del Grupo Aval y se realizan los siguientes cambios: • En el numeral 6 se incluye que la política no tiene excepciones. • Se adiciona en el numeral 7.1 la obligatoriedad de instalación del software que considere la Organización, para garantizar la protección de la confidencialidad, integridad, disponibilidad y privacidad de la información de la Organización, por parte de los funcionarios en los dispositivos en los que se autorice dicho acceso. • Se ajusta numeral 14 incluyendo charla de seguridad de la información y ciberseguridad a los funcionarios nuevos dentro de la etapa de inducción. • Se ajusta numeral 15 incluyendo la obligatoriedad en el cumplimiento de las políticas y normas por parte de los funcionarios.

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
5	17/11/2023	• Se reemplaza en la introducción la frase "Alta Dirección" por Asamblea de Accionistas, Junta Directiva, Representante Legal. • Se ajusta la declaración de compromiso del numeral 6, relacionando la aplicabilidad a *"Todos los miembros de la organización"*. • Se relaciona en el numeral 7 aplicabilidad de la descripción a terceros independientes que tengan acceso a información. • Se elimina la Dirección del diagrama del gobierno para la gestión de S.I.
6	13/12/2024	• Se ajusta el nombre del documento de "Política en seguridad de la información y ciberseguridad" por "Política de Ciberseguridad y S.I" • Se realiza actualización de los cargos relacionados en el documento, según la descripción del actual organigrama. • Se adiciona en las responsabilidades del Comité de Ciberseguridad y S.I, la función de verificar los avances de implementación del sistema de gestión. De la misma manera se ajustan las responsabilidades de la Gerencia de Riesgo y Cumplimiento y Gerencia T.I • Se agrega en el Gobierno para la gestión de Ciberseguridad y S.O referenciado en el numeral 8 a la Gerencia de Inversiones e Innovación • Se ajusta en todo el documento la frase "seguridad de la informacion y Ciberseguriad" por "Ciberseguridad y S.I"
7	29/08/2025	• Se realiza actualización de la referencia de la Gerencia de Riesgo y Cumplimiento, por la Gerencia de Innovación, Ciberseguridad y S.I, de acuerdo con las modificaciones organizacionales presentadas. • Se elimina la definición de Política de Ciberseguridad. • Se ajusta el gráfico del Gobierno para la Gestión de Ciberseguridad y S.I. • Se unifican los roles y responsabilidades del Comité Corporativo de Ciberseguridad y S.I de Grupo Aval y Corficolombiana. • Se modifican los roles y responsabilidades del *"Gerente de Innovación, Ciberseguridad y S.I."*, y del *"Coordinador de Ciberseguridad y S.I."*

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
8	27/03/2026	• Se modifica el código del documento, pasando de *DG-0201* a *PNDS-PO-GRC-01* • Se actualiza la dependencia de Ciberseguridad y S.I de la Gerencia de Innovación por el Área de Riesgo y Cumplimiento. • Se actualiza la estructura de Gobierno del numeral 8 cambiando la gerencia de innovación por Área de Riesgo y Cumplimiento. • Actualización de la información del Gobierno para la Gestión de Ciberseguridad y S.I. • Ajuste de los roles y responsabilidades de las actividades, así como la redacción de la seguridad en nuevas tecnologías y riesgos emergentes. • De manera general se ajusta redacción, contenido y ortografía en todo el documento.

16. FIRMAS DE REVISIÓN Y APROBACIÓN

El documento original está firmado y controlado por Proindesa S.A.S.