POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ELABORÓ	ELABORÓ	REVISÓ	REVISÓ	-REVISÓ	APROBÓ
					Aprobado en Acta No. 118 del 15 febrero de 2024
Sonia Alonso Oficial de Seguridad de la Información	**John Guerrero Jefe TI**	**Esperanza Moreno Coordinador GRC**	**Diana Porras Gerente Financiero y Administrativo**	**Ricardo Postarini Gerente General**	**Junta Directiva**

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el presente documento se incluyen los aspectos que deben tenerse en cuenta por parte de todos los trabajadores para que la información 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 autorizadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad), que sea utilizada para los propósitos que fue obtenida (Privacidad) y que se deje el rastro de los eventos que ocurren al tener acceso a la información (Auditabilidad).

Por lo tanto, los trabajadores de la Concesionaria Vial Andina S.A.S. en adelante Coviandina S.A.S., deben actuar teniendo en cuenta los lineamientos consignados en este documento; la Alta Dirección de la Organización tiene un firme propósito de apoyar todas las actividades necesarias para alcanzar las metas y principios de seguridad de la información, de acuerdo con las responsabilidades asignadas dentro de la organización en relación con este tema.

2. OBJETIVO

2.1. OBJETIVO GENERAL

Establecer los lineamientos, controles y medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, a fin de proteger la seguridad de la información, los equipos y servicios tecnológicos que soportan los procesos de la Organización.

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.
- 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.
- 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.
- 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

Esta Política aplica para todos los niveles de la organización, incluyendo usuarios (que incluye trabajadores y accionistas), Clientes, Terceros (que incluye proveedores y contratistas), Entes de Control y Entidades relacionadas; que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación, así como los aspectos del entorno tecnológico de Coviandina (administración, operación y mantenimiento).

Por lo tanto, los trabajadores de Coviandina, actúan teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, que soportan la Política de Seguridad de la Información y ciberseguridad.

4. DEFINICIONES

- **Activo de Información:** Recurso considerado importante que contiene información sensible para el correcto funcionamiento de la organización.
- **Antivirus:** Sistema de seguridad informática de protección que se implementa en los computadores para proteger contra posibles ataques informáticos.
- **CASB**: (Cloud Access Security Broker) es un tipo de software que tiende a proteger las aplicaciones de las empresas para que los datos de la organización estén seguros.
- **Ciberseguridad:** Es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica.
- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta, sólo es accedida por personas o sistemas autorizados.
- **Correo electrónico corporativo:** Es el servicio de correo que le asigna la organización a cada colaborador para que lo utilice en el desarrollo de sus funciones.
- **Criptografía**: Técnica de protección de la información mediante el uso de códigos que permite que solo el destinatario del mensaje pueda leer y procesar, con el fin de mantener segura la información que se transmite en el mensaje**.**
- **Disponibilidad:** Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **DLP**: Data Loss Prevention, por sus siglas en ingles “Prevención de Perdida de Datos”, sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la red corporativa.
- **Doble factor de autenticación:** Medida de protección adicional utilizada para garantizar el acceso seguro, sistema que agrega un nivel adicional de seguridad donde se requiere que el usuario se identifique de dos maneras diferentes.
- **Email Security:** Herramienta de seguridad de la información que detecta amenazas basadas en el correo electrónico corporativo.

- **Incidente de seguridad de la información:** Un evento o serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Integridad:** Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Office 365:** Herramienta ofimática tipo empresarial de Microsoft que permite utilizar programas como Word, Excel, PowerPoint y otras herramientas como Teams, OneDrive, Outlook.
- **OneDrive:** Plataforma en la nube de Microsoft que permite guardar los archivos o documentos en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet.**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.**
- **Política:** Declaración de alto nivel que describe la posición de la Organización sobre un tema específico.
- **Privacidad:** Propiedad de la información que garantiza el uso adecuado de la misma, así esté legítimamente autorizado a manejarla**.**
- **Responsabilidad:** Obligación de la que una persona debe responder, comprometerse a cumplir las obligaciones que se derivan de una asignación de función o actividad.
- **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.
- **SAP:** Es un sistema informático, cuya sigla proviene del nombre alemán original de la empresa: Systemanalyse Programmentwicklung, que en español significa "Desarrollo de programas de sistemas de análisis".
- **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información sensible de la organización.
- **SharePoint:** Herramienta de Microsoft de almacenamiento en la nube que permite organizar y compartir información.
- **Software Operacional:** Programas y/o sistemas operativos utilizados para dar soporte a las actividades propias de los diferentes procesos de la organización, a nivel transaccional y de control.
- **TI:** Tecnología de la información, es un concepto genérico que se refiere a las tecnologías que facilitan el procesamiento de la información.
- **VPN:** Virtual Private Network (Red privada virtual) es una tecnología de red que permite establecer una conexión protegida a una red privada cuando se utiliza una red pública.
- **Vulnerabilidad:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas.
- **Wifi:** Tecnología que permite conectar diferentes equipos informáticos a través de una red inalámbrica de banda ancha.

5. EXCEPCIONES

Cualquier excepción relacionada con la habilitación de puertos USB y navegación a sitios no autorizados, deberá ser aprobada por los miembros del comité de seguridad de la información y ciberseguridad, previa solicitud realizada por parte del jefe del área, quien remitirá la solicitud mediante correo electrónico al oficial de seguridad de la información, indicando los usuarios excepcionados y la justificación pertinente. Una vez aprobada la solicitud por parte de los miembros del comité, el área de Tecnología de la Información procederá a implementar las excepciones en las IP de los equipos requeridos e informará tanto al área solicitante como a los miembros del comité la implementación de estas.

Cada vez que se reciba una solicitud de excepción, el oficial de seguridad de la información llevará el registro y control de las solicitudes de excepción .en el formato Excepciones de USB y navegación a internet FT-TEC-020.

6. MARCOS DE REFERENCIA Y REGULACION

- 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 27001-2022: 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. 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.
- 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 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.

7. 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 en la misma, 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.

Cada colaborador, contratista y/o proveedores, son responsables de aplicar los criterios definidos en esta política y por ajustar sus actuaciones de acuerdo con los lineamientos establecidos en seguridad de la información y ciberseguridad; de igual forma es responsable de reportar los incidentes de los que pudiera tener conocimiento a través de los canales de comunicación establecidos.

8. POLITICA DE SEGURIDAD DE LA INFORMACION 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 colaboradores de COVIANDINA S.A.S. y proveedores de la organización 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:

8.1. SEGURIDAD DE LA INFORMACIÓN

- La información de Coviandina S.A.S., sin importar su presentación, medio o formato, en el que sea creada o utilizada para el soporte a las actividades de negocio, se califica como información del negocio o activo de información.
- La Seguridad de la información del negocio es el conjunto de medidas de protección que toma Coviandina S.A.S., contra la divulgación, modificación, hurto o destrucción accidental o maliciosa de su información. Dichas medidas de protección se basan en el valor relativo de la información y el riesgo en que se pueda ver comprometida.
- Los dueños de la información son los responsables de asegurar que la información del negocio cuenta con la protección apropiada para así preservar la Confidencialidad, Integridad y Disponibilidad de la información.

- Coviandina S.A.S., cuenta en la estructura organizacional, con el responsable de seguridad de la información (Oficial de Seguridad de la Información), quien controla las medidas preventivas ante un evento o incidente de seguridad y ciberseguridad de la información que se presente.
- Coviandina S.A.S., cuenta con el cifrado y protección de discos duros de cada equipo, como se detalla en el procedimiento Encriptación y/o cifrado de discos duros PR-TEC-008.
- Coviandina cuenta con la implementación de herramientas de seguridad de la información a fin de proteger sistemas de información tales como correo electrónico, prevención de perdida de datos – DLP, protección de dispositivos (antivirus) y protección perimetral (firewall)
- La política de seguridad de la información es revisada y actualizada cada vez que se requiera, mínimo con una periodicidad anual, de acuerdo con las nuevas instrucciones o requerimientos de Coviandina S.A.S y/o la casa matriz.

8.2. RESPONSABLES DE LA INFORMACIÓN

- Coviandina S.A.S., utiliza información para realizar sus actividades. Esta se crea y se entrega a cada colaborador para que pueda desarrollar y cumplir sus respectivas metas dentro del marco del negocio.
- La información que Coviandina S.A.S., utilice para el desarrollo de sus objetivos de negocio tiene asignado un responsable, quien la utiliza en su área y es el encargado de su correcto uso. Así, él toma las decisiones que son requeridas para la protección de su información y determina quiénes son los usuarios y sus privilegios de uso mediante los lineamientos definidos en el instructivo Gestión de usuarios en los sistemas de información IN-TEC-010.

8.3. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

- Cada usuario de la información está enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de Coviandina S.A.S., y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información.
- Con base a la instrucción de seguridad de la información y ciberseguridad– Actualización metodología gestión del riesgo, emitida por el grupo Aval se tiene definido e implementado la matriz de riesgos de seguridad de la información, ciberseguridad y gestión tecnológica, la cual se actualiza según se requiera, teniendo en cuenta cambios e identificación de nuevos riesgos y controles, que puedan llegar a impactar la operatividad de Coviandina S.A.S.

8.4. CAPACITACIÓN Y CREACIÓN DE CULTURA EN SEGURIDAD DE LA INFORMACIÓN

- Coviandina S.A.S., capacita a los usuarios a través del plan de capacitación anual permitiendo asegurar que permanezca informados acerca de las responsabilidades en seguridad de la información y de las continuas amenazas que colocan en riesgo la información que maneja, además

se les comunica los procedimientos de seguridad de la información para realizar su función de trabajo.

- Las capacitaciones están enfocadas en cumplimiento a los siguientes lineamientos:

  - Campañas de concienciación sobre cumplimiento de políticas de seguridad de la información y ciberseguridad dirigidas a todos los trabajadores de Coviandina.

  - Charlas estructuradas sobre vulnerabilidades, riesgos en seguridad de la información y ciberseguridad dirigidas a los trabajadores que hacen parte de áreas importantes y sensibles a la operación de Coviandina.

8.5. SEGURIDAD EN EL PERSONAL

- Los trabajadores que ingresen a Coviandina S.A.S., cumplen con el proceso de PR-GTH-002 Inducción formación, capacitación y entrenamiento, quienes recibirán copia del documento PO-DIR-010 Política de seguridad de la Información y ciberseguridad para el conocimiento, dejando registro en el FT-DIR-006 Declaración de compromiso con las políticas organizacionales, por parte de Gestión Humana, lo cual se archiva en la hoja de vida de cada trabajador.
- Los contratos de los trabajadores, incluye cláusulas que indican las responsabilidades correspondientes para con la seguridad de la Información y el cumplimiento del código de conducta, haciéndole conocer las consecuencias en caso de no ser seguidas y cumplidas.
- Los trabajadores que realicen cambio de cargo al interior de Coviandina realizan entrega de la información al jefe o líder de área. La información está disponible y completa para ser entregada al nuevo trabajador que va a reemplazar el cargo.

8.6. TERCEROS QUE ACCEDEN A INFORMACIÓN DE COVIANDINA S.A.S., LOCAL O REMOTAMENTE

- El uso de la información de Coviandina S.A.S., por terceros, ya sea local o remotamente, es formalizada por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política.
- En los contratos u ordenes de servicio, se incluye la obligación de proteger la información de Coviandina S.A.S., los requisitos de seguridad para mitigar los riesgos sobre la información y las consecuencias a que estarían sujetos en caso de incumplirla, como también la cláusula de ciberseguridad establecida a nivel Corporativo.
- La transferencia, envió y recepción de información a terceros se realiza a través de mecanismos de comunicación seguros, como el correo corporativo y en el OneDrive

8.7. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL

- Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de Coviandina S.A.S., por tanto, la identidad de cada usuario de los recursos informáticos es establecida y autenticada de una manera única y no podrá ser compartida.
- Los usuarios de Coviandina S.A.S., una vez creados y asignadas sus autorizaciones en los sistemas de Información establecidos por Coviandina S.A.S., podrán acceder a la información mediante su usuario y clave de autenticación. Dependiendo del valor de la información y del nivel de riesgo.
- Coviandina S.A.S., definirá medios de autenticación apropiados, que no podrán ser compartidos (como la clave de acceso) y dichos medios de autenticación contienen información confidencial que no es revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas

8.8. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN

- Coviandina S.A.S. cuenta con mecanismos de control de acceso físico y lógico relacionados con seguridad y autenticación en los sistemas de información para asegurar que los activos de información se mantengan protegidos de una manera consistente con su valor para el negocio y con los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información.
- Los derechos de acceso no comprometen la segregación de tareas y responsabilidades. El acceso a la información de Coviandina S.A.S., es otorgado sólo a usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad. El acceso a los recursos de Coviandina S.A.S., es restringido en todos los casos, y se da específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.
- El área de TI implementa mecanismos de autenticación que eviten accesos no autorizados a redes inalámbricas. Para el caso de personal externo a la organización, se le otorgará una conexión por WIFI de invitados, que será gestionado por el área de tecnología con autorización del personal encargado.
- Para los trabajadores que cuentan con acceso remoto de trabajo en casa se deberá dar cumplimiento a los lineamientos establecidos en el Procedimiento habilitación trabajo en casa PR-SST-010.

8.8.1. Gestión de retiro de usuarios

En el momento que se termine la relación contractual del colaborador con la organización el área de TI elimina inmediatamente los permisos que fueron otorgados en los diferentes sistemas de información. Respecto a la información manejada por el usuario retirado se deberá el manejo correspondiente de acuerdo con los lineamientos establecidos en el Instructivo Gestión de usuarios en los sistemas de información – IN-TEC-010.

8.8.2. Ingreso seguro a los sistemas de información

- Para el ingreso seguro a los sistemas de información o plataformas como SAP y VPN - Coviandina S.A.S. lleva un control de seguimiento a través de logs de los ingresos exitosos y fallidos.
- Para el sistema de información WorkManager y la plataforma Office 365 el Oficial de seguridad de la información realiza monitoreo periódico sobre la gestión realizada por los usuarios administradores, para lo cual se emite un informe con los resultados obtenidos, remitido al jefe de TI y la Gerencia Financiera y Administrativa para su gestión. El área de TI implementa un mecanismo seguro que permita bloquear los equipos de cómputo con un tiempo de quince (15) minutos para que se active automáticamente, después del periodo de inactividad, de acuerdo con lo definido en el Instructivo Configuraciones básicas de TI y principios de seguridad de la información – IN-TEC-011.
- En los aplicativos utilizados en la organización, no se visualizan las contraseñas de ingreso de los usuarios.
- Las plataformas VPN y OFFICE 365, cuentan con un mecanismo alterno de doble factor de autenticación, con el objetivo de minimizar el riesgo de accesos no autorizados.

8.8.3. Sistema de gestión de contraseñas

La gestión de contraseñas para el ingreso a los sistemas de información de CVA se encuentra definida en el Instructivo Configuraciones básicas de TI y principios de seguridad de la información – IN-TEC-011.

8.8.4. Manejo de dispositivos

- Todos los dispositivos de almacenamiento externo se encuentran restringidos a través de la consola del antivirus Symantec Endpoint Protection.
- Cualquier excepción deberá ser aprobada por los miembros del comité de seguridad de la información, previa solicitud realizada por parte del jefe del área quien remitirá la solicitud mediante correo electrónico, indicando los usuarios excepcionados y la justificación pertinente.

8.9. CONTINUIDAD DEL NEGOCIO

Coviandina S.A.S. cuenta con la definición del plan de continuidad del negocio y de su componente recuperación tecnológica ante desastres, establecida en el documento l PL-TEC-001.

8.10. SEGURIDAD FÍSICA

El control de acceso físico a las instalaciones se realiza de forma segura a través del cumplimiento de los lineamientos establecidos en el documento IN-TEC-001 Control de acceso físico y lógico a Coviandina.

8.10.1. Protección de Equipos

- Los trabajadores y/o proveedores que tenga acceso a las instalaciones de Coviandina S.A.S. no pueden fumar y consumir algún tipo de alimento cerca de los equipos de cómputo.
- Los equipos de la organización, como servidores, equipos de comunicaciones, centros de cableado, UPS, aire acondicionado, telefonía, estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contenga o brinde información sensible, están protegidos y ubicados de forma adecuada.
- No es autorizado el acceso a los recursos tecnológicos de la organización en equipos diferentes a los asignados al colaborador.

8.10.2. Retiro y seguridad de equipos, medios de información

- Todos los trabajadores de Coviandina S.A.S. son responsables de velar por la seguridad de los equipos que se encuentran fuera de las instalaciones.
- Para los equipos portátiles se tiene especial cuidado, y no es permitido exponerlos a cualquier riesgo que pueda afectar la confidencialidad de la información y la integridad física del trabajador.
- En caso de pérdida o robo de un equipo de Coviandina S.A.S., se reporta de forma inmediata al jefe del área, para realizar los respectivos trámites internos y externos, como reconstruir la información a través del backup e interponer la denuncia ante las autoridades competentes.
- El retiro de equipos de cómputo, dispositivos de almacenamiento, software y medios magnéticos con información sensible de Coviandina S.A.S., se realiza por medio de los procedimientos establecidos por el área de tecnología.
- El trabajador que se retire de la empresa realiza entrega de su equipo de cómputo asignado y/o herramientas tecnológicas.
- La información que se encuentre en el perfil de office 365 del colaborador retirado, se dispondrá de acuerdo con los lineamientos establecidos en el Instructivo Gestión de usuarios en los sistemas de información – IN-TEC-010.

8.10.3. Bloqueo y cierre de sesión de trabajo

El bloqueo y cierre de sesión de trabajo se realiza de acuerdo con los lineamientos establecidos en el Instructivo Configuraciones básicas de TI y principios de seguridad de la información – IN-TEC-011.

8.10.4. Escritorio y pantalla limpia

Todos los equipos de cómputo usan papel tapiz y protector de pantalla corporativo, con un tiempo de quince (15) minutos para que se active automáticamente, después del periodo de inactividad, adicionalmente se deberá dar cumplimiento a las directrices establecidas en el Instructivo Configuraciones básicas de TI y principios de seguridad de la información – IN-TEC-011.

8.10.5. Dispositivos móviles

Los colaboradores que manejen información de la organización a través de dispositivos móviles son responsables de protegerla física y lógicamente con el fin de evitar el hurto, acceso o divulgación de información no autorizada conforme a lo citado en el procedimiento manejo de celulares corporativos PR-TEC-009

8.11. USO DE LOS RECURSOS INFORMÁTICOS DE LA EMPRESA

8.11.1. El uso de los recursos informáticos de la Organización deberá cumplir con los lineamientos establecidos en el Instructivo Control de acceso físico y lógico a Coviandina – IN-TEC-001 Uso Adecuado del Internet .

Los trabajadores realizan buen uso del internet, no accediendo a paginas desconocidas o con contenido indebido y así mismo cumpliendo con los protocolos de seguridad recomendados y lineamientos establecidos en el instructivo Configuraciones básicas de TI y principios básicos de seguridad de la información – IN-TEC-011.

8.12. SEGURIDAD DE LAS OPERACIONES

Con el objetivo de asegurar las operaciones del entorno tecnológico de Coviandina S.A.S., a fin de cumplir con las condiciones de seguridad requeridas para mantener la confidencialidad, disponibilidad e integridad de la información, la organización adelanta las actividades relacionadas a continuación.

8.12.1. Protección contra software malicioso

- La organización cuenta con herramientas de seguridad como antivirus, antispam, y otras aplicaciones como Email security, DLP, CASB y Symantec Endpoint Protection, las cuales brindan protección contra código malicioso, pishing, suplantación de identidad, con el fin de evitar la divulgación, modificación o pérdida de la información.
- Proporcionar los mecanismos para generar cultura de seguridad entre los trabajadores de la organización y terceros frente a posibles ataques de software malicioso.
- Asegurar que el software de antivirus, Antispam, y demás aplicaciones cuenten con licencias de uso requerido.
- En cada equipo de Coviandina S.A.S., se tiene configurado un perfil de usuario final y un perfil de administrador quien es el único que permite descargar e instalar software.

8.12.2. Copias de respaldo

La organización asegura que la información de los aplicativos y de las diferentes áreas de la empresa, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su

confidencialidad, integridad y disponibilidad, de acuerdo con las directrices establecidas en el Instructivo Realizar copias de respaldo de la información Backup IN-TEC-005.

8.12.3. Control del software operacional

El oficial de seguridad de la información semestralmente realiza seguimiento y control al software operacional instalado en los diferentes equipos de la entidad, dejando como evidencia la remisión de un informe de la validación realizada y remisión de este al jefe de TI y la Gerencia Financiera y Administrativa para su gestión. Los usuarios o trabajadores de Coviandina, no están autorizados para instalar ningún tipo de software o programa que no esté relacionado con las funciones y responsabilidades en el cargo. En caso de necesitar algún tipo de programa para ejercer sus funciones, este mismo es solicitado y autorizado al jefe de TI o quien haga sus veces.

En el formato FT-TEC-017 Inventario TI Software se encuentra la relación del software CORE del negocio.

8.13. AUDITABILIDAD DE LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

- El oficial de seguridad de la información define los eventos considerados como críticos (intentos de acceso fallido al sistema de información y borrado o alteración de la información) y los respectivos registros de seguridad de la información.
- Los incidentes de seguridad de la información se registran y monitorean en el formato de FT-TEC-007 Bitácora de eventos e incidentes de seguridad de la información.
- Los usuarios reportan al líder de seguridad de la información cualquier tipo de anomalía o incidente de seguridad que se presente.

8.14. ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

- Los usuarios que lo requieran pueden almacenar la información en carpetas compartidas para obtener una seguridad y respaldo de la información de acuerdo con los lineamientos establecidos en el Instructivo Realizar copias de respaldo de la información Backup IN-TEC-005.El envío y recepción de información que no pueda ser tramitada por correo electrónico corporativo, es emitida o compartida a través del OneDrive, tanto para personal interno y personal externo.
- No se puede realizar envío de software o compartir archivos utilitarios a través de la nube OneDrive.
- A través de la herramienta Email Security, se tiene configurado políticas de restricción y transferencia de información a correos externos no autorizados por Coviandina.
- Mediante la herramienta SharePoint, se tiene configurado políticas de seguridad para solo compartir y enviar información entre correos con dominio de Coviandina
- Se tiene restringido en la red de Coviandina páginas web que permitan enviar o transferir información de forma no segura entre trabajadores internos y externos.

8.15. GESTIÓN DE ACTIVOS

Con el fin de asegurar que los activos de información, de la organización cuenten con un propietario responsable y estos cumplan con el nivel de protección adecuado, Coviandina S.A.S., adelanta las siguientes actividades.

8.15.1. Inventario de activos de información

Los líderes de cada proceso son los propietarios de la información, quienes identifican los activos de información de las áreas a su cargo, con el fin de elaborar el inventario de activos de información y velar por mantenerlo actualizado con una periodicidad de seis (6) meses. El jefe de TI o quien haga sus veces, realizará seguimiento de la actualización.

El inventario de activos de información y su respectiva clasificación por cada proceso se administra en el formato FT-TEC-008 Activos de información, como responsables de la custodia.

8.15.2. Publicación y actualización de los activos de información

El inventario de activos de información es un documento clasificado como “Confidencial” y no tiene características que lo permitan modificar por los usuarios autorizados. Sólo tiene acceso de modificación a este documento el líder del proceso con previa autorización del jefe de TI o quien hagas sus veces.

Los activos de información se actualizan semestralmente por el líder de cada proceso relacionando la documentación física y lógica. Esta actualización se realiza en el formato FT-TEC-008 Activos de información y será remitida mediante correo electrónico al jefe de TI o quien haga sus veces para consolidación, control y seguimiento.

8.15.3. Uso aceptable de los activos de información

Los trabajadores no deben divulgar información pública, confidencial, reservada o datos sensibles de la entidad con personas no autorizadas o entes externos, a menos que se realice por un canal oficialmente establecido y con la aprobación previa del líder de proceso.

La información sólo podrá ser utilizada para los fines propios del negocio y su remisión se realiza por el canal que esté oficialmente establecido y con las autorizaciones respectivas.

La información de la entidad no podrá ser divulgada sin contar con los permisos correspondientes, además, ningún trabajador, contratista o consultor podrá extraer información inclusive después de finalizada su relación contractual con la compañía conforme al Principio de Confidencialidad contemplado en la Política para el tratamiento de datos personales (PO-DIR-008).

8.15.4. Devolución de los activos de información

El propietario y/o custodio del activo de información garantiza la devolución de este, una vez finalice el vínculo contractual con la entidad o se realice una modificación a las funciones asignadas de acuerdo con el perfil y al área/proceso en el cual se desempeñe.

8.15.5. Clasificación de los activos de información

Los activos de información se clasifican de acuerdo por su confidencialidad, disponibilidad e integridad:

- **Confidencialidad**

Para Coviandina la información que sea confidencial no deberá estar disponible ni ser revelada a personas, entidades o procesos no autorizados, la cual será determinada bajo los siguientes niveles:

INFORMACIÓN PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PUBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los trabajadores de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades

- **Disponibilidad**

Para Coviandina S.A.S., la información se encontrará disponible cuando sea accesible y utilizable por solicitud de una persona entidad o proceso autorizado, en el momento y en el formato que sea requerido, así como los recursos necesarios para su uso. Los niveles de clasificación para esta propiedad están sujeto a la no disponibilidad de la información teniendo en cuenta lo siguiente:

ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.

MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

- **Integridad**

Para Coviandina S.A.S., la integridad de la información se define de acuerdo con la exactitud y completitud de esta, permitiendo que sea precisa, coherente y completa desde su creación hasta su destrucción. Se clasificará bajo los siguientes niveles:

ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de imagen moderado a trabajadores de la entidad.
BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

8.15.6. Seguridad de los activos de información

Los activos de información de Coviandina S.A.S. cuentan con medidas y controles que permitan proteger la información contra diferentes amenazas que puedan afectar la integridad, confidencialidad y disponibilidad. La seguridad de los activos de información deben ser responsabilidad de los dueños o propietarios de la información que maneja cada proceso o área de la entidad.

8.15.7. Gestión de activos físicos

El área de Tecnología de la Información en la actividad de alistamiento, soporte, revisión y mantenimiento de los equipos de cómputo y comunicaciones existentes en Coviandina S.A.S, diligenciará el formato FT-TEC-001 Ficha Técnica Hoja de Vida Equipos de Cómputo donde se especifica para cada activo las características básicas, los diagnósticos y mantenimiento solicitados por los usuarios previa solicitud vía correo electrónico. el responsable de TI encargado de realizar las actividades de mantenimiento y soporte necesarias y autorizaciones pertinentes.

La actualización del diligenciamiento de la Ficha Técnica Hoja de Vida Equipos de Cómputo FT- TEC-001 de cada equipo, se realizará cada vez que sea requerido.

8.16. PREVENCION PARA LA FUGA DE INFORMACIÓN.

La Organización ha establecido los siguientes lineamientos para prevenir la fuga de información sensible:

- La gestión y administración de la información para el envío y/o recepción de información, debe realizarse a través de correo electrónico corporativo o por el SharePoint. Los puertos USB, deben estar bloqueados para los equipos de cómputo de los trabajadores de Coviandina S.A.S, para que no les permita el ingreso de memorias USB o cualquier dispositivo de almacenamiento externo.
- El oficial de seguridad de la información realizará un monitoreo semestral sobre la restricción total de los puertos USB en los equipos de cómputo de Coviandina, para lo cual remite informe con los resultados obtenidos al jefe de TI o quien haga sus veces y la Gerencia Administrativa y Financiera para su debida gestión.
- El almacenamiento de información en las carpetas compartidas por cada área se encuentra restringido para que no pueda acceder cualquier usuario. Cada usuario tiene acceso a su respectiva carpeta o información correspondiente al área en que se encuentra laborando.
- Existe configurada una regla o directriz en el SharePoint, que permite guardar y almacenar información de forma segura, para cada usuario. Esta información es almacenada en una carpeta del OneDrive por cada usuario, el cual tiene seguridad y restricción de acceso para los demás usuarios.
- Se tiene restringido el uso de correos personales en la red interna de Coviandina, para no permitir el almacenamiento de información sensible de la empresa, en los respectivos correos personales. Solo se tiene permitido el uso del correo corporativo asignado a cada trabajador para la gestión de sus labores.
- Coviandina S.A.S., tiene implementada la herramienta de seguridad DLP que filtra y valida la información enviada a través de los correos corporativos. El DLP tiene como finalidad prevenir la fuga de información confidencial compartida por medio del correo electrónico corporativo, así mismo se cuenta con la implementación de la herramienta de seguridad CASB cuya funcionalidad está orientada a prevenir la fuga de información confidencial alojada en la nube (OneDrive)

8.17. APROBACION DE LA POLITICA DE SEGURIDAD Y CIBERSEGURIDAD

En el momento de realizar algún tipo de cambio o actualización, la política deberá ser revisada y aprobada por el Comité de Seguridad de la Información y ciberseguridad, así como de la Gerencia General, para posterior presentación a la junta directiva para su aprobación.

8.18. ROLES Y RESPONSABILIDADES

Para dar cumplimiento a 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
Junta Directiva	• Aprobar la Política de Seguridad de la Información y Ciberseguridad
	• Velar porque se cuente con los recursos técnicos y humanos suficientes para gestionar adecuadamente la Seguridad de la Información y Ciberseguridad
	• Aprobar las actualizaciones de la Política de Seguridad de la Información cada vez que se requiera. • Exigir el cumplimiento de las normas y regulaciones gubernamentales de seguridad de la información y ciberseguridad.
Gerencia General	• Aprobar, apoyar y promover al interior de la Organización la política de Seguridad de la Información y Ciberseguridad
	• Evaluar el seguimiento del nivel de madurez en el Modelo de Seguridad de la Información e implementación de los controles asociados a la norma ISO 27001
	• Promover la aplicación y apropiación de buenas prácticas de Seguridad de la Información y Ciberseguridad
Gerente Financiera y Administrativa	• Aprobar las solicitudes de inversión y compra de herramientas tecnológicas perimetrales sugeridas por Grupo Aval
	• Proporcionar los medios necesarios para la normalización y funcionamiento de los aspectos contemplados en la política de Seguridad y Ciberseguridad de la Información • Participar en el comité de seguridad de la información de Coviandina S.A.S.
Comité de Seguridad de la Información y ciberseguridad	• Velar por el cumplimiento de los lineamientos establecidos en la Política de Seguridad de la Información y Ciberseguridad
	• Desarrollar estrategias que fortalezcan y aseguren el cumplimiento de los objetivos trazados para la Seguridad de la Información
	• Promover una cultura de Seguridad de la Información a través del apoyo a los programas de capacitación y sensibilización relacionados con Seguridad de la Información y Ciberseguridad
	• Apoyar los mecanismos de revisión, control, seguimiento, implementación y toma de decisiones para establecer acciones correctivas, preventivas o disciplinarias relacionadas con la Seguridad de la Información y que resulten de los procesos de investigación.
	• Aprobar las actualizaciones y cambios esenciales en la Política de Seguridad de la Información y los manuales o procedimientos, previos a la presentación de la Junta Directiva.
	• Acompañar e impulsar el desarrollo de los proyectos relacionados con Seguridad de la Información y Ciberseguridad
	• Revisar y aprobar las solicitudes de excepción de USB y navegación en internet a sitios no autorizados.

ACTOR	ACTIVIDADES
	• Actuar como organismo consultivo en casos e incidentes referentes a la Seguridad de la Información donde por su competencia y funciones no son de control o responsabilidad exclusiva del Oficial de Seguridad de la Información.
	• Colocar en conocimiento de la entidad los documentos y/o estrategias generadas al interior del comité de Seguridad de la Información y que impacten de manera transversal a toda la compañía
	• Apoyar la atención de requerimientos e investigaciones relacionadas con incidentes de Seguridad de la Información
	• Colocar en conocimiento de la junta directiva las situaciones relacionadas con posibles afectaciones críticas a los activos de Información y/o infraestructura tecnológica.
	• Asistir a las reuniones semestrales y a las sesiones extraordinarias convocadas por incidentes o novedades referentes a Seguridad de la Información
Coordinación de GRC	• 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. • Responsable de presentar los resultados de gestión directamente a la Gerencia General y estar familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios de Seguridad de la información y Ciberseguridad.
Oficial de Seguridad de la Información	• Identificar la aplicabilidad de buenas prácticas de Seguridad de la Información, de acuerdo con la situación de la Organización a fin de implementar controles y medidas preventivas para mitigar los riesgos relacionados con temas de ciberataques, pérdida de Información, fraude, secuestro de Información, etc.
	• Dar tratamiento y planes de respuesta a los incidentes de Seguridad de la Información y Ciberseguridad que se presenten en Coviandina S.A.S..
	• Adoptar los lineamientos establecidos por la Casa Matriz.
	• Actualizar la Política de Seguridad de la Información y Ciberseguridad cada vez que se requiera • Participar en el comité de seguridad de la información de Coviandina S.A.S.
Oficial de Protección de Datos Personales	• Apoyar el cumplimiento de los principios y compromisos contemplados en la política para la protección de datos personales (PO-DIR-010) y el manual para el debido tratamiento de datos personales (MA-JUR-001) • Participar en el comité de seguridad de la información de Coviandina S.A.S.
Jefe de Tecnología o	• Implementar a través de las herramientas tecnológicas e infraestructura de TI, las directrices a nivel de Seguridad de la Información con base a los controles y lineamientos establecidos.

ACTOR	ACTIVIDADES
quien haga sus veces	• Apoyar la actualización de la Política de Seguridad de la Información y Ciberseguridad.
	• Informar al Oficial de Seguridad de la Información sobre nuevos riesgos identificados de Seguridad de la Información y Ciberseguridad
	• Adoptar los lineamientos establecidos por la Casa Matriz.
	• Implementar y operar los controles de Seguridad de la Información y Ciberseguridad • Participar en el comité de seguridad de la información de Coviandina S.A.S.
Trabajadores de Coviandina S.A.S.	• Usuarios de la Información (colaboradores, contratistas y/o terceros que accedan a cualquier activo de Información de propiedad de Coviandina S.A.S.) responsables de cumplir con los lineamientos y directrices especificadas en la política de Seguridad y Ciberseguridad de la Información.
	• Reportar al Oficial de Seguridad de la Información y Coordinación de TI, cualquier incidente de Seguridad de la Información y Ciberseguridad.
Proveedores	• Cumplir con los acuerdos definidos contractualmente en la cláusula de Ciberseguridad.
	• Implementar políticas y procedimientos para gestionar los riesgos y amenazas de Seguridad de la Información y Ciberseguridad inherentes al servicio objeto de su negocio, incluyendo la adopción de estándares internacionalmente aceptados de conformidad con las líneas de negocio y servicios prestados
	• En caso de que el tercero subcontrates servicios de computación en la nube o algún otro servicio de computación pactados contractualmente cumple con las normas, políticas y requisitos en materia de Seguridad y Ciberseguridad
	• Reportar todos los incidentes que se presenten en su operación y que afecte la Información de Coviandina S.A.S. en un plazo no mayor a veinticuatro (24) horas contadas a partir de la fecha de ocurrencia del incidente

8.19. CONTROLES CRIPTOGRAFICOS

Coviandina cuenta con el mecanismo de cifrado de disco duro PGP de Symantec y BitLocker de Windows, de acuerdo con los lineamientos definidos en el Instructivo Herramientas para cifrado de discos- IN-TEC-009. Lo anterior, para dar protección a la información almacenada en los equipos portátiles. Este mecanismo se encuentra instalado en los equipos portátiles del área administrativa que hacen parte de la operación sensible y critica del negocio.

El oficial de seguridad de la información realiza monitoreo semestral del cifrado de discos duros, para lo cual remite un informe con los resultados obtenidos al jefe de TI y Gerencia Financiera y Administrativa para su debida gestión.

Adicionalmente, Coviandina S.A.S., cuenta con la administración de conexiones remotas de acuerdo con los lineamientos definidos en el Instructivo Gestión VPN- IN-TEC-012.

8.20. CONTROL DE ACCESO EN LA RED

Para conexión a la red local de Coviandina mediante WI-FI, el área de TI realiza la configuración, previa entrega del equipo al usuario final. Para los usuarios externos se cuenta con una red WI-FI de invitados, quienes deberán solicitar el acceso al área de TI, los cuales se encargarán de proceder con la conexión.

8.21. ROLES Y RESPONSABILIDADES DE CIBERSEGURIDAD DE TERCEROS

Los terceros como proveedores y clientes realizan o responden cualquier tipo de solicitud para atender el incidente de ciberseguridad que se presente:

- **Proveedor Antivirus:**
  - Realizar las respectivas actualizaciones de la consola de administración.
  - Atender y dar respuesta a requerimientos técnicos en caso de un incidente de ciberseguridad relacionado con virus.
- **Proveedor infraestructura y telecomunicaciones:**
  - Atender los requerimientos y solicitudes registradas en la herramienta Service Manager, relacionadas con el incidente de ciberseguridad.
- **Proveedor SAP:**
  - Dar respuesta a los requerimientos y solicitudes realizadas relacionadas con el incidente de ciberseguridad.
  - Cumplir con los requerimientos de seguridad de la información

8.22. SEGURIDAD EN GESTIÓN HUMANA

Para controlar la seguridad durante el desarrollo de las actividades del colaborador desde su ingreso, la organización realizará las siguientes actividades de control y seguimiento:

- Anualmente en el proceso de reinducción se evalúa el conocimiento PO-DIR-010 Política de seguridad de la Información y ciberseguridad, dando cumplimiento a lo establecido en el PR-GTH-002 Inducción, formación, capacitación y entrenamiento. Lo anterior para firmar los términos y condiciones que contienen responsabilidades referentes a seguridad de la información, las cuales incluyen la confidencialidad, la protección de los datos, la ética, el uso adecuado de las instalaciones y los equipos, entre otros.
- El oficial de seguridad de la información monitorea el cumplimiento de la PO-DIR-010 Política de seguridad de la Información y ciberseguridad establecida, en caso de algún incumplimiento por parte de algún trabajador de la entidad, será comunicado de forma inmediata al jefe inmediato y al responsable de Gestión humana para realizar el respectivo procedimiento para comprobación de faltas en cumplimiento del PO-DIR-001 Reglamento Interno de Trabajo.

8.23. GESTION DE ACCESOS EN LOS SISTEMAS DE INFORMACION

Con el fin de identificar que los usuarios que estén ingresando a los sistemas de información SAP y WorkManager sean los autorizados, semestralmente el Oficial de seguridad de la información y la Coordinación de TI emiten certificación sobre la revisión de roles según la matriz de accesos generada en las citadas plataformas. De igual forma, el oficial de seguridad de la información realiza validación trimestral sobre la actualización de los interlocutores válidos de SAP para lo cual emite certificación.
Para el seguimiento de las actividades de los usuarios administradores de Microsoft Office 365 y WorkManager, el oficial de seguridad de la información realiza monitoreo semestral de las mismas a través de reportes generados en la consola de administración, para lo cual mediante informe reporta los resultados obtenidos al jefe de TI y Gerencia Financiera y Administrativa para su gestión.

Adicionalmente, se realiza seguimiento y monitoreo semestral sobre las conexiones remotas mediante la VPN, a fin de validar que los usuarios que tienen asignada VPN se encuentren activos en la organización, dejando como evidencia un acta de validación suscrita por el Coordinador de TI y el Oficial de Seguridad de la Información, la cual es remitida al jefe de TI y Gerencia Financiera y Administrativa para su gestión.

8.24. REPORTES DE EVENTOS DE SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD

El oficial de seguridad de la información mensualmente comunica mediante correo electrónico campañas de aspectos relacionados con seguridad de la información y ciberseguridad a todos los trabajadores de la organización, con el objetivo de alertar y prevenir a los trabajadores de Coviandina S.A.S. de nuevas amenazas, a fin de evitar posibles engaños o manipulaciones.

En el evento que se presente la materialización de un incidente o vulnerabilidad de seguridad de la información y ciberseguridad donde se vea afectada la integridad, disponibilidad y confidencialidad de la información, y una vez gestionado el mismo como se detalla en el documento “Administración y gestión de incidentes de seguridad” PR-TEC-005 el oficial de seguridad de la información deberá reportar el incidente o vulnerabilidad al correo electrónico: contacto@colcert.gov.co registrando la información relacionada en la página web de COLCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), enlaces https://www.colcert.gov.co/800/w3-article-198656.html opción “Reportar Incidente” y https://www.colcert.gov.co/800/w3-article-198655.html opción “Denunciar Ciberdelitos”.

8.25. GESTIÓN DE CONTRASEÑAS SENSIBLES

Las contraseñas o claves de acceso a plataformas sensibles, tanto de infraestructura tecnológica como de sistemas de información, que son administradas por el personal del área de tecnología son almacenadas en la caja fuerte del director Contable en sobre sellado.

En el Procedimiento PR-TEC-007 se detalla las actividades para la custodia y manejo de las claves del administrador de las plataformas tecnológicas.

8.26. ADQUISICION Y LICENCIAMIENTO DEL SOFTWARE

El software que adquiere y mantiene Coviandina S.A.S. es de uso legal, el cual es adquirido bajo las directrices establecidas por la casa matriz. Estos programas hacen referencia al paquete ofimático, software de seguridad y sistemas de información que la compañía requiere para ejercer sus funciones y operaciones diarias. El licenciamiento es coordinado, administrado y gestionado por el jefe de TI o quien haga sus veces mediante revisiones semestrales con el fin de verificar que el software instalado se encuentre licenciado y autorizado para el uso de funciones y operaciones diarias de Coviandina S.A.S, dejando como soporte la actualización del inventario TI Software FT-TEC-017.

8.27. PROTECCION DE DATOS PERSONALES

Estas medidas de seguridad aplican para todo tipo de datos (públicos, semiprivados, privados y sensibles), de acuerdo con la definición establecida en la Ley estatutaria 1581 de 2012, que se encuentren en base de datos automatizadas o no automatizadas.

Los responsables delegados de las bases de datos (Administradores de las Bases de Datos), serán los encargados de asegurar el cumplimiento de los controles aplicables a las bases de datos automatizadas y no automatizadas, el área de GRC y la gerencia administrativa y financiera apoyara la implementación de los controles

8.27.1. Control de acceso

El personal de Coviandina S.A.S solamente accede aquellos datos y recursos, necesarios para el desarrollo de sus labores y sobre los cuales se encuentran autorizados por el responsable del tratamiento.

El área de tecnología se ocupa de una lista actualizada de usuarios, perfiles de usuarios y de los accesos autorizados para cada uno de ellos. En el caso de soportes informáticos puede consistir en la información de contraseñas y en el caso de documentos en la entrega de llaves o mecanismos de apertura donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos de la lista actualizada, corresponde de forma exclusiva al personal autorizado.

Cualquier personal ajeno a Coviandina, que de forma autorizada y legal tenga acceso a los recursos protegidos estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad del personal propio.

8.27.2. Archivos de documentos

Coviandina S.A.S., fija los criterios y procedimientos de actuación que se utilizan para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizan la conservación, localización y consulta de los documentos y hacen posible los derechos de consulta y reclamo de los Titulares.

Para los documentos que sean archivados se consideran, entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la compañía.

Los dispositivos de almacenamiento de documentos disponen de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso Coviandina S.A.S, adoptará las medidas necesarias para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de su medio de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de estos es custodiado para impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los medios de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible se encuentran en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas permanecen cerradas cuando no se precise el acceso a dichos documentos.

8.27.3. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado por los responsables del tratamiento, siguiendo los mecanismos y procedimientos definidos.
El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado; si se realiza por personas no autorizadas son reportados como un incidente de seguridad.

8.27.4. Copias de respaldo y recuperación de datos personales

Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos. La recuperación de los datos tiene como objetivo garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción.

Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello. Coviandina S.A.S., se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos diariamente.

Coviandina S.A.S., conserva una copia de respaldo de los datos y de los procedimientos de recuperación de estos, en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar cumple en todo caso con las mismas medidas de seguridad exigidas para los datos originales.

8.27.5. Medidas para el transporte, destrucción y reutilización de documentos y soportes

Coviandina S.A.S. validará la supresión de datos personales sólo en los casos en que sea procedente, suprimirlos o revocar la autorización otorgada para su tratamiento de no existir una relación contractual vigente o un cumplimiento legal que requiera el tratamiento del dato personal.

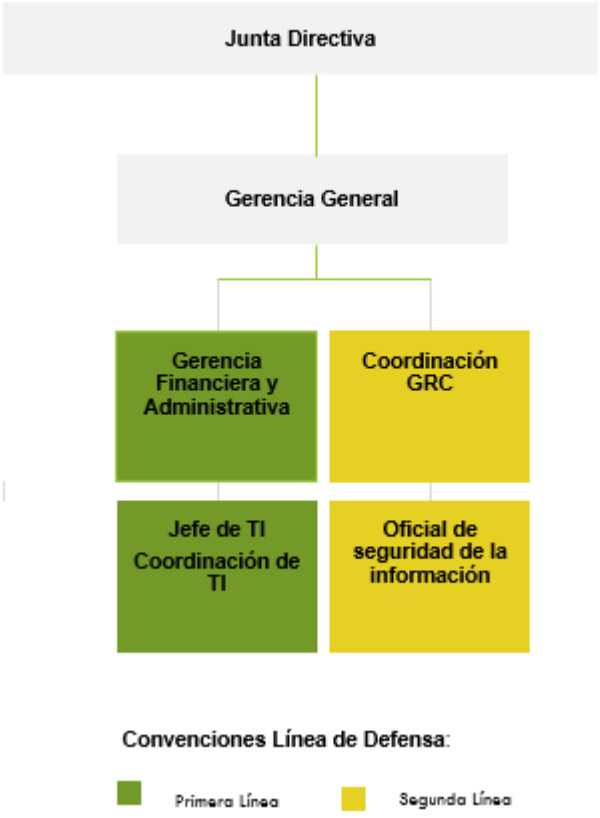
Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales se procede a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte. Cuando se lleve a cabo el traslado físico de documentos o soportes se adoptan las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma. Los datos contenidos en dispositivos portátiles son cifrados cuando se hallen fuera de las instalaciones que están bajo control de Coviandina S.A.S. Cuando no sea posible el cifrado, se evita el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos que puedan llegarse a presentar.

Las bases de datos identificadas con datos personales sensibles contienen los controles de seguridad necesarios para restringir el acceso a personal no autorizado y así mismo cumplir con los criterios de confidencialidad, integridad y disponibilidad.

8.28. ACTUALIZACION ANTIVIRUS Y SERVIDOR PRINCIPAL

Cada vez que el fabricante libere un nuevo parche o versión, el cual es informado mediante correo electrónico por el Proveedor al jefe de TI o quien haga sus veces se procede a programar la actividad técnica con el proveedor para realizar la actualización. Este procedimiento se realiza con el acompañamiento del área de TI, directamente en la plataforma de administración principal del antivirus. Una vez finalizada la actividad el proveedor remite a través de correo los soportes pertinentes al jefe de TI o quien haga sus veces, quien ratifica la ejecución de la misma, mediante la validación de la última versión instalada y desplegada en la consola. El oficial de seguridad de la información realizará monitoreo y seguimiento semestral sobre las actividades realizadas por el área de tecnología.

9. GOBIERNO PARA LA GESTION DE LA SEGURIDAD DE LA INFORMACION Y CIBERSEGURIDAD



- **Primera Línea**

La primera línea la constituye el área de TI 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.

- **Segunda Línea**

Esta línea está conformada por la Coordinación de GRC donde depende el oficial de seguridad de la información, la cual debe establecer los lineamientos en esta materia y realizar un seguimiento continuo al cumplimiento de los lineamientos establecidos de Seguridad de la Información y Ciberseguridad.

La Coordinación de GRC, como responsable debe presentar los resultados de gestión directamente a la Dirección General y estar familiarizado con las políticas y normas vigentes, sus requisitos legales y reglamentarios relacionados con Seguridad de la información y Ciberseguridad.

10. 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, Coviandina 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 27001:2022 y en el Framework de Ciberseguridad NIST.

11. 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.

12.REPORTES

Coviandina deberá informar a Proindesa, 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.

13.INVESTIGACIÓN Y SANCIONES

El cumplimiento de la Política de Seguridad de la Información y Ciberseguridad, con sus respectivas normas es de obligatorio cumplimiento para los trabajadores de Coviandina S.A.S. Cada integrante, entiende su rol, conoce y asume su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información de la organización.

Coviandina 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.

14.DOCUMENTOS DE REFERENCIA Y ANEXOS

- PO-DIR-008 Política para el Tratamiento de datos personales
- MA-JUR-001 Manual para el debido tratamiento de datos personales
- PL-TEC-001 Plan continuidad del negocio
- PR-GTH-002 Inducción formación, capacitación y entrenamiento
- PR-TEC-007 Custodia y manejo de claves del administrador de las plataformas tecnológicas
- FT-DIR-006 Declaración de compromiso con las políticas organizacionales
- FT-GTH-015 Evaluación de Inducción.
- FT-TEC-001 Ficha Técnica Hoja de Vida - Equipos De Cómputo y Comunicaciones
- FT-TEC-007 Bitácora de eventos e incidentes de seguridad de la información
- FT-TEC-008 Activos de información
- FT-TEC-017 Inventario TI Software
- IN-TEC-011 - Instructivo Configuraciones básicas de TI y principios de seguridad de la información.

- IN-TEC-012 Instructivo Gestión VPN.

15.CONTROL DE CAMBIOS

FECHA	VERSIÓN	NATURALEZA
25-May-2017	1	Creación del Documento
20-Feb-2020	2	Revisión general del documento
08-Jul-2020	3	Revisión y actualización del documento, relacionado con los puntos: 2.7; 2.9; 2.10; 2.11; 2.13; 2.14; 2.16; 2.17; 2.18
20-Ago-2020	4	Revisión y actualización del documento en el numeral 2.4, relacionado con la matriz de riesgos de seguridad de la información, ciberseguridad y gestión tecnológica,
08-Jun-2020	5	Revisión y actualización del documento, se incluye los numerales 2.19 Gestión de Activos y 2.20 Prevención para la Fuga de Información.
24-Jun-2021	6	Revisión y actualización del documento, se incluye los numerales 2.21. Revisión por la gerencia, 2.22. Roles y responsabilidades de seguridad de la información, 2.23. controles criptográficos y 2.25. Cumplimiento de políticas de seguridad de la información
05-Oct-2021	7	Revisión y actualización del documento se modificó el ítem 2.11.1 Seguridad física y 2.11.2. Retiro y seguridad de equipos, medios de información, se añadieron los siguientes ítems 2.19.6. Devolución de los activos de información, 2.23.1. Gestión de VPN, 2.24. Control de acceso en la red, 2.25. roles y responsabilidades de ciberseguridad de terceros y 2.28. protección de la información de registro.
10-may-2022	8	Revisión y actualización del documento, se incluye los numerales 2.19.6. Seguridad de los activos de información, 2.29. Reportes de eventos de seguridad de la información y ciberseguridad, 2.30. Gestión de contraseñas sensibles 2.31. Legalidad del software
13-sep-2022	9	Actualización del documento complementando el numeral 4.6 Seguridad en el personal, 4.11 Seguridad física, 4.25 Roles y responsabilidades de ciberseguridad de terceros ,4.31 Protección de datos personales, inclusión del numeral 4.19.7, Actualización inventario activos de información, inclusión del numeral 4.33 y 4.34
17-Ago-2023	10	Revisión y actualización general de la Política, contemplando las observaciones realizadas por la Contraloría de Corficolombiana. Se incluyen los numerales: 4. Excepciones, 5. Definiciones, 6. Marcos de referencia. Actualización del documento complementando los numerales 7.19.1 Inventario de activos de información, 7.11.2 Retiro y seguridad de equipos, medios de información, 7.21 Aprobación de la política, 7.22 Roles y responsabilidades, 7.27 Protección de la información de registros, 7.28 Reportes de eventos de seguridad de la información y ciberseguridad, 7.29 Gestión de contraseñas sensibles, 7.31 Protección de datos personales, 7.33 Monitoreo plataformas tecnológicas, 7.34 actualización antivirus y servidor Principal, entre otros.
15-Feb-2024	11	Revisión y actualización general de la Política, de acuerdo con la instrucción de seguridad de la información y ciberseguridad No. 29 del Grupo Aval.