CONTENIDO

1. INTRODUCCIÓN

Las amenazas que vulneran la Seguridad de la Información y Ciberseguridad pueden afectar considerablemente la reputación de Proindesa S.A.S. y sus sociedades administradas en adelante "La Organización", así como sus activos de información más importantes. Conscientes de las consecuencias como el valor de la información en formato físico o digital, los sistemas interconectados que la procesan, almacenan o trasmiten y como respuesta a su compromiso en la protección de los pilares de Seguridad de la información y Ciberseguridad, la Organización extiende la presente Política en aras de proteger y garantizar la disponibilidad, confidencialidad, integridad y privacidad de la información, desarrollando actividades que permitan establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información y Ciberseguridad.

Por lo tanto, los miembros de Asamblea de Accionistas, Junta Directiva, Representante Legal, Presidente, Vicepresidentes, y funcionarios de la Organización deben actuar conforme a los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos que soporten la Política de Seguridad de la Información y Ciberseguridad; teniendo en cuenta que la Alta Dirección tiene el firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de Seguridad de la Información y Ciberseguridad de la Organización.

2. OBJETIVO

2.1. Objetivo General

Proteger los activos de información de la Organización, gestionando y cumpliendo los principios generales que preservan la Confidencialidad, Integridad, Disponibilidad y Privacidad de la información mediante la definición de políticas y directrices que permitan identificar los riesgos y sus actividades de control, fijando los roles y responsabilidades de los actores clave, que intervienen en el Sistema de Gestión de Seguridad de la Información (SGSI).

2.2. Objetivos Específicos

Los objetivos específicos que persigue la Política de Seguridad de la Información y Ciberseguridad son:

- Establecer lineamientos para mantener los pilares de Seguridad de la Información y Ciberseguridad en la Organización.
- Definir de qué manera la información debe ser protegida de forma homogénea con base en la valoración de los activos críticos de información de la Organización.
- Cumplir las directrices corporativas de Grupo Aval y Corficolombiana, en los temas relacionados con Seguridad de la Información y Ciberseguridad que le sean aplicables de acuerdo con el negocio.
- Garantizar la adecuada gestión de los riesgos de Seguridad de la Información y Ciberseguridad en la Organización.
- Identificar, establecer e implementar actividades de control que preserven los pilares de Seguridad de la Información y Ciberseguridad en la Organización.
- Establecer los roles y responsabilidades en materia de control de los pilares de Seguridad de la Información y Ciberseguridad en la Organización.

- Establecer canales de comunicación que le permitan a la Alta Dirección mantenerse informada de los riesgos y uso inadecuado de los activos de información y las acciones tomadas para su mitigación.
- Definir el Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad tomando marcos de referencia y buenas prácticas, así como los lineamientos corporativos emitidos en materia por Grupo Aval, que se adapten a los requisitos de la Organización
- Garantizar la continuidad de las operaciones de las áreas críticas de la organización definidas por la Alta Dirección que permitan el cumplimiento de acuerdos contractuales al presentarse interrupciones imprevistas.

3. ALCANCE

La política de Seguridad de la Información y Ciberseguridad aplica a miembros de Alta Dirección y funcionarios de Proindesa S.A.S. y sociedades administradas[1], en adelante "La Organización"; asimismo, se extenderá a los proveedores de la Organización que mantengan relación con el desarrollo del objeto del negocio, que en el ejercicio de sus funciones utilicen información y servicios tecnológicos o cuando la situación así lo amerite; deberán adoptarla de acuerdo con la naturaleza, tamaño complejidad y estructura de sus operaciones.,

4. GLOSARIO

- Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento que tenga valor para la organización y que se debe identificar, clasificar y proteger de acuerdo con su valor, criticidad y nivel de exposición.
- Alta Dirección: Asamblea de Accionistas, Junta Directiva, Representantes Legales, Presidente, Vicepresidentes
- Administración: Presidente, Vicepresidentes de Proindesa S.A.S y quienes hagan sus veces en las sociedades administradas.
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- Apetito de Riesgo: Nivel de riesgo que acepta la Organización. Corresponde a una ponderación de alto nivel frente a la cuantificación del riesgo que la Alta Dirección está dispuesta a aceptar en el logro de sus metas.
- Ciberespacio: Entorno complejo resultante de la interacción de personas, software y servicios en internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.
- Ciberamenaza o Amenaza cibernética: Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.
- Ciber riesgo o Riesgo cibernético: Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.
- Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

[1] Incluye a todas las sociedades (vehículos de inversión) con las cuales Proindesa a la fecha tenga suscrito del Acuerdo de colaboración.

- **Comunidad:** Son los usuarios de la información del negocio.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Políticas, procedimientos, prácticas y estructuras organizativas concebidas, que sirven como medida para mantener y gestionar los riesgos de ciberseguridad y seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Control Correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.
- **Control Detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control Preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad.
- **Estándares y Buenas Prácticas de seguridad de la información:** Conjunto de medidas implementadas para asegurar que la información de la entidad y aquella que se encuentre en su poder sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones del negocio (confidencialidad), que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (integridad), que esté disponible cuando sea requerida (disponibilidad) y que sólo sea utilizada para los propósitos con que fue obtenida (privacidad y reserva) y única y exclusivamente para fines del negocio.
- **Evaluación de Riesgos:** Proceso global de identificación, análisis y estimación de riesgos
- **Evento de ciberseguridad:** Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la Organización que son esenciales para el negocio.
- **Framework Ciberseguridad NIST:** Marco de políticas se seguridad informática para evaluar y mejorar capacidad de prevenir, detectar, y responder a los ataques cibernéticos.
- **Funcionario:** Trabajadores, incluyendo la Alta Dirección, estudiantes en práctica y aprendices de Proindesa S.A.S.
- **Identificación de riesgos:** Proceso para encontrar, enumerar y caracterizar los elementos del riesgo.
- **Impacto:** El costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información
- **Incidente de Incidente de Ciberseguridad:** Ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.
- **Incidente Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.
- Información o Información del Negocio: Es toda aquella que, sin importar su presentación, medio o formato, en el que sea creada o utilizada, sirve de soporte a las actividades de negocio y la toma de decisiones.
- Norma: Conjunto de reglas requeridas para implantar las políticas. Las normas hacen mención específica de tecnologías, metodologías, procedimientos de aplicación y otros factores involucrados y son de obligatorio cumplimiento.
- No repudio: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación.
- Organización de Seguridad de la Información: Estructura organizacional que soporta la Seguridad de la Información, donde se definen roles y responsabilidades de cada uno de sus integrantes.
- Perímetros o áreas seguras: Un área o agrupación dentro de la cual un conjunto definido de políticas de seguridad y medidas se aplica, para lograr un nivel específico de seguridad. Las áreas o zonas son utilizadas para agrupar activos de información con requisitos de seguridad y niveles de riesgo similares, para asegurar que cada zona se separa adecuadamente de las otras.
- Pilares de seguridad de la información: Son los principios fundamentales de Seguridad de la Información que permiten la gestión de riesgos asociados a la perdida de Confidencialidad, Integridad y Disponibilidad de los activos de información.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- Política: Es un conjunto de ordenamientos y lineamientos enmarcados, en los diferentes instrumentos jurídicos y administrativos que rigen una función, en este caso la Seguridad de la Información y la Ciberseguridad.
- Política de Seguridad de la Información y la Ciberseguridad: Documento donde se establecen las directrices y los lineamientos relacionados a la protección, manejo seguro de la información. como el desarrollo de capacidades empresariales para defender y anticipar de amenazas informáticas de los activos expuestos en Proindesa y sus sociedades administradas (vehículos de inversión e infraestructura vial).
- Privacidad: Propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla.
- Probabilidad de Ocurrencia: Es la posibilidad que un riesgo se materialice. Para determinar esta probabilidad se puede utilizar el análisis cualitativo o cuantitativo.
- Proceso de Evaluación de Administración de Riesgo: Proceso de identificación y análisis de riesgos relevantes existentes y que impiden el logro de los objetivos; formando una base para determinar cómo deben ser administrados, transferidos, controlados o asumido.
- Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.
- Responsable de la información: Es el colaborador para quien la información fue creada con el objetivo de realizar sus funciones en el negocio y que tiene la responsabilidad de administrarla, clasificarla y evaluar los riesgos que pueden afectarla. También es el primer responsable de implantar la Política de Seguridad de la Información y Ciberseguridad dentro de su área y para poder realizarlo debe conocer el valor de su información, los usuarios que deben tener acceso a ella y los privilegios que requieren para su uso.

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo emergente: Entiéndase por aquellos riesgos nuevos o no identificados que nunca han sido considerados previamente por la entidad, o riesgos conocidos que están evolucionando de manera inesperada, que puedan afectar no solo a una compañía sino a todo un sector o toda la economía.
- Riesgo Genérico: Son todos aquellos riesgos identificados por la segunda línea de Grupo Aval/Entidades
- Riesgo Inherente (RI): Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. En otras palabras, Riesgo Inherente es la probabilidad de que una Entidad pueda incurrir una pérdida material como resultado de su exposición a, y de la incertidumbre que surge de, potenciales eventos adversos futuros. Una pérdida material es una pérdida o combinación de pérdidas que puede dañar/deteriorar la condición financiera de una Entidad o Conglomerado, de manera que tenga la potencialidad de generar pérdidas para los depositantes, aseguradores e inversionistas. El RI es intrínseco a cada actividad significativa y se evalúa sin tener en consideración el tamaño de esta en relación con la organización y antes de evaluar la calidad de la administración de los riesgos que ésta realiza. Para identificar y evaluar los RI a los que está expuesta una organización es esencial tener un conocimiento profundo tanto de la naturaleza de las actividades que ésta realiza como del entorno en el que opera.
- Riesgo Residual: También conocido como riesgo neto, es el resultado de la mitigación de los riesgos inherentes por parte de la gestión operativa y las funciones de supervisión. En otras palabras, es el riesgo que permanece tras haberse ejecutado. los controles y se hayan tomado las medidas preventivas para dar respuesta a los riesgos identificados.
- Riesgo de seguridad de la información: Potencial para que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de una combinación de la probabilidad de que suceda un evento y sus consecuencias.
- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. También denominada el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.
- Sistema de gestión de seguridad de la información y ciberseguridad: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- Tecnología disruptiva: Es aquella que desplaza a una tecnología sostenida, basada en productos innovadores que crean una industria completamente nueva.
- Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.
- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. También denominada debilidad de un activo o control que puede ser explotado por una amenaza.

5. MARCOS DE REFERENCIA Y REGULACIÓN

- ISO/IEC 27701: Estándar que especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de privacidad de la información.
- NTC-ISO/IEC 27000: Tecnología de la información- Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información.
- NTC-ISO/IEC 27001-2013: Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI).
- NTC-ISO/IEC 27002-2013: Técnicas de seguridad Código de practica para controles de seguridad de la información.
- NTC-ISO/IEC 27005: Técnicas de seguridad. Gestión del riesgo en la seguridad de la información.
- 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 y la proveniente de terceros países y se dictan otras disposiciones.
- 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
- Ley SOX: Ley estadounidense emitida en 2002 que tiene como objetivo mejorar el ambiente de control interno de las empresas que cotizan en las bolsas de valores de los estados unidos; definir y formalizar responsabilidades sobre su cumplimiento para la prevención de errores contables y de reporte SEC (Securities and Exchange Commission - "SEC", por sus siglas en inglés): Organismo del Gobierno Federal de Estados Unidos que ejerce supervisión sobre los participantes clave en el mercado de valores y cuya misión es proteger a los inversionistas, mantener el mercado de valores ordenado, eficiente y protegido contra el fraude, mantener información relevante sobre el mismo y facilitar la creación de capitales.
- Framework de Ciberseguridad NIST: Marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo de ciberseguridad.

6. DECLARACIÓN DE COMPROMISO

La Organización está comprometida con la Política de Seguridad de la Información y Ciberseguridad, promoviendo una cultura de cumplimiento y control de acuerdo con los pilares establecidos por el sistema de gestión de seguridad de la información y ciberseguridad, por lo anterior debe:

- Prevenir los daños a la imagen y reputación a través de la adopción y cumplimiento de la Política de Seguridad de la Información y Ciberseguridad.
- Promover continuamente una cultura de seguridad de la información y ciberseguridad.
- Gestionar de manera estructurada y estratégica los riesgos de seguridad de la información y ciberseguridad 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 seguridad de la información y ciberseguridad; de igual forma son responsables de reportar los incidentes de los que pudiera a tener conocimiento a través de los canales de comunicación establecidos.

7. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La organización reconoce la importancia de proteger adecuadamente la información de amenazas que vulneren la continuidad del negocio, por lo anterior establece el desarrollo de actividades para la protección de los activos de información, gestión y administración de riesgos de seguridad de la información y ciberseguridad, protección de los datos personales, cultura de seguridad y las conductas que deben adoptar todos los miembros de la organización y terceros independientes que en el ejercicio de sus funciones utilicen información y servicios tecnológicos, preservando la confidencialidad, integridad, disponibilidad y privacidad de la información; por lo anterior, la organización deben velar por:

1. El cumplimiento de los requisitos y pilares de Seguridad de la Información y Ciberseguridad.
2. Proteger los activos de información y los activos tecnológicos de la Organización.
3. Administrar, gestionar y mitigar los riesgos asociados a seguridad de la información y ciberseguridad en los procesos de la Organización.
4. Establecer y divulgar las directrices, normas, políticas, estándares, procedimientos e instructivos de seguridad de la información y ciberseguridad, generando compromiso en todas las áreas de la organización.
5. Fortalecer la cultura de Seguridad de la Información de los funcionarios de Proindesa S.A.S. y proveedores, que administren activos de información de la Organización.
6. Garantizar los requisitos de seguridad de la información y ciberseguridad en el plan de continuidad del negocio frente a incidentes de Seguridad de la Información y Ciberseguridad
7. La Política de Seguridad de la Información y Ciberseguridad se debe preservar en el tiempo. Por lo anterior, es necesario efectuar una revisión anual o ante cambios estructurales que afecten a La Organización, para asegurar que esta cumple con el cambio de las necesidades de negocio.
8. Cualquier miembro de La Organización puede identificar la necesidad de modificar la política de seguridad de la información y ciberseguridad. Dichas inquietudes y sugerencias deben ser comunicadas a un Representante Legal, o al Especialista en Seguridad de la Información o a la Dirección de Riesgos de PROINDESA S.A.S.

Acorde con lo anterior, la organización acoge las siguientes políticas sobre las cuales se fundamenta y estructura el Sistema de Gestión de Seguridad de la Información (SGSI). Tales Políticas son expresiones de la Alta Dirección para una presentación y valoración justa y transparente de riesgos de Seguridad de la Información y Ciberseguridad. Lo anterior permite hacer una adecuada identificación de los controles que mitigan razonablemente los riesgos identificados:

7.1. Garantizar la 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 garantizar y 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[2], 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[3], o una app de antivirus, con el fin de garantizar 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). La Dirección de Riesgos o quien haga sus veces, en conjunto con la Vicepresidencia Financiera y Administrativa o quien haga sus veces en su ausencia 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 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).

No podrá negarse a la Organización la descarga o instalación de software o apps en los dispositivos propios frente a la evidencia de uso para fines Corporativos, así sea de manera ocasional, so pena de incumplir la presente Política.

7.2. Adoptar y mantener una sólida cultura de Seguridad de la Información y Ciberseguridad

Las tres líneas deben tomar la iniciativa en el establecimiento de una sólida cultura de Seguridad de la Información y Ciberseguridad donde:

- La primera línea debe ser ejemplo y replicador de una sólida cultura y conciencia en seguridad de la información y ciberseguridad, en el cumplimiento de políticas y procedimientos organizacionales definidos.

---

[2] Roles y Responsabilidades definidos en el *Procedimiento de Monitoreo de Seguridad de la Información P-0201.*

[3] Se descargará el MFA Authenticator de Microsoft, según el documento *Línea Base de Software Corporativo DG-0828* detallado en el numeral 6.1., cuyo propósito sea desarrollar la gestión operativa de accesos corporativos, promoviendo las buenas prácticas de seguridad a través de la autenticación multifactor.

- La segunda línea debe definir y ejecutar actividades de concienciación y cultura sobre las políticas y procedimientos organizacionales de seguridad de la información y ciberseguridad, 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 seguridad de la información y ciberseguridad.

7.3. Implementar y mantener un sistema de gestión integral de riesgos de Seguridad de la Información y Ciberseguridad

Todos los funcionarios de la Organización deberán utilizar un marco de control interno generalmente aceptado donde defina los elementos que se espera que estén presentes y funcionando en un sistema de control interno efectivo. Para el efecto se deberá alinear con los lineamientos corporativos del Grupo Aval contenidos en su Modelo Corporativo de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.

7.4. 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 Seguridad de la Información y Ciberseguridad del Grupo Aval para 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 Seguridad de la Información y Ciberseguridad.

7.5. Evaluación de riesgos de Seguridad de la Información y Ciberseguridad

La Organización debe contar con un proceso para identificar, evaluar, documentar, gestionar y mitigar los riesgos de Seguridad de la Información y Ciberseguridad. Este proceso se hace 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 de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad.

7.6. Supervisar la Administración del Sistema de Gestión de Seguridad de la Información y Ciberseguridad

La Alta Dirección y la segunda línea deben establecer, aprobar y revisar periódicamente el "Sistema de Gestión de Seguridad de la Información y Ciberseguridad", así mismo, debe supervisar la Administración para asegurarse de que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

7.7. Gestionar el cambio

La Alta Dirección y la segunda línea deben asegurar que haya un proceso de aprobación que evalué plenamente los riesgos de Seguridad de la Información y Ciberseguridad en todos los nuevos procesos, actividades, productos y sistemas críticos, así como que se identifiquen nuevas amenazas. Por ejemplo, cada vez que se realicen 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.

7.8. Realizar Seguimiento y Presentar Informes

La segunda línea de la Organización debe implementar un proceso para monitorear regularmente los perfiles de riesgo de Seguridad de la información y las exposiciones a pérdidas importantes. Adicionalmente debe realizar un diagnóstico 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 basados en directrices corporativas que apoyen su desarrollo.

7.9. Controlar y mitigar

La primera y segunda línea de la Organización deben tener un fuerte "ambiente de control", estructurado mediante políticas, procedimientos, estándares, sistemas, controles internos adecuados y la ponderada mitigación o compensación de los riesgos.

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).

7.10. Garantizar el sistema de Seguridad de la Información y Ciberseguridad en situaciones de contingencia

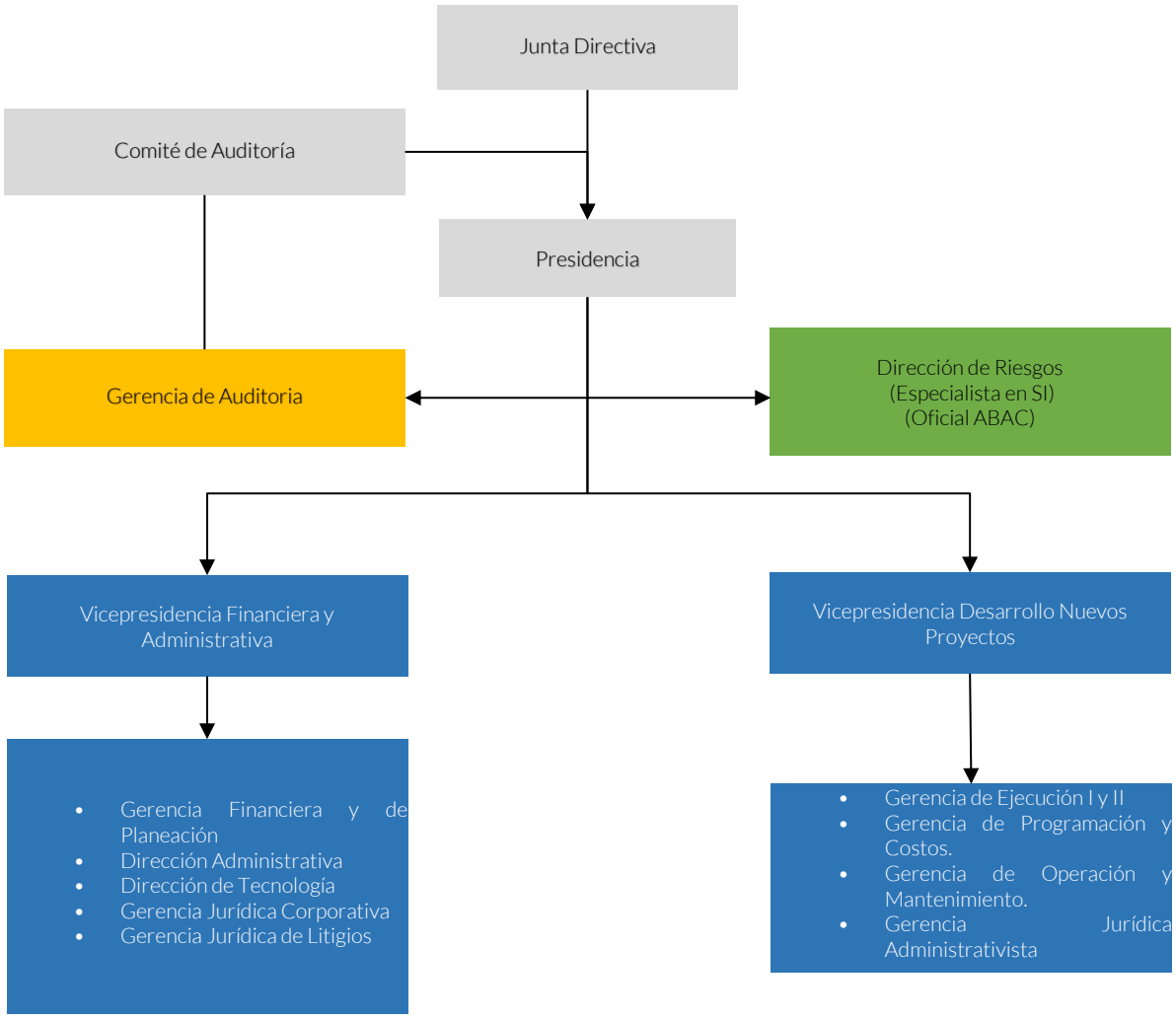
La segunda línea o el responsable de Seguridad de la información de la Organización, debe velar porque en los planes de continuidad del negocio se incluyan y garanticen los pilares de la Seguridad de la Información y Ciberseguridad.

7.11. 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.

8. GOBIERNO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Proindesa S.A.S., debe estructurar las funciones y responsabilidades frente al Riesgo de Seguridad de la Información y Ciberseguridad y frente a la gestión de todos los riesgos, este marco de referencia define el esquema de las tres líneas, considerando (i) la gestión por línea de negocio, (ii) una función de gestión de riesgo de Seguridad de la Información independiente, y (iii) una revisión independiente.



Convenciones Líneas:

Primera Línea | Segunda Línea | Tercera Línea

8.1. Primera Línea

La primera línea la constituyen los responsables de Seguridad Informática (Dirección de Tecnología) y todos los funcionarios de La Organización. La Política de Seguridad de la Información y Ciberseguridad reconoce a estos como responsables en primera medida de identificar, evaluar, gestionar, monitorear y reportar los riesgos e incidentes de seguridad de la información y ciberseguridad 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 Seguridad de la Información y Ciberseguridad.

8.2. Segunda Línea

Esta línea está conformada por la Dirección de Riesgos donde depende el área de seguridad de la información, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de todas las obligaciones de Riesgo en Seguridad de la Información y Ciberseguridad.

La Dirección de Riesgos, esta 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 Seguridad de la Información y Ciberseguridad. Para ello, debe estar plenamente familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios y los riesgos de Seguridad de la información derivados del negocio, incluyendo temas específicos de Ciberseguridad.

8.3. Tercera Línea

La tercera línea juega un papel importante al evaluar de forma independiente la gestión y los controles de los riesgos de la seguridad de la información y ciberseguridad, 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 o por personal independiente del proceso o sistema que se examina, pero también puede involucrar actores externos debidamente calificados.

9. ROLES Y RESPONSABILIDADES

Para dar cumplimiento a los objetivos de la Política de seguridad de la información y ciberseguridad, se han definido los siguientes actores clave en la Gestión de Seguridad de la información:

Actor	Actividades	
	De ejecución	De Supervisión
Comité Corporativo de seguridad de la información de Grupo Aval	• Proveer principios, directrices y lineamientos Corporativos de Seguridad de la información y Ciberseguridad, tomar las acciones preventivas y correctivas pertinentes para las Entidades del Grupo Aval. • Identificar, evaluar e incluir los requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las entidades. • Tomar decisiones relacionadas con la Seguridad de la información y Ciberseguridad 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 Seguridad de la Información y Ciberseguridad. • Definir requerimientos de Seguridad de la Información y Ciberseguridad 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 seguridad de la información y ciberseguridad en cada entidad
Comité Corporativo de Seguridad de la Información de Corficolombiana	• Proveer principios, directrices y lineamientos Corporativos de Seguridad de la Información y Ciberseguridad, tomar las acciones preventivas y correctivas pertinentes para las Entidades del Grupo Aval. • Identificar, evaluar e incluir los requerimientos de Seguridad de la Información y Ciberseguridad en las iniciativas corporativas realizadas para las entidades. • Tomar decisiones relacionadas con la Seguridad de la Información y Ciberseguridad 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 Seguridad de la Información y Ciberseguridad.	• Monitorear el cumplimiento a nivel corporativo de las políticas del Sistema de gestión de Seguridad de la Información y Ciberseguridad en cada entidad. • Monitorear el cumplimiento a nivel internos de las políticas del Sistema de gestión de Seguridad de la Información y Ciberseguridad en cada entidad.

Actor	Actividades	
	De ejecución	De Supervisión
	• Definir requerimientos de Seguridad de la Información y Ciberseguridad 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.	
Junta Directiva o quien haga sus veces	• Aprobar la Política de la Seguridad de la Información y Ciberseguridad 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 seguridad de la información y ciberseguridad. • Exigir el cumplimiento de las normas y regulaciones gubernamentales de seguridad de la información y ciberseguridad. • Participar en programas de concientización y capacitación en temas de Seguridad de la información y Ciberseguridad.	• Supervisar la seguridad de la información y ciberseguridad en la Organización, comprendiendo los riesgos y asegurando que estos sean gestionados.
Alta Dirección	• Evaluar el seguimiento del nivel de madurez y monitoreo de las políticas propuestas del Sistema de Gestión de Seguridad de la Información y Ciberseguridad. • Evaluar los informes que le presente la Dirección de Riesgos como responsable del área de Seguridad de la Información sobre los resultados de la evaluación de efectividad del programa de seguridad de la información y ciberseguridad, propuestas de mejora en materia de Ciberseguridad y resumen de los incidentes que afectaron a la Organización. • Promover la aplicación y apropiación de buenas prácticas de seguridad de la información y ciberseguridad. • Garantizar la evaluación de seguridad de la información y ciberseguridad de todos sus activos de información sin excepción. • Fortalecer la cultura de Seguridad de la Información de los funcionarios de La Organización, funcionarios temporales, proveedores y terceras partes, que administren activos de información de La Organización.	• Supervisar la seguridad de la información en la Organización, comprendiendo los riesgos y asegurando que estos sean gestionados.

Actor	Actividades	
	De ejecución	De Supervisión
Comité de Seguridad de la Información y Ciberseguridad	• Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de Proindesa y sus sociedades administradas. • Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información y ciberseguridad para los sistemas o servicios de Proindesa y sus sociedades administradas. • Promover la difusión, sensibilización y apoyo a la Seguridad de la Información y Ciberseguridad dentro de Proindesa y sus sociedades administradas. • Velar por la actualización continúa de la documentación del sistema de seguridad de la información • Velar porque que las actividades de control definidas frente a los riesgos de seguridad de la información y ciberseguridad identificados a la fecha, se tenga en cuenta en todos los proyectos de Tecnología de la Organización, desde su especificación inicial hasta su puesta en producción. • Validar y presentar oportunidades de mejora al Sistema de Gestión de seguridad de la Información. • Revisar los resultados obtenidos por la función de seguridad de la información.	• Monitorear la gestión realizada por medio de los reportes consolidados que le presente periódicamente la Dirección de Riesgos. 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 Especialista en Seguridad de la Información o el Director de Riesgos, escalaran el tema para validación por parte de los responsables en Corficolombiana como casa matriz de Proindesa y de las Sociedades Administradas. • Conocer los Incidentes de Seguridad de la Información y presentados en las entidades y que hayan tenido impacto significativo, reportados por Proindesa o las filiales directas de sus sociedades administradas, así como de los planes de acción definidos para la mitigación de estos.
Dirección de Riesgos	• Validar las directrices para el mejoramiento de la gestión de seguridad de la información y ciberseguridad, de acuerdo con el Modelo Corporativo de Seguridad de la Información y Ciberseguridad y las mejores prácticas en materia. • Preparar reportes de Seguridad de la Información y ciberseguridad para la Alta Dirección. • Definir los lineamientos de mejora en los procesos del Sistema de Gestión de Seguridad de la Información y ciberseguridad, en consenso con Corficolombiana. • Divulgar las instrucciones corporativas que, en materia, remita Corficolombiana y/o Grupo Aval, hacia las filiales de las sociedades administradas. Cumplir con las demás responsabilidades que sean definidas para la Alta Dirección.	• Monitorear el cumplimiento de reportes y de indicadores del sistema de gestión de seguridad de la información y ciberseguridad de Proindesa, las sociedades administradas y de las filiales de estas últimas. Mantener actualizados los lineamientos de Seguridad de la Información y ciberseguridad 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 Seguridad de la Información y Ciberseguridad de la Organización

Actor	Actividades	
	De ejecución	De Supervisión
Especialista en Seguridad de la Información o quien haga sus veces	• Preparar el informe de gestión definido por casa matriz, referente a la gestión de Riesgos de seguridad de la información y Ciberseguridad. • Participar el Comité de Seguridad de la Información y Ciberseguridad de la Organización. • Adoptar y socializar las mejores prácticas sugeridas en el Comité. • Propiciar la actualización del inventario de riesgos de Seguridad de la Información. y Ciberseguridad. • Mantener actualizada la matriz de riesgos de SI y Ciberseguridad 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 seguridad de la información y ciberseguridad • Mantener actualizados los lineamientos de Seguridad de la Información y Ciberseguridad de la Organización. • Capacitar periódicamente a los funcionarios de la Organización, con el fin de fortalecer la cultura de prevención de riesgos de Seguridad de la información y Ciberseguridad. • Recibir y consolidar información de Seguridad de la Información y Ciberseguridad de las filiales de las sociedades administras por Proindesa para generar reportes de monitoreo periódicos, de acuerdo con el protocolo de comunicaciones corporativo.	• Conocer los incidentes de Seguridad de la Información 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 Seguridad de Información y Ciberseguridad.

Actor	Actividades	
	De ejecución	De Supervisión
Responsables de Seguridad Informática (Dirección de Tecnología)	• Participar en el Comité de Seguridad de la Información y Ciberseguridad 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 Especialista en seguridad de la información. • Informar al Especialista en Seguridad de Información sobre nuevos riesgos identificados y de manera particular sobre nuevos riesgos de Ciberseguridad. • 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 TI y Ciberseguridad.	• Velar por que se adopten medidas para responder a los incidentes presentados y para prevenir futuros incidentes. • Adoptar las mejores prácticas vigentes en el mercado con respecto a la administración de infraestructura y apoyo en la respuesta a incidentes al especialista en seguridad de la información. • Apoyar la definición y medición de indicadores clave de desempeño sobre la gestión de seguridad informática y Ciberseguridad
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 y la Organización. • Conocer los riesgos de Seguridad de la Información que le son aplicables. • 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 seguridad de la información, cualquier incidente de seguridad de la información y de manera particular cualquier evento material de seguridad de la información o Ciberseguridad.	• Vigilar y velar que su equipo de trabajo dé cumplimiento a la Política de Seguridad y Ciberseguridad de la Organización.
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 Seguridad de la Información y Ciberseguridad.

10. SEGURIDAD EN NUEVAS TECNOLOGÍAS Y RIESGOS EMERGENTES

Es importante implementar un plan de seguridad de la información y ciberseguridad, con relación a los servicios de infraestructura de la Organización con el fin de integrar 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 debe:

- Establecer políticas de seguridad sobre las nuevas tecnologías que se implementen en la Organización.
- Adoptar procedimientos de clasificación de la información, gestión y administración de usuarios, definición de responsables y propietarios, de la información que se va a procesar en las nuevas tecnologías para determinar y aplicar los controles de seguridad de la información y ciberseguridad.
- Documentar los procedimientos de muestreo hasta la presentación de reportes, flujos de los procesos de automatización, codificación y pruebas de las nuevas tecnologías utilizadas por la organización.
- Establecer la gestión y monitoreo de los riesgos cibernéticos y riesgos de terceros que surgen de la implementación de las nuevas tecnologías como lo son los riesgos operacionales, financieros, regulatorios, organizacionales y tecnológicos.
- Incluir en el plan de continuidad del negocio los requisitos de seguridad para reanudar las operaciones orientadas en los sistemas automatizados y servicios digitales.
- Supervisar el cumplimiento del trabajo que desempeñan los sistemas automatizados, asegurando que estos sistemas se adhieran a los requerimientos regulatorios y a las políticas de la Organización.

11. MODELO DE EVALUACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Para la identificación de riesgos y la aplicación de controles de seguridad de la información y ciberseguridad, la Organización adopta y da a conocer el Modelo de Evaluación de Seguridad de la Información y Ciberseguridad emitido por Grupo Aval. Este modelo tiene como propósito evaluar el nivel de madurez del sistema de gestión de seguridad de la información y ciberseguridad e identificar las oportunidades de mejora que permitan fortalecerlo, basado en los dominios y controles propuestos en la norma NTC-ISO 27001:2013 y en el Framework de Ciberseguridad NIST.

12. 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 Seguridad de la Información Corporativo (Grupo Aval) emite Instrucción General a Presidentes, Líderes de Seguridad de la Información y cuando aplique Dueños de Proceso de los cuatro Bancos y Corficolombiana. 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 de Riesgos 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 Seguridad de la Información Corporativo emite Conceptos a los Líderes de Seguridad de la Información de los cuatro Bancos y Corficolombiana, así como filiales adicionales en casos especiales, y éstos a su vez divulgan los Conceptos a los Líderes de Seguridad de la Información 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.

13. 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 deberán informar a Corficolombiana, aquellos incidentes Seguridad de la Información y Ciberseguridad que hayan afectado de manera significativa la confidencialidad, integridad, disponibilidad y privacidad de la información de la sociedad en el momento en que estos sucedan, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlos.

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

14. CAPACITACIÓN Y ENTRENAMIENTO

Los funcionarios y terceros deben tener conocimiento de las políticas y procedimientos de seguridad de la información y ciberseguridad 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 la organización debe asistir durante el periodo de inducción, a una charla sobre los requerimientos de seguridad de la información y ciberseguridad de Proindesa y sus sociedades administradas.

Así mismo, anualmente para la totalidad de los funcionarios debe realizarse una capacitación y/o actualización sobre Seguridad de la Información y Ciberseguridad. 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 de Gestión de Seguridad de la Información y Ciberseguridad

15. INVESTIGACIÓN Y SANCIONES

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad con sus respectivas normas es de obligatorio cumplimiento para todos los funcionarios, de forma que cada funcionario debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en seguridad de la información y ciberseguridad, así como de la protección de los activos de información de Proindesa y sus sociedades administradas.

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 penales y pecuniarias establecidas en las leyes locales. Dicho proceso se realizará de acuerdo con las políticas internas de la Organización relacionadas con el manejo de faltas.

16. DOCUMENTOS Y REGISTROS REFERENCIADOS

- DG- 0202 Normas de Seguridad de la Información y Ciberseguridad

17. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	22/06/2017	Creación del documento
2	25/09/2020	Actualización general del documentos 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 de el diagrama del gobierno para la gestión de S.I.

18. FIRMAS DE REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:		Aprobado por:
Diego Alejandro Pinzón Acevedo Firmado digitalmente por Diego Alejandro Pinzón Acevedo Nombre de reconocimiento (DN): cn=Diego Alejandro Pinzón Acevedo, o=Proindesa, ou=Analista de Calidad II, email=diego.pinzon@proindesa.com.co, c=CO Fecha: 2023.11.30 09:59:24 -05'00'	Manuel Ricardo Parra Aguilar Firmado digitalmente por Manuel Ricardo Parra Aguilar Fecha: 2023.11.30 10:09:43 -05'00'	Jenny Alexandra Gomez Sarmiento Firmado digitalmente por Jenny Alexandra Gomez Sarmiento Fecha: 2023.12.01 11:08:18 -05'00'	Vanesa Garay Guzmán Firmado digitalmente por Vanesa Garay Guzmán Fecha: 2023.12.01 15:15:30 -05'00'
ANALISTA DE CALIDAD III	ESPECIALISTA EN SEGURIDAD DE LA INFORMACIÓN	DIRECTORA DE RIESGOS	VICEPRESIDENTE FINANCIERA Y ADMINISTRATIVA
Diego Alejandro Pinzón Acevedo	Manuel Ricardo Parra Aguilar	Jenny Alexandra Gómez Sarmiento	Vanessa Garay Guzmán

Documento aprobado en la sesión de Junta Directiva No.146 del 17 de Noviembre de 2023 .