POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ELABORÓ:	REVISÓ:	REVISÓ:	APROBÓ: Aprobado en Acta No. 95 del 10 de mayo de 2022
Christian Fajardo Caicedo Oficial de Seguridad de la información	Guillermo Bolaños Coordinador Tecnología de la Información	Ricardo Postarini Herrera Gerente General	Junta Directiva

1. INTRODUCCIÓN

El propósito de este documento es abordar las amenazas de seguridad e implementar estrategias para mitigar las vulnerabilidades de seguridad de IT, así como definir cómo recuperarse cuando se produce un incidente. Además, las políticas proporcionan pautas a los empleados sobre qué hacer y qué no hacer en caso de un evento.

Esta Política de Seguridad de la Información y ciberseguridad aplica para todos los niveles de la organización: Usuarios (que incluye empleados 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.

Por lo tanto, los trabajadores de la Concesionaria Vial Andina COVIANDINA S.A.S, deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, ya que éstos soportan la Política de Seguridad de la Información y ciberseguridad; en el entendido que la alta gerencia tiene el 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 los siguientes temas.

2. OBJETIVO

Definir los lineamientos, controles y dar a conocer a los trabajadores de COVIANDINA S.A.S, la Política de Seguridad de la Información y ciberseguridad establecida para la protección de la información.

3. ALCANCE

Esta Política de Seguridad de la Información y ciberseguridad aplica para todos los niveles de la organización: Usuarios (que incluye empleados 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.

Por lo tanto, los trabajadores de la Concesionaria Vial Andina COVIANDINA S.A.S, deben actuar teniendo en cuenta los lineamientos consignados en este documento y los que se desarrollen en las normas, estándares y procedimientos, ya que éstos soportan la Política de Seguridad de la Información y ciberseguridad; en el entendido que la alta gerencia tiene el 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 los temas relacionados en el documento.

4. GENERALIDADES

4.1. 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, Disponibilidad, Privacidad y Auditabilidad de la información.
- COVIANDINA S.A.S, debe disponer de los medios necesarios para asegurarse de que cada miembro de la Comunidad 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, debe contar con una estructura organizacional de seguridad de la información que permita gestionar y controlar lo dispuesto en el Modelo de Seguridad de la Información.
- COVIANDINA S.A.S, debe controlar la copia de información por medio de dispositivos USB, para ello COVIANDINA S.A.S tiene disponible el antivirus SYMANTEC ENDPOINT PROTECTION el cual permite el bloqueo y administración de los puertos USB.
- COVIANDINA S.A.S, debe controlar el bloqueo y protección de Discos Duros de cada equipo, para ello COVIANDINA S.A.S tiene disponible en la configuración del sistema operativo el aplicativo de cifrado de unidades BITLOCKER, el cual permite el bloqueo y cifrado de los Discos Duros de cada equipo de la empresa.
- La política de seguridad de la información debe ser actualizada por mínimo una vez en el semestre, de acuerdo con nuevas instrucciones o requerimientos en COVIANDINA S.A.S

4.2. 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, debe ser protegido contra un develado, descubrimiento o uso que menoscabe la competitividad de COVIANDINA S.A.S.

4.3. RESPONSABLES DE LA INFORMACIÓN.

- COVIANDINA S.A.S, utiliza información para realizar sus actividades. Esta se crea y se entrega a cada empleado 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 debe tener 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.

4.4. ADMINISTRACIÓN DEL RIESGO EN SEGURIDAD DE LA INFORMACIÓN

- Establecidos el nivel de riesgo y el valor de la información, cada responsable debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por COVIANDINA S.A.S.
- Cada usuario de la información debe estar 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 No 22 – 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 del grupo aval. (F2-M-AR-SI Matriz Riesgos Control SI y CI Riesgo CV), el cual se debe actualizar semestralmente teniendo en cuenta cambios e identificación de nuevos riesgos y controles, que puedan llegar a impactar la operatividad de COVIANDINA S.A.S.

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

- COVIANDINA S.A.S, capacita a los usuarios y terceros (Contratistas y Proveedores), 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.
- Los trabajadores y proveedores y Contratista deben estar enterados de los procedimientos de seguridad de la información que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo.
- Las capacitaciones están enfocadas en cumplimiento a los siguientes lineamientos:

  - ✓ Charlas de concientización 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.

4.6. SEGURIDAD EN EL PERSONAL

- Los empleados que ingresen a COVIANDINA S.A.S, deben cumplir 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 diligenciando del formato FT-GTH-015 Evaluación de Inducción.
- Los contratos de los empleados deben incluir cláusulas que indiquen 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.

4.7. TERCEROS QUE ACCEDEN 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, debe ser formalizado por medio de acuerdos y/o cláusulas que hagan obligatorio el cumplimiento de la presente Política.
- En los contratos se debe incluir 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.
- La transferencia, envió y recepción de información a terceros debe ser realizada a través de mecanismos de comunicación seguros.

4.8. IDENTIFICACIÓN Y AUTENTICACIÓN INDIVIDUAL

- Cada usuario es responsable por sus acciones mientras usa cualquier recurso de información de COVIANDINA S.A.S., Por lo tanto, la identidad de cada usuario de los recursos informáticos deberá ser 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 SAS, 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 debe ser revelada o almacenada en lugares que puedan ser accedidos por personas no autorizadas.

4.9. CONTROL Y ADMINISTRACIÓN DEL ACCESO A LA INFORMACIÓN

- Se deben establecer mecanismos de control de acceso físico y lógico 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, Disponibilidad, Privacidad y Auditabilidad de la información.
- Los derechos de acceso no deben comprometer la segregación de tareas y responsabilidades. El acceso a la información de COVIANDINA S.A.S, deberá ser 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, debe ser restringido en todos los casos, y se debe dar específicamente bajo las premisas de necesidad de conocer y menor privilegio posible.
- El acceso a plataformas y aplicaciones debe ser asignado de acuerdo con las políticas definidas, y teniendo en cuenta las funciones de los cargos en las diferentes áreas de la organización.
- **VPN:** La conexión remota al área local debe realizarse a través de una conexión VPN segura suministrada por la organización, el cual debe ser aprobada y registrada.

- **Redes inalámbricas:** El área de tecnología debe implementar mecanismos de autenticación que eviten accesos no autorizados. Para el caso de personal externo a la organización, se le otorgará una conexión por WIFI de invitados, que se será gestionado por el área de tecnología con autorización del personal encargado.

4.9.1. Gestión de accesos de usuarios

- La organización establecerá 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 velará que los trabajadores y personal tengan acceso a información con base a las funciones o responsabilidades asignadas.
- Todo trabajador que requiera tener acceso a los sistemas de información de la entidad debe ser autorizado y así mismo acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (contraseña).
- Cada trabajador debe hacerse 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 el contrato laboral, el trabajador de la entidad o tercero, se debe inactivar o retirar inmediatamente los permisos que fueron otorgados en los diferentes sistemas de información.

4.9.2. Revisión de los derechos de acceso

Los derechos de acceso, de los trabajadores a los diferentes aplicativos o sistemas de información, se deben revisar después de cada cambio, promoción, cambio de cargo o terminación de contrato.

4.9.3. Procedimiento de ingreso seguro

- Para el ingreso seguro a los sistemas de información o aplicativos, la entidad debe llevar un control de registro a través de un log de los ingresos exitosos y fallidos.
- Se debe implementar un mecanismo seguro que permita bloquear los equipos de cómputo en cierto periodo de inactividad.
- En los aplicativos, no se debe visualizar las contraseñas de ingreso de los usuarios.
- Los tiempos de conexión deben ser restringidos para brindar seguridad a los diferentes aplicativos.
- Los sistemas de información o plataformas principales como SAP, 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.

4.9.4. Sistema de gestión de contraseñas

- La contraseña de los usuarios de los diferentes aplicativos o sistemas de información, deben cumplir con los parámetros mínimos de seguridad como número mínimo de caracteres, uso de mayúsculas y minúsculas, uso de caracteres especiales, entre otros) para tener una contraseña fuerte y segura.
- Para el uso y administración de contraseñas, se debe tener en cuenta los siguientes aspectos:

    - ✓ Que sean fáciles de recordar

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

- Los sistemas de información o aplicativos deben exigir el cambio periódico de contraseñas a los usuarios.

4.9.5. Manejo de medios

- La información almacenada en cualquier medio removible debe ser 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 debe proteger la información que contiene los medios removibles.
- Los medios removibles que estén a punto de perder su funcionalidad, se debe realizar una copia de seguridad para evitar la pérdida de información.
- Los equipos de cómputo no deben contar con el acceso o el permiso para el ingreso de 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.

4.10. CONTINUIDAD DEL NEGOCIO

La información debe estar disponible para su uso autorizado cuando COVIANDINA S.A.S., la requiera en la ejecución de sus tareas regulares. Por lo que se deben desarrollar, documentar, implementar y probar periódicamente procedimientos para asegurar una recuperación razonable y a tiempo de la información crítica de COVIANDINA S.A.S, sin disminuir los niveles de seguridad establecidos. Esto debe ser independiente tanto del medio tecnológico que utilice COVIANDINA S.A.S., como de la posibilidad de que la información se dañe, se destruya o no esté disponible por un lapso.

La entidad tiene definido a través de sus procedimientos documentados las actividades a desarrollar para la activación del plan de continuidad del negocio, las cuales deben ser desarrollado como mínimo una (1) vez al año.

La organización cuenta con una estructura adecuada sobre un centro alterno de operaciones, el cual tiene como funcionalidad preparar, mitigar y responder ante un evento que requiera la activación del plan de continuidad del negocio.

4.11. SEGURIDAD FÍSICA

- Las áreas físicas construidas para soportar toda la operación del negocio deberán estar provistas de los controles adecuados (por ejemplo: puertas, cerraduras, lectores de tarjetas, biométricos, entre otros) según el valor de la información que contienen.

- Los recursos informáticos de COVIANDINA S.A.S, deben estar 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, desarrollará un programa que permita prevenir que la información crítica del negocio sea accedida sin autorización, dentro de lo cual está comprendido la implantación y cumplimiento de las directrices de Escritorio Limpio y Pantalla Limpia.
- El acceso al centro de cómputo y a las oficinas principales no se permite el uso de equipos fotográficos, de video, de audio, ni otro equipo de grabación como cámaras en dispositivos móviles, a menos que esté autorizado.
- El acceso a las instalaciones físicas de COVIANDINA S.A.S debe ser en horario laboral permitido, en caso contrario debe realizarse con previa autorización.
- El control de acceso físico a las instalaciones se debe realizar 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.

4.11.1. Protección de Equipos

- Los trabajadores y/o proveedores que tenga acceso a las instalaciones de COVIANDINA S.A.S no puede fumar y consumir algún tipo de alimento cerca de los equipos de cómputo.
- Los equipos de la entidad, como servidores, equipos de comunicaciones, centros de cableado, UPS, aire acondicionado, planta telefónica, estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contenga o brinde información sensible deben estar protegidos y ubicados de forma adecuada.
- No se debe realizar uso de un PC diferente al asignado al trabajador, el cual se puede realizar en casos importantes que requiera la operación de la organización.

4.11.2. 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.
- Los equipos portátiles deben tener especial cuidado, y no 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 debe 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, deben seguir con los procedimientos establecidos por el área de tecnología.
- El trabajador que se retire de la empresa debe realizar entrega de su equipo de cómputo asignado y/o herramientas tecnológicas.
- La información que se encuentre en el equipo de cómputo del trabajador retirado debe ser removida o trasladada al servidor principal en la nube donde se están realizando las copias de seguridad.

4.11.3. Equipo de usuario sin atención

- El usuario en su equipo de cómputo asignado debe bloquear la sesión en el momento que deje de realizar funciones sobre él o realice cualquier cese de actividades.
- Es responsabilidad de todos los trabajadores cerras las sesiones y dejas los equipos apagados cuando termine sus labores.

4.11.4. Escritorio y pantalla limpia

- Todos los equipos de cómputo deben usar papel tapiz y protector de pantalla corporativo, con un tiempo de cinco (5) minutos para que se active automáticamente, después del periodo de inactividad.
- Los trabajadores deben ser responsables de la información bajo su custodia, manteniéndola segura bajo llave, en el momento de abandonar su puesto de trabajo o se deje desatendido.

4.11.5. Dispositivos móviles

- Los trabajadores que manejen información de la entidad a través de dispositivos móviles deberán 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 entidad, deben estar autorizados por el líder o jefe de área.

4.12. CONECTIVIDAD

- Las conexiones a la red privada de COVIANDINA S.A.S, deben realizarse de una manera segura para preservar la confidencialidad, integridad, disponibilidad y privacidad de la información trasmitida sobre la red. Igualmente, todos los accesos de salida a otras empresas deben realizarse sobre redes aprobadas por COVIANDINA S.A.S.
- Los miembros de la Comunidad que se conecten a la red privada deben cumplir con la presente Política antes de que se realice la misma. Esto aplica igualmente a cualquier conexión actual o futura en la red de COVIANDINA S.A.S, que utilice medios públicos para integrar lugares que estén geográficamente dispersos.
- Se requiere la aprobación del responsable de la Información para poder acceder remotamente a la información de COVIANDINA S.A.S, y dichos accesos deben cumplir con la Identificación y Autenticación requerida.

4.13. USO DE LOS RECURSOS INFORMÁTICOS DE LA EMPRESA

- Los recursos informáticos de COVIANDINA S.A.S, son exclusivamente para propósitos del negocio y deben ser tratados como activos dedicados a proveer las herramientas para realizar el trabajo requerido. Miembros de la Comunidad que intenten acceder a información para la que no tienen un requerimiento autorizado de negocio, 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 responsable de Seguridad de la Información.
- El uso del correo electrónico debe ser realizado de forma adecuada por los trabajadores, y con fines netamente laborales.

4.14. USO ADECUADO DEL INTERNET

- Los trabajadores deben realizar buen uso del internet, no accediendo a paginas desconocidas o con contenido pornográfico y así mismo cumpliendo con los protocolos de seguridad recomendados.
- No acceda 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 (es decir escribiendo www.sitio_que_quiero_visitar.com
- El uso de YouTube, grooveshak, 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 empresa.
- Se tiene configurado y establecido un firewall para no permitir el acceso a páginas web o sitios no autorizados para tener una navegación segura como Yahoo, Hotmail, Gmail, WeTransfer, DropBox, entre otros.

4.15. SEGURIDAD DE INFORMACIÓN EN LOS PROCESOS DE ADMINISTRACIÓN DE SISTEMAS

- Actividades, normas y responsabilidades en seguridad de la información deben ser 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.
- La Dirección de TIC debe crear y mantener una metodología que controle el ciclo completo de desarrollo y mantenimiento seguro de sistemas e infraestructura. Los requerimientos de seguridad de la información deben ser identificados previos al diseño y desarrollo de los sistemas de tecnología de la información.
- Durante el desarrollo, estos requerimientos deben ser incluidos dentro de los sistemas y si una modificación es requerida, ésta debe cumplir estrictamente con los requerimientos de desarrollo seguro y seguridad de la información que han sido previamente establecidos. El nivel de Seguridad de la Información de un sistema no puede verse disminuido, por lo que la información y los sistemas en producción no serán utilizados para desarrollo, prueba o mantenimiento de aplicaciones.
- La implantación de un sistema nuevo o cambio significativo a los existentes debe ser revisada por medio de una evaluación de riesgo, que permita la detección de riesgos, la ubicación de controles apropiados que los mitiguen o eliminen y la operación segura.

- 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 debe asegurar el cumplimiento de la Política de Seguridad y ciberseguridad de la Información y sus respectivas normas, y en caso de exponer a COVIANDINA S.A.S, a un riesgo en seguridad de la información, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo responsable de la Información.
- En la gestión de Incidentes de seguridad de la información, se registra, asigna, hace seguimiento y resuelve situaciones (problemas) que comprometen la disponibilidad de los servicios que provee tecnología al negocio.

4.16. SEGURIDAD DE LAS OPERACIONES

Garantizar las operaciones de la entidad, cumplan con las condiciones de seguridad requeridas para mantener su confidencialidad, disponibilidad e integridad.

4.16.1. Protección contra software malicioso

- La entidad 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 entidad y terceros frente a los ataques de software malicioso.
- Asegurar que el software de antivirus, Antispam, y otras aplicaciones cuenten con licencias de uso requerido.
- Se tiene configurado y establecido un mecanismo a través del firewall que no permite descargar programas no autorizados.

4.16.2. Copias de respaldo

- La entidad debe asegurar 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 entidad 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.
- Los medios magnéticos que contienen la información sensible deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo debe contener los mecanismos de seguridad adecuados.

4.16.3. 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 debe ser solicitado y autorizado al oficial de seguridad de la información y al coordinador de TI.

4.17. 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 que deben ser registrados.
- 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 deben reportar al líder de seguridad de la información cualquier tipo de anomalía o incidente de seguridad que se presente.

4.18. ALMACENAMIENTO Y TRANSFERENCIA DE INFORMACIÓN

- Los usuarios deben almacenar o guardar 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, debe ser 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 del OneDrive y SharePoint, 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.

4.19. GESTIÓN DE ACTIVOS

Garantizar que los activos de información, de la entidad cuenten con un propietario, adicionalmente que cumpla con el nivel de protección adecuado.

4.19.1. Inventario de activos de información

Los líderes de cada proceso son los propietarios de la información, quienes deben identificar los activos de información 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 12 meses.

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.

4.19.2. Publicación

El inventario de activos de información debe ser un documento clasificado como "***Confidencial"***, y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien hagas sus veces.

4.19.3. Uso aceptable de los activos de información

Los trabajadores no deben divulgar información pública o reservada o dato sensible de la entidad a personas no autorizadas o a 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 deberá realizarse por el canal que esté oficialmente establecido o con las autorizaciones respectivas.

La información de la entidad no debe ser divulgada sin contar con los permisos correspondientes, además, ningún trabajador, contratista o consultor debe copiarla o extraerla en el momento en que se retire de la entidad o durante su permanencia.

4.19.4. Devolución de los activos de información

El propietario y/o custodio del activo de información deberá garantizar 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.
En los casos en que el empleado o parte externa compre el equipo de la organización o use su propio equipo personal, se deberían seguir procedimientos para asegurar que toda la información pertinente sea transferida a la organización y borrada del equipo en forma segura.

4.19.5. Clasificación de los activos de información

Los activos de información se deben clasificar de acuerdo con:

- **La Confidencialidad**

Para Coviandina la información que sea Confidencial no deberá estar disponible ni ser revelada a individuos, 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

- **La disponibilidad**

Para Coviandina 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.

- **La integridad**

Para Coviandina 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.

4.19.6. Seguridad de los activos de información

Los activos de información de Coviandina deben contar 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.

4.20. PREVENCION PARA LA FUGA DE INFORMACIÓN.

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

- La gestión y administración de la información para él envió 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 realiza un monitoreo trimestral 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.
- A través de la herramienta o plataforma office 365, se tiene implementado una configuración de seguridad llamada DLP, con el objetivo de restringir fuga de información que se maneja por cada buzón o cuenta de correo.

4.21. REVISIÓN POR LA GERENCIA

La política de seguridad de la información y ciberseguridad es revisada y aprobada por la 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.

4.22. ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

- **Oficial de seguridad de la información:** Implementar controles y medidas preventivas para mitigar los riesgos relacionados con temas de ciberataques, perdida de información, fraude, secuestro de información, etc. De igual forma dar tratamiento y planes de respuesta a los incidentes de seguridad de la información y ciberseguridad que se presenten en Coviandina.
- **Coordinador de tecnología:** Implementar los controles y dar soluciones a las instrucciones emitidas por el oficial de seguridad de la información a través de las herramientas tecnológicas e infraestructura que tiene actualmente Coviandina.
- **Trabajadores de Coviandina:** Comunicar al Oficial de seguridad de la información los incidentes de seguridad de la información que se presenten en su entorno laboral.

- **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.
  - ✓ Cumplir cualquier instrucción que sobre la materia se incluya en los acuerdos de Niveles de Servicio que se convengan.
  - ✓ En caso de que el tercero subcontrates servicios de computación en la nube o algún otro servicio de computación pactados contractualmente, deben cumplir 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 en un plazo no mayor a veinticuatro (24) horas contadas a partir de la fecha de ocurrencia del incidente.
- **Gerente Financiera y Administrativa:** Aprobar las solicitudes de inversión y compra de herramientas tecnológicas perimetrales sugeridas por grupo Aval.
- **Junta directiva:** Aprobar la estrategia y modelo de seguridad de la información que se está implementando en Coviandina.

4.23. CONTROLES CRIPTOGRAFICOS

Coviandina cuenta con un mecanismo de cifrado de disco duro llamado BITLOCKER, 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 al negocio.

4.23.1. Gestión de VPN

Los usuarios deben utilizar 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.

4.24. CONTROL DE ACCESO EN LA RED

Para el ingreso o acceso a la red local de Coviandina, el usuario debe requerir una autorización y permiso al coordinador de tecnología a través de un usuario para su respectiva autenticación. Los invitados de igual forma deben solicitar al coordinador de TI, la clave de ingreso para conectarse a la red LAN de Coviandina. La red se encuentra segmentada en división A y B. En la red tipo A tienen permiso de navegación todos los usuarios de la empresa a nivel de Gerencia administrativa, coordinación y auxiliares en el que se

encuentra bloqueado todas las páginas web como YouTube, redes sociales, paginas para descargar programas, páginas de contenido no autorizado, etc.
En la red tipo B se encuentra la Gerencia general, el cual no tiene bloqueo de salidas, el cual pueden entrar a YouTube y ciertas páginas web autorizadas.

4.25. ROLES Y RESPONSABILIDADES DE CIBERSEGURIDAD DE TERCEROS

Los terceros como proveedores y clientes deben realizar o responder cualquier tipo de solicitud que se realice 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:
  - Monitorear y reportar cualquier actividad o conexión sospechosa a través del Firewall de Coviandina.
  - Atender los requerimientos y solicitudes realizadas relacionadas con el incidente de ciberseguridad.
- Proveedor SAP:
  - Dar respuesta a los requerimientos y solicitudes realizadas relacionadas con el incidente de ciberseguridad.

4.26. SEGURIDAD EN GESTIÓN HUMANA

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

4.27. PROTECCION DE LA INFORMACION DE REGISTRO

- Se deben generar logs de registro y de accesos de los sistemas de información, para evaluar y verificar controles de acceso. Este monitoreo se debe realizar trimestralmente con el fin de identificar que los usuarios que este ingresando a los sistemas de información, sean los autorizados.

- Se debe monitorear y controlar 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
- También se debe ejecutar actividades de seguimiento a las herramientas de seguridad perimetrales, en este caso la gestión y administración de las VPN.

Lo anterior se debe llevar a cabo a través del diligenciamiento del formato FT-TEC-012 Seguimiento reportes de operación.

4.28. REPORTES DE EVENTOS DE SEGURIDAD DE LA INFORMACION Y CIBSERSEGURIDAD

El oficial de seguridad de la información mensualmente comunica campañas de prevención sobre posibles vulnerabilidades que se presentan a diario con el objetivo de alertar a los trabajadores de COVIANDINA de nuevas amenazas y evitar la posibilidad de que caigan de forma ingenua y se materialice el riesgo de pérdida de confidencialidad, integridad y disponibilidad de la información.
Se tiene como contacto principal, dirigirse a la página web principal del grupo de respuesta de emergencias cibernéticas de Colombia “COLCERT”, para consultar las comunicaciones diarias y eventos de seguridad de la información y ciberseguridad.
De igual forma en el momento que se materialice algún evento de riesgo de seguridad de la información, en el que se vea afectado la integridad, disponibilidad y confidencialidad de la información, este debe ser comunicado y denunciado en la página de la policía nacional en la opción denuncias virtuales.

4.29. 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 deben ir guardadas en un sobre bien sellado. Este sobre va guardado en una caja fuerte, el cual solo tiene acceso personal autorizado del área de contabilidad.

4.30. LEGALIDAD DEL SOFTWARE

El software que adquiere y mantiene COVIANDINA 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 de que el software instalado se encuentre licenciado y autorizado para el uso de funciones y operaciones diarias de COVIANDINA.

4.31. 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 nombrados de las bases de datos no automatizadas (Propietarios de la información), serán los encargados de asegurar el cumplimiento de los controles aplicables a las mismas para las bases de datos automatizadas, el área de GRC y la gerencia administrativa y financiera apoyara la implementación de los controles

Control de acceso:

El personal de Coviandina S.A.S solamente debe acceder 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.

Archivos de documentos:

Coviandina S.A.S., fija los criterios y procedimientos de actuación que se deben utilizar 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 debe considerar, 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 deben disponer 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 los mismos debe custodiarlos e 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 deben encontrarse 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 deben permanecer cerradas cuando no se precise el acceso a dichos documentos.

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 deberá ser reportado como un incidente de seguridad.

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., debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

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 deber legal que requiera el tratamiento del dato personal.

Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse 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 deben adoptar 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 deben estar cifrados cuando se hallen fuera de las instalaciones que están bajo control de Coviandina S.A.S. Cuando no sea posible el cifrado, se debe evitar 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.

El oficial de seguridad de la información debe monitorear y realizar seguimiento del cumplimiento de los criterios de seguridad mencionados anteriormente.

4.32. ADQUISICION DE SOFTWARE:

- El software que adquiera Coviandina debe cumplir 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.

4.33. 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 SAS. Cada integrante, debe entender su rol, conocer y asumir su responsabilidad respecto a los riesgos en seguridad de la información y la protección de los activos de información de COVIANDINA S.A.S.

5. DOCUMENTOS DE REFERENCIA Y ANEXOS

- FT-TEC-007 Bitácora de eventos e incidentes de seguridad de la información
- FT-TEC-012 Seguimiento reportes de operación
- FT-TEC-008 Activos de información
- PR-GTH-002 Inducción formación, capacitación y entrenamiento
- PO-DIR-001 Reglamento Interno de Trabajo.

6. 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