POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ELABORÓ	ELABORÓ	REVISÓ	REVISÓ	APROBÓ	APROBÓ
					Aprobado en Acta No. 111 del 17 de Agosto de 2023
Sonia Alonso Oficial de Seguridad de la Información	Guillermo Bolaños Coordinador Tecnología de la Información	Esperanza Moreno Díaz Coordinador GRC	Diana Porras Gerente Financiero y Administrativo	Ricardo Postarini Herrera 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

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.

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. EXCEPCIONES

Cualquier excepción a alguno de los lineamientos de la presente política, deberá ser aprobada por el comité de seguridad de la información dejando como soporte acta de reunión y la divulgación a través de los correos electrónicos corporativos. Únicamente en los casos que estos consideren, será escalado el evento de excepción para aprobación por parte de la Dirección General.

5. 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.
- **Política:** Declaración de alto nivel que describe la posición de la Organización sobre un tema específico.
- **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.
- **System Encryption Desktop:** Es una herramienta de seguridad que utiliza criptografía para proteger sus datos contra el acceso no autorizado.
- **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.

6. MARCOS DE REFERENCIA

Coviandina S.A.S, en cumplimiento de las disposiciones de la casa Matriz y reglamentarias debe cumplir con las regulaciones de Seguridad de la Información vigentes y con regulaciones internacionales que se deban adoptar. Como mejores prácticas del mercado, son utilizados los siguientes marcos de referencia. Es de precisar que las practicas relacionadas a continuación no pretenden ser un listado taxativo.

- ISO/IEC 27000: Es un grupo de estándares internacionales. Tiene como fin ayudar a las organizaciones de todo tipo y tamaño a implementar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI).
- NTC-ISO-IEC 27001: Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, dentro del contexto de la organización. La presente norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicados a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.
- Framework de Ciberseguridad NIST: Marco de trabajo basado en estándares, directrices y prácticas existentes para que las organizaciones gestionen el riesgo de ciberseguridad.

7. GENERALIDADES

7.1. 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 responsables 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., dispone de los medios necesarios para asegurarse de que el trabajador preserve y proteja los activos de información de una manera consistente y confiable. Cualquier persona que intente inhabilitar, vencer, o sobrepasar cualquier control de seguridad será sujeto de las acciones disciplinarias correspondientes.
- 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, a través de las herramientas System Encryption Desktop con servicios PGP y Bitlocker de Windows.
- 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.

7.2. PROPIEDAD INTELECTUAL

- La Propiedad Intelectual se define como cualquier patente, derecho de autor, invención o información que es propiedad de Coviandina S.A.S.
- Todo el material que es desarrollado mientras se trabaja para Coviandina S.A.S., se considera que es de su propiedad intelectual y de uso exclusivo de la misma, por lo tanto, es protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de Coviandina S.A.S.

7.3. 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 responsable por 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.

7.4. 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.

7.5. 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:

    - Charlas 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.

7.6. 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.
- El Oficial de Seguridad de la Información realiza la inducción a los nuevos trabajadores, dejando como evidencia del conocimiento y entendimiento el diligenciamiento del formato FT-GTH-015 Evaluación de Inducción.
- 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.

7.7. 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.

7.8. 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.

7.9. 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 acceso a plataformas y aplicaciones es asignado de acuerdo con las políticas definidas, y teniendo en cuenta las funciones de los cargos en las diferentes áreas de la organización.
- La conexión remota al área local se realiza través de una conexión VPN segura suministrada por la organización, el cual debe ser aprobada y registrada.
- 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.

7.9.1. Gestión de accesos de usuarios

- La organización establece privilegios para el control de acceso, de cada usuario o grupo de usuarios, a los distintos aplicativos o sistemas de información. De igual forma se vela que los trabajadores y personal tengan acceso a información con base a las funciones o responsabilidades asignadas.
- Todo colaborador que requiera tener acceso a los sistemas de información de la entidad es autorizado para así mismo acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y autenticación (contraseña).
- Cada trabajador se hace responsable del uso y manejo de credenciales asignadas, evitando publicarlas o compartirlas.
- La creación, modificación y eliminación de usuarios, contraseñas y privilegios de acceso en infraestructura es responsabilidad del área de tecnología.
- En el momento que se termine la relación contractual o el contrato laboral con la organización o con el tercero, se inactiva inmediatamente los permisos que fueron otorgados en los diferentes sistemas de información, previa solicitud del jefe del área o quien haga sus veces, mediante correo electrónico.

7.9.2. Revisión de los derechos de acceso

Los derechos de acceso de los trabajadores a los diferentes aplicativos o sistemas de información de la organización, son revisados por cada jefe de área, una vez surtan cambios de cargo, promociones y/o ascensos, nuevos ingresos, o terminación de contrato.

7.9.3. Ingreso seguro a los sistemas de información

- Para el ingreso seguro a los sistemas de información o plataformas como SAP, WORKMANAGER, VPN y OFFICE 365, Coviandina S.A.S. lleva un control de seguimiento a través de logs de los ingresos exitosos y fallidos.
- La Coordinación 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.
- En los aplicativos utilizados en la organización, no se visualizan las contraseñas de ingreso de los usuarios.
- Los tiempos de conexión son restringidos para brindar seguridad a los diferentes aplicativos.
- 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.

7.9.4. Sistema de gestión de contraseñas

- La contraseña de los usuarios de los diferentes aplicativos o sistemas de información, cumplen con los parámetros mínimos de seguridad, tales como número mínimo de caracteres, uso de mayúsculas y minúsculas, caracteres alfanuméricos, uso de caracteres especiales, a fin de tener una contraseña fuerte y segura.
- Para el uso y administración de contraseñas, se tiene en cuenta los siguientes aspectos:
    - Que sean de fácil recordación

- No estar basadas en algo que otra persona pueda descifrar fácilmente como por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.
- Estar libres de caracteres numéricos o alfabéticos idénticos o consecutivos.

- Los sistemas de información o aplicativos exigen el cambio periódico de contraseñas a los usuarios con una parametrización y periodicidad máxima de 3 meses.

7.9.5. Manejo de dispositivos

- La información almacenada en cualquier medio removible (Unidades USB, Discos Duros portables, Tarjetas SD, CD, DVD, e incluso unidades de almacenamiento de Smartphone o Tabletas), es eliminada en el momento de ser entregada algún ente externo, con el fin de que no se pueda recuperar.
- El trabajador autorizado para el acceso y manejo de medios removibles protege la información que contiene los medios removibles.
- Los equipos de cómputo cuentan con acceso restringido para la extracción de información a través de medios removibles, memorias USB o cualquier dispositivo de almacenamiento externo.
- Los cargos autorizados como excepción a la política de restricción de puertos USB son: Gerente General, Gerente Financiera y Administrativa y cargos de operación técnica que tengan relación con trabajo de campo.
- El Oficial de Seguridad de la Información realiza un monitoreo al estado de los puertos y cifrado de discos duros con periodicidad semestral.

7.10. CONTINUIDAD DEL NEGOCIO

Coviandina S.A.S. cuenta con la definición del plan de continuidad del negocio en el PL-TEC-001.

7.11. SEGURIDAD FÍSICA

- Las áreas físicas construidas para soportar toda la operación del negocio están provistas de los controles de acceso adecuados (Ejemplo: puertas, cerraduras, lectores de tarjetas, registro de acceso biométrico, entre otros) según el valor de la información que contienen.
- Los recursos informáticos de Coviandina S.A.S., están físicamente protegidos contra amenazas de acceso no autorizado y amenazas ambientales para prevenir exposición, daño o pérdida de los activos e interrupción de las actividades de negocio.
- La información clasificada como confidencial o restringida no se dejará desatendida o sin control, por lo que Coviandina S.A.S., implementa las directrices de Escritorio Limpio y Pantalla Limpia.
- Para el acceso al centro de cómputo, Centros de Control de Operaciones (CCO), no se permite el uso de equipos fotográficos, de video, de audio, ni otro equipo de grabación como cámaras en dispositivos móviles, sin previa autorización.
- El acceso a las instalaciones físicas de Coviandina S.A.S., es en el horario laboral permitido, en caso contrario debe realizarse con previa autorización.

- 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.
- Se tiene definido controles de autenticación a través de sistema biométrico para el ingreso a lugares sensibles o críticos como el centro de cómputo y servidores.
- El acceso al centro de cómputo ubicado en la calle 26, se gestiona por el asistente administrativo y autorizado por el coordinador de TI.
- Si la pérdida del equipo o dispositivo involucra la perdida de bases de datos con información personal se realizará entrevista con el/los trabajadores comprometidos en el incidente de seguridad, en presencia del coordinador de tecnología, el oficial de protección de datos personales y el oficial de seguridad de la información.

7.11.1. 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.

7.11.2. 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, como poner 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, una vez el Coordinador TI o quien haga sus veces bloqueé la cuenta, la copia de la información queda almacenada en el Tenant de Office 365. De ser necesario su consulta, el jefe del área deberá solicitar acceso mediante correo electrónico al Coordinador TI o quien haga sus veces, para habilitar el acceso a dicha información.

7.11.3. Bloqueo y cierre de sesión de trabajo

- El usuario bloquea la sesión del equipo cuando se ausente de su puesto de trabajo.
- Es responsabilidad de todos los trabajadores cerrar las sesiones y dejar los equipos apagados cuando termine sus labores.

7.11.4. 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.
- Los trabajadores son responsables de la información bajo su custodia, manteniéndola segura bajo llave, en el momento de abandonar su puesto de trabajo.

7.11.5. 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.
- La utilización de los dispositivos móviles para el manejo de información de la organización, son autorizados por el líder o jefe de área.

7.12. CONECTIVIDAD

- Las conexiones a la red privada de Coviandina S.A.S., se realizan de manera segura para preservar la confidencialidad, integridad y disponibilidad de la información trasmitida sobre la red.
- Los colaboradores de la Organización, antes de acceder a la red privada de Coviandina S.A.S., deben conocer y dar cumplimiento a la presente Política. Esto aplica igualmente a las conexiones a través de la VPN.
- Se requiere la aprobación del Coordinador de TI o quien haga sus veces para poder acceder remotamente a la información de Coviandina S.A.S., y dichos accesos cumplen con la Identificación y Autenticación requerida.

7.13. USO DE LOS RECURSOS INFORMÁTICOS DE LA EMPRESA

- Los recursos informáticos de Coviandina S.A.S., son exclusivamente para propósitos del negocio y son tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Los colaboradores de la organización que intenten acceder a información a la que no cuentan con acceso autorizado están violando la presente Política.
- Coviandina S.A.S., se reserva el derecho de restringir el acceso a cualquier información en el momento que lo considere conveniente. Personal seleccionado por Coviandina S.A.S., podrá utilizar tecnología de uso restringido como la de monitoreo de red, datos operacionales y eventos en seguridad de la información. Ningún hardware o software no autorizados serán cargados, instalados o activados en los recursos informáticos, sin previa autorización formal del Coordinador TI o quien haga sus veces

- El uso del correo electrónico se realiza de forma adecuada por los trabajadores, y con fines netamente laborales.

7.14. 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.
- No acceder a sitios web a través de enlaces incluidos en mensajes de correo electrónico o en sitios web de terceros; usualmente la suplantación de identidades (Phishing) se vale de este medio para recolectar los datos de los usuarios y cometer fraude. La forma más segura de ingresar es digitando la dirección del sitio que se desea en el navegador de internet.
- El uso de YouTube, ChatGpt, redes sociales, Spotify, Google Play, RealPlayer, emisoras por internet, servicios de reloj por Internet, estado del tiempo, horóscopos, calendarios, protectores de pantalla o cualquier servicio que se actualice por Internet, consumen grandes cantidades de recursos de red (ancho de banda), ocupan la memoria y sobrecargan el procesador. Como consecuencia, el desempeño del computador y de la red corporativa serán lentos para todos los usuarios dificultando la tarea de quienes requieren los recursos de la red disponibles para el envío de mensajes importantes en el desempeño de sus labores y perjudicando en general a toda la organización.
- Se tiene configurado y establecido un firewall para no permitir el acceso a páginas web o sitios no autorizados para tener una navegación segura, tales como Yahoo, Hotmail, Gmail, WeTransfer, DropBox, entre otros. El Coordinador TI por medio de la plataforma Service Manager cada vez que se requiera, solicitará la inclusión o modificación de políticas o reglas al proveedor Claro quienes administran el Firewall. El Oficial de Seguridad de la Información semestralmente realizará seguimiento sobre las actividades realizadas por el área de tecnología, dejando como evidencia un informe de la validación realizada y remisión de este a la Coordinación de Tecnología y Gerencia Financiera y Administrativa

7.15. SEGURIDAD DE LA INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACIÓN DE SISTEMAS

- Actividades, normas y responsabilidades en seguridad de la información son incluidas dentro de cada uno los procesos de administración de sistemas de Coviandina S.A.S., para lograr el cumplimiento de la Política y las Normas de Seguridad de la Información.
- El Coordinador TI, crea y mantiene una metodología que controle el ciclo completo de implementación y mantenimiento de sistemas e infraestructura. Los requerimientos de seguridad de la información son identificados previos a la planeación e implementación de los sistemas de tecnología de la información.
- La implementación de un sistema nuevo o cambio significativo a los existentes es revisada por la Coordinación TI y el Oficial de Seguridad de la Información realizará seguimiento sobre las actividades realizadas por el área de tecnología.
- La realización de un cambio tecnológico que no considere los requerimientos de seguridad de la Información hace que Coviandina S.A.S., este expuesta a riesgos. Por lo tanto, cada cambio tecnológico deberá dar cumplimiento a los lineamientos establecidos en la Política de Seguridad y ciberseguridad de la Información.

7.16. 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.

7.16.1. Protección contra software malicioso

- La organización cuenta con herramientas de seguridad como antivirus, antispam, y otras aplicaciones las cuales brindan protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño permanente 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.

7.16.2. 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.
- La organización establece un plan de restauración de copias de seguridad que serán probadas a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo mínimo de 6 meses.
- Los medios magnéticos que contienen la información sensible son almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo contiene los mecanismos de seguridad adecuados.

7.16.3. Control del software operacional

- El oficial de seguridad de la información realiza seguimiento y control al software operacional instalado en los diferentes equipos de la entidad. 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 coordinador 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.

7.17. 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.

7.18. ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

- Los usuarios almacenan o guardan la información en las carpetas direccionadas para obtener una seguridad y respaldo de la información a través de un dispositivo de almacenamiento conectado a la red.
- 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 envió 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.
- A través de la herramienta SharePoint, se tiene configurado políticas de seguridad para solo permitir compartir y enviar información entre correos con dominio de Coviandina a nivel interno.
- 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.

7.19. 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.

7.19.1. 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. La Coordinación de Tecnología 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.
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 fechas de mantenimientos, 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.

Para la administración y custodia de la información en los discos duros de los equipos de cómputo en los diferentes procesos de Coviandina S.A.S. se utiliza la herramienta System Encryption Desktop con servicios PGP.

El control y manejo del cifrado de discos en los equipos de cómputo, es conformado con el número del inventario, seguido del nombre del usuario.
Ejemplo: 0001PPerez
No. Inventario del equipo: 0001
Nombre de Usuario: Pedro
Apellido: Pérez

A continuación, se relaciona captura de pantalla de la consola PGP.

Para la configuración de la herramienta se creó el correo pgp@coviandina.com con el fin de unificar el proceso de instalación y configuración en los equipos terminales.

La administración de la herramienta PGP es realizada mediante un servidor, con acceso del Coordinador de TI o quien haga sus veces.

7.19.2. Publicación

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 Coordinador de TI o quien hagas sus veces.

7.19.3. 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 el 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 o 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).

7.19.4. 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.

7.19.5. 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.

7.19.6. 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.

7.19.7. Actualización activos de información:

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 a la Coordinación de TI o quien haga sus veces para consolidación, control y seguimiento.

7.20. 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.
- En caso de que un trabajador requiera la utilización de un puerto para el ingreso de una memoria USB o cualquier medio de almacenamiento externo, por tema de algún caso urgente o de contingencia, se debe solicitar por medio de correo electrónico inicialmente al oficial de seguridad de la información para su aprobación y posteriormente se envía al coordinador de TI, para que realice la respectiva gestión.
- 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. En caso de identificar una inconsistencia, esta misma será comunicada al Coordinador TI, para su respectiva solución.
- 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, a los trabajadores 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 Cloud 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.
- Coviandina S.A.S., tiene implementada la herramienta de seguridad CASB CLOUD cuya funcionalidad está orientada a prevenir la fuga de información confidencial alojada en la nube (OneDrive)

7.21. APROBACION DE LA POLITICA

La política de seguridad de la información y ciberseguridad es revisada y aprobada por el Comité de Seguridad de la Información y ciberseguridad y Gerencia General, en el momento de realizar algún tipo de cambio o actualización, la cual es presentada ante la junta directiva para su conocimiento y aprobación.

7.22. 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.
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
	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

ACTOR	ACTIVIDADES
	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
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.
Coordinador de Tecnología	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.
	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

ACTOR	ACTIVIDADES
	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

7.23. CONTROLES CRIPTOGRAFICOS

Coviandina cuenta con el mecanismo de cifrado de disco duro PGP de Symantec y BitLocker de Windows, 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.

Gestión de VPN

Los usuarios utilizan la conexión VPN o licencia asignada para conectarse a través de trabajo remoto desde casa u otro sitio diferente al servidor y aplicaciones de la oficina principal. De igual forma se debe utilizar la VPN, para conexión interna en el momento que el usuario se encuentre en las oficinas principales de Coviandina.

La gestión y administración de las VPN, se realiza a través de la consola principal de administración, el cual tiene configurado unos parámetros de seguridad y son los siguientes:

- Solo permite conectar equipos con IP identificada y asociada a la consola.
- Permite conectar los equipos que tengan instalado el antivirus correspondiente con la última actualización.
- Permite conectar equipos que tenga sistema operativo Windows 10 y Windows 11.

7.24. CONTROL DE ACCESO EN LA RED

Para el ingreso a la red local de Coviandina por Wifi, el usuario solicita autorización al Coordinador de tecnología o quien haga sus veces, quien se autentica para el acceso a la red. Los usuarios invitados, de igual forma solicitan al coordinador de TI, la clave de ingreso para conectarse a la red Wifi de Coviandina.

7.25. 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 Claro:**
  - 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

7.26. SEGURIDAD EN GESTIÓN HUMANA

Para controlar la seguridad durante el desarrollo de las actividades del colaborador desde su ingreso, el oficial de seguridad de la información 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.

7.27. PROTECCION DE LA INFORMACION DE REGISTROS

- Se generan logs de registro y de accesos de los sistemas de información, para evaluar y verificar controles de acceso. Este monitoreo se debe realizar semestralmente con el fin de identificar que los usuarios que este ingresando a los sistemas de información, sean los autorizados. Para el caso de la plataforma SAP semestralmente se genera certificación sobre la revisión de roles según la matriz de accesos generada en SAP.
- Se monitorea y controla las actividades del administrador de las herramientas tecnológicas como Microsoft Office 365, a través de reportes generados de la consola de administración. Esta actividad se debe realizar trimestralmente por parte del oficial de seguridad de la información.
- Realizar seguimiento trimestral de la revisión de estados de la gestión y administración del acceso remoto mediante la VPN con el fin de verificar que los usuarios registrados de uso de VPN se encuentren activos dentro de la organización, dejando como evidencia un acta de validación suscrita por el Coordinador de TI y el Oficial de Seguridad de la Información.

7.28. 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 presentará 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”.

7.29. GESTIÓN DE CONTRASEÑAS SENSIBLES

Las contraseñas o claves de acceso a plataformas sensibles, como la herramienta Microsoft Office 365, VPN, OneDrive, SharePoint, antivirus, que son administradas principalmente por el personal de tecnología son guardadas 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.

7.30. LEGALIDAD DEL SOFTWARE

El software que adquiere y mantiene Coviandina S.A.S. es de uso legal, el cual es adquirido por medio de compras a empresas que certifican su respectivo licenciamiento. Estos programas hacen referencia a los paquetes ofimáticos, 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 coordinador de TI. Se llevan a cabo revisiones mensuales 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.

7.31. 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

7.31.1. 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.

7.31.2. 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 son custodiados 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.

7.31.3. 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.

7.31.4. 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.

7.31.5. 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.

7.32. ADQUISICION DE SOFTWARE:

- El software que adquiera Coviandina S.A.S., cumple como mínimo con los siguientes requerimientos de seguridad:

    - Este legalmente constituido y patentado por el desarrollador
    - El producto este debidamente licenciado
    - El software tenga un módulo adecuado de seguridad que permita gestionar la administración de usuarios, roles y permisos.
    - El software cuente con un sistema de copias de seguridad eficiente
    - El software cuente con un manual de usuario.

7.33. MONITOREO PLATAFORMAS TECNOLOGICAS

El oficial de seguridad de la información valida los controles de acceso a las plataformas tecnológicas críticas de Coviandina. Para el caso del sistema SAP, monitorea semestralmente que los usuarios retirados se encuentren inactivos en el sistema, emitiendo certificación sobre la revisión de roles según la matriz de accesos generada en SAP. De igual forma realiza una validación trimestral sobre la actualización de los interlocutores válidos de SAP para lo cual se emite certificación.

Para la plataforma tecnológica office 365 y el sistema de gestión documental Work Manager, realiza un monitoreo trimestral a través de logs de auditoría, de las actividades realizadas por el administrador de la plataforma y/o sistema de información, con el fin de verificar y analizar los registros de actividad de los usuarios administradores y consistencia de las actividades realizadas frente a los permisos y atribuciones asignadas a los administradores del sistema. El informe con los resultados obtenidos es presentado a la Gerencia Administrativa y Financiera y la Coordinación de Tecnología para su gestión.

7.34. ACTUALIZACION ANTIVIRUS Y SERVIDOR PRINCIPAL

Cada vez que el fabricante libere un nuevo parche o versión, el cual es informado mediante correo electrónico al Coordinador TI, quien realiza la actualización de los agentes del antivirus requiriendo la última versión suministrada por el proveedor. Este procedimiento se realiza directamente en la plataforma de administración principal del antivirus. De igual forma el coordinador TI realiza actualización de última versión del sistema operativo que maneja el servidor principal de Coviandina. El oficial de seguridad de la información realizará monitoreo y seguimiento sobre las actividades realizadas por el área de tecnología.

7.35. CUMPLIMIENTO Y MANEJO DE VIOLACIONES A LA POLÍTICA

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.

8. DOCUMENTOS DE REFERENCIA Y ANEXOS

- PO-DIR-008 Política para el Tratamiento de datos personales
- PO-DIR-001 Reglamento Interno de Trabajo.
- 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-GRC-004 Matriz De Continuidad De Negocio
- 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

9. 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.