SISTEMA INTEGRADO DE GESTIÓN

DC-DIR-09

POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

COMPAÑÍA DE SERVICIOS DE VIGILANCIA PRIVADA PORTILLA Y PORTILLA LTDA

VERSION 4

ELABDORADO POR:	REVISADO POR:	APROBADO POR:
Firmado en original **FIRMA: DIRECCION DE PROYECTOS**	Firmado en original **FIRMA: DIRECCION SIG**	Firmado en original **FIRMA: GERENTE GENERAL**
NOMBRE: JOSEPP CARRERA	**NOMBRE: ANGELA GONZALEZ ROMERO**	**NOMBRE: C. ADRIANA PORTILLA SANCHEZ**
FECHA: 21 de abril del 2025		**N° DE FOLIOS 13**

1. INTRODUCCIÓN

Con el propósito de garantizar la continuidad operativa y la protección de los activos críticos de COSERVIPP Ltda., la Compañía ha adoptado una Política de Seguridad de la Información y ciberseguridad destinada a preservar la confidencialidad, integridad y disponibilidad de los datos, así como la infraestructura, las tecnologías de apoyo y demás herramientas se deben incluir para garantizar la confidencialidad y protección integral de la información

La política establece directrices claras para proteger los activos de información frente a amenazas, ataques, accesos no autorizados y demás riesgos que puedan comprometer la seguridad de la organización. Asimismo, define las responsabilidades que deben asumir los colaboradores, proveedores y terceros, fomentando una cultura organizacional orientada a la protección de la información.

La implementación rigurosa de esta política es esencial para prevenir incidentes de seguridad y salvaguardar la integridad operativa de la empresa. Por tanto, todo el personal de COSERVIPP Ltda. está llamado a cumplir las normas establecidas y a participar activamente en la protección de los sistemas y la información de la Compañía.

2. OBJETIVO:

Establecer los lineamientos del Sistema de Gestión para la Seguridad de la Información (SGSI) de COSERVIPP Ltda. definiendo un conjunto de directrices y controles para la protección efectiva de los activos de información. A su vez, busca promover una cultura de seguridad entre: los empleados, proveedores y terceros que interactúan con la empresa, con el fin de mitigar la materialización de los riesgos de seguridad de la información, así como el cumplimiento de las normativas y regulaciones vigentes

3. ALCANCE:

Esta política se extiende a todos los directivos, empleados, practicantes, contratistas, proveedores, terceros y demás partes interesadas que tienen acceso a los activos de información de COSERVIPP Ltda., quienes deben cumplir con los procedimientos y normas establecidas para garantizar su manejo en condiciones de seguridad.

En cuanto a los activos de información de COSERVIPP Ltda., se incluyen todos los datos y documentos en formatos físicos y digitales, que sean de su propiedad o que estén bajo su custodia. Esto comprende información confidencial y/o sensible, personal o de carácter estratégico, así como los sistemas, redes, bases de datos y aplicaciones que procesan, almacenan o transmiten dicha información.

Asimismo, la Política se aplica a todos los procesos administrativos, operativos y técnicos que involucren la gestión, almacenamiento, transmisión y eliminación de la información. Para ello, se establecen controles específicos que permiten asegurar que todos los procedimientos de la Compañía se alineen con los principios fundamentales de confidencialidad, integridad y disponibilidad de los datos, en concordancia con los estándares normativos y de buenas prácticas en seguridad de la información.

4. DEFINICIONES

- **Sistema de Gestión para la Seguridad de la Información (SGSI):** Conjunto de políticas, procedimientos, procesos y controles que se implementan dentro de COSERVIPP Ltda. para gestionar y proteger los activos de información, garantizando la confidencialidad, integridad y disponibilidad de los datos.
- **Activo de la información**: Dato, documento, sistema o recurso, en formato físico o digital que se considere como valioso para la compañía y que sea susceptible de ser protegido para garantizar su seguridad y correcto manejo.
- **Acuerdo de confidencialidad:** Arreglo mediante el cual las contrapartes de COSERVIPP Ltda. se comprometen a garantizan la no divulgación de documentos o información que revistan un carácter de reserva y especial protección de la compañía.
- **Incidente de seguridad de la información:** Intento de acceso, acceso, uso, divulgación, modificación, destrucción o cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de los activos de información.
- **Integridad:** Cualidad de los datos que garantiza que la información se mantenga completa y sin modificaciones no autorizadas, preservando su exactitud y confiabilidad.
- **Disponibilidad:** Disposición de que los sistemas, datos e información estén accesibles y utilizables cuando se necesiten, por los usuarios autorizados.
- **Respaldo:** Consiste en la (s) copia (s) de seguridad de los datos o sistemas importantes de la empresa, creada con el fin de resguardar la información ante posibles pérdidas, daños o fallos.
- **Riesgo de Seguridad de la Información**: Probabilidad de que una amenaza se materialice en un incidente sobre un activo de información, causando un impacto negativo a la compañía.
- **Amenaza**: Situación o acción con el potencial de afectar negativamente la seguridad de la información, ya sea causando daño, alteración, acceso no autorizado o pérdida de los datos o sistemas.
- **Vulnerabilidad**: Debilidad o falla en un sistema, proceso o control que puede ser aprovechada por una amenaza para comprometer la seguridad de la información.
- **Usuario Autorizado**: Persona cuyo acceso a determinados recursos o información de la compañía ha sido previamente verificado y aprobado, otorgándole los permisos necesarios para su uso de acuerdo con su rol y/o función.
- **Gestión de Incidentes**: Proceso que abarca la identificación, evaluación, respuesta y resolución de eventos que puedan afectar la seguridad de la información, con el objetivo de minimizar su impacto y restaurar las condiciones normales de operación.
- **Control de Acceso:** hace referencia a los mecanismos dispuestos por COSERVIPP Ltda. para limitar el acceso a la información, los cuales están determinados por los lineamientos internos de seguridad previstos en esta Política.
- **Repositorio:** Hace referencia al lugar o ubicación lógica donde se permite el almacenamiento de los datos y/o informaciones pertenecientes a la organización

5. PRINCIPIOS DE LA POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN:

COSERVIPP Ltda. ha establecido los siguientes principios básicos como criterios rectores a implementarse durante el proceso de desarrollo y ejecución de los sistemas de seguridad de la información.

- **Confidencialidad:** la información debe ser accesible únicamente a los individuos o sistemas debidamente autorizados, protegiendo así los datos sensibles de accesos no permitidos y salvaguardando la privacidad de la información.

- **Responsabilidad**: El manejo inadecuado de la información o la infracción de las políticas de seguridad, así como el incumplimiento o inobservancia de las normativas internas establecidas, conllevarán la correspondiente atribución de responsabilidad.

- **Gestión del Riesgo**: la identificación, evaluación y mitigación de los riesgos asociados a la seguridad de la información, se implementarán conforme a la presente Política, ello con el fin de reducir la probabilidad de materialización de incidentes y su impacto negativo.

- **Proporcionalidad:** Las medidas de protección, detección y recuperación implementadas por COSERVIPP Ltda. deberán ser apropiadas y equilibradas en relación con los riesgos potenciales, implicando que, a mayor riesgo o importancia de los activos, se deberán aplicar controles más rigurosos para garantizar su seguridad.

- **Seguridad Integral:** Se entenderá como un proceso constituido por elementos organizativos, humanos, técnicos y materiales, encaminado a garantizar el acceso y uso de la información en condiciones de seguridad para la compañía.

- **Mejora continua:** Los procesos establecidos para la seguridad de la información serán **evaluados, actualizados y fortalecidos de manera periódica**, con el fin de garantizar su eficacia frente a la constante evolución de los riesgos, tecnologías y amenazas. La gestión de la seguridad de la información se llevará a cabo mediante un enfoque sistemático y proactivo, siendo **revisada y auditada regularmente por personal calificado**, lo que permitirá la **adopción de medidas correctivas y preventivas**, y la **adaptación continua** a los nuevos desafíos del entorno digital.

- **Integralidad:** La presente Política de Seguridad de la Información y ciberseguridad se enmarca en la regulación interna de COSERVIPP Ltda. y se integra con el Reglamento Interno de Trabajo, la Políticas de Protección de Datos Personales y todos los demás instrumentos normativos existentes que guarden relación y se armonicen con sus lineamientos.

6. COMPROMISOS DE LA DIRECCIÓN EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

COSERVIPP Ltda. reconociendo la importancia fundamental de implementar esta Política de Seguridad de la Información y ciberseguridad para proteger sus activos informáticos y alcanzar sus objetivos estratégicos, se compromete a:

- Liderar y promover una cultura de seguridad de la información en todos los niveles de la empresa, generando espacios de sensibilización sobre la importancia de la protección de los activos de información con sus colaboradores y partes interesadas.

- Asegurar los recursos financieros, tecnológicos y humanos necesarios para implementar, mantener y mejorar continuamente las medidas de seguridad de la información de acuerdo con las mejores prácticas y normativas vigentes.

- Cumplir todas las leyes, regulaciones y normativas aplicables, incluyendo aquellas relativas a la protección de datos personales, ciberseguridad y manejo de información sensible.
- Monitorear la implementación de mecanismos de revisión periódica al Sistema de Gestión para la Seguridad de la Información de la compañía, corrigiendo debilidades para asegurar su efectividad y adaptación a nuevas amenazas.
- Promover la difusión de los objetivos y procedimientos de la Política de Seguridad de la Información y ciberseguridad a sus colaboradores y partes interesadas, promoviendo una política de transparencia y responsabilidad.
- Fomentar el desarrollo de programas de capacitación y sensibilización en seguridad de la información para sus empleados, asegurando que comprendan sus responsabilidades y los riesgos asociados.

7. INFORMACIÓN REGLAS PARA LA SEGURIDAD DE LA INFORMACIÓN EN COSERVIPP Ltda.

Con el objetivo de asegurar la correcta aplicación de la presente Política en todas las áreas de la organización, se implementarán una serie de pautas de gestión que deberán ser cumplidas rigurosamente por todos los empleados, sin importar su nivel o ámbito de actuación. Estas pautas han sido diseñadas para integrar de manera efectiva los principios de seguridad de la información en cada uno de los procesos organizacionales, garantizando su cumplimiento y la protección adecuada de los activos de información en todos los niveles.

7.1. Gestión y clasificación de activos de información

Todos los activos de información de COSERVIPP Ltda. incluyendo los datos, documentos y sistemas de información, deben ser identificados y registrados en un inventario centralizado a cargo de director de proyectos de tecnología. Este inventario será actualizado cada año, para reflejar cambios, altas o bajas de activos y en él se definirá el ciclo de vida de los datos, según las necesidades de la Compañía.
Cada activo de información debe ser clasificado según su nivel de sensibilidad y valor para la empresa, según dicha información sea: pública, interna, confidencial o restringida. Esta clasificación se realizará conforme a criterios claros y el personal deberá ser informado sobre las categorías de información y sus respectivos niveles de protección.
Los accesos a los activos de información se establecerán en función de su clasificación y del rol de cada usuario. Los activos con clasificación confidencial o restringida estarán accesibles únicamente para personal autorizado con necesidades específicas de uso.

7.2. Gestión de Vulnerabilidad

El área de tecnología establecerá unos monitoreos periódicos a efectos de verificar la existencia de eventuales vulnerabilidades y amenazas que comprometan la seguridad de la información de la organización.
A su vez, todo el personal que tenga conocimiento de una posible vulnerabilidad en el tráfico de la información, deberá reportarla inmediatamente al equipo de tecnología, donde se evaluará la tipificación y registro de vulnerabilidad en el tablero de control de seguimiento para asegurar su gestión en el menor tiempo posible, a efectos de prevenir potenciales daños y adoptar acciones correctivas permanentes.

7.3. Gestión de riesgos en activos de información

Para todos los efectos, los activos de información deben ser identificados y clasificados de acuerdo con su valor para la organización, y así valorar los posibles riesgos de manera regular e identificar potenciales amenazas y vulnerabilidades al sistema de información de la organización.

7.3.1. Responsable de la gestión de riesgos en activos de información.

El coordinador de riesgos de la compañía deberá identificar, evaluar y valorar de manera permanente los posibles riesgos emergentes, e implementar los controles de seguridad idóneos a efectos de reducir el porcentaje de probabilidad de ocurrencia de estos.

El responsable de la gestión de riesgos convocará a un comité de seguridad de la información por lo menos una vez a cada tres (3) meses o cada vez que se requiera, para monitorear los riesgos de seguridad de la información, así como la efectividad de los controles implementados por la Compañía., así como para adaptarlos a nuevas amenazas y eventuales avances tecnológicos. De cada comité se dejará un acta en la que conste por lo menos; los asistentes, los riesgos identificados, los controles desplegados y las oportunidades de mejora en materia de seguridad de la información.

7.3.2. Responsable de la designación de los mecanismos tecnológicos a implementar en la protección de la información.

El coordinador de riesgos de la compañía en coordinación con el director de proyectos de tecnología y bajo la supervisión de la Gerencia, serán los encargados de realizar un análisis de las amenazas y vulnerabilidades asociadas a los activos de información de la compañía para determinar los mecanismos tecnológicos más adecuados, así como las herramientas y soluciones de seguridad que se ajusten a las necesidades de COSERVIPP Ltda.

7.4. Gestión de Incidentes de Seguridad

7.4.1. Responsable de la gestión de Incidentes de Seguridad

El director de proyectos de tecnología será el responsable de liderar y coordinar todas las actividades relacionadas con la identificación, evaluación, respuesta y resolución de incidentes que puedan comprometer la seguridad de la información. Sus funciones y responsabilidades incluyen:

- Dirigir la respuesta ante incidentes de seguridad, asegurando que se implementen los procedimientos adecuados para la contención, mitigación y recuperación de los activos afectados.
- Supervisar la implementación de herramientas y procesos para la detección temprana de incidentes, así como la evaluación de su naturaleza y severidad.
- Mantener el registro detallado de todos los incidentes de seguridad, incluyendo su origen, evolución, acciones tomadas y resultados, para facilitar análisis posteriores y auditorías.
- Actuar como punto de contacto principal para la comunicación sobre incidentes de seguridad, informando a la dirección y, cuando sea necesario, a partes externas sobre el estado y las acciones tomadas.
- Realizar análisis exhaustivos después de cada incidente para identificar causas, evaluar la efectividad de la respuesta y proponer mejoras a las políticas y procedimientos de seguridad.
- Trabajar de manera colaborativa con otras áreas (Operaciones, recursos humanos, legal, etc.) para garantizar que la gestión de incidentes sea integral y esté alineada con los objetivos organizacionales.

Cualquier colaborador de la compañía que detecte un incidente de seguridad tiene la obligación de reportarlo de manera inmediata al director de proyectos de tecnología, por medio del siguiente correo electrónico (dir.proyectos@coservippltda.com.co). Lo anterior, con el fin de ser evaluado el presunto incidente, y así determinar su naturaleza, nivel de riesgo y posible impacto, permitiendo coordinar las acciones de contención, mitigación y resolución del incidente de manera eficiente, siguiendo un plan de respuesta que involucre a las áreas técnicas y operativas relevantes.

7.4.2. Procedimiento en casos de delitos informáticos

El siguiente procedimiento detalla los pasos a seguir para realizar una denuncia ante las autoridades competentes, como la policía y la Seccionales de Investigación Judicial y Criminal (SIJIN), en caso de un incidente o robo de información, identificados como Phishing, Spyware, Malware y distintos Ransomware.

- El director de proyectos de tecnología responsable de la seguridad de la información documentará la naturaleza del incidente, la fecha y hora de la detección, así como cualquier evidencia preliminar disponible.
- Asimismo, evaluará la gravedad del incidente, determinando si se trata de un robo de información, acceso no autorizado, o cualquier otra amenaza que comprometa la seguridad de los activos informacionales.
- Se tomarán medidas inmediatas para contener el incidente y minimizar su impacto, como el aislamiento de sistemas afectados o el bloqueo de accesos no autorizados.
- Con posterioridad, se reunirá toda la información relevante, incluyendo logs de sistemas, correos electrónicos, grabaciones de video y cualquier otra evidencia que respalde el caso, así como la consolidación de declaraciones de testigos o personas involucradas en el incidente, que puedan aportar información adicional sobre lo ocurrido.
- A su vez, el director de proyectos de tecnología elaborará un informe detallado que contenga la descripción del incidente, el análisis del impacto, todas las evidencias recopiladas, así como las medidas adoptadas para la mitigación del daño.
- El director de proyectos de tecnología en trabajo conjunto con la dirección general y el departamento legal de la compañía, identificaran la autoridad competente a la que se realizará la denuncia ante la Fiscalía General de la Nación, a efecto de poner en conocimiento los hechos que revisten carácter delictivo, para lo cual se entregará el informe de incidente y la documentación recopilada a la autoridad competente, a efectos de que ésta adelante las indagaciones, investigaciones y/o acciones judiciales correspondientes. Asimismo, se deberá informar a la gerencia sobre el avance de la denuncia y las acciones que se están tomando por parte de las autoridades.
- Una vez resuelto el incidente, realizar un análisis de la respuesta y el proceso de denuncia para identificar áreas de mejora en la gestión de incidentes futuros.

7.5. Gestión de riesgos en procesos

En cada proceso de la organización, se debe realizar de forma continua la identificación de riesgos potenciales que puedan afectar la seguridad, calidad, o eficiencia del proceso. Esta identificación debe revisarse y/o actualizarse con una periodicidad de una (1) vez al año o cuando se presenten cambios significativos en el proceso o en el entorno.

En cualquier proyecto conjunto con terceros o asociaciones estratégicas, se debe realizar una evaluación de riesgos compartidos. Esto implica analizar los controles de seguridad que las empresas asociadas tienen implementados para asegurar la protección de los activos de información que serían compartidos; por lo que todo proceso de colaboración con otras compañías debe formalizarse mediante acuerdos de confidencialidad y protección de la información, especificando responsabilidades, controles y estándares de seguridad que garanticen la integridad de la información en ambos lados.

7.6. Gestión de riesgos en Proyectos

COSERVIPP Ltda. implementará a través de la dirección de proyectos de tecnología, los controles de seguridad a ser considerados en la fase de diseño de toda clase de proyectos que participe la empresa. Esto incluye la definición de requisitos de seguridad y su implementación en todas las etapas del ciclo de vida del proyecto.

Quien adelante un proyecto en nombre de la compañía, o suscriba contratos o convenios con terceros, deberá contar previamente con la autorización correspondiente para el uso y tratamiento de la información perteneciente a la organización.

Adicionalmente, se deberá establecer de forma expresa, dentro de los términos contractuales o del acuerdo, que todas las partes involucradas en el proyecto se comprometen a cumplir con la **Política de Seguridad de la Información y Ciberseguridad**, así como con la **Política de Tratamiento de Datos Personales de COSERVIPP Ltda.**

Este compromiso incluye la protección de la confidencialidad, integridad y disponibilidad de la información, el uso responsable de los activos digitales y físicos de la organización, y el cumplimiento de las disposiciones legales vigentes en materia de protección de datos y ciberseguridad.

Todos los lineamientos establecidos en la presente política como normas y responsabilidades son aplicables a todos los participantes y colaboradores en el proyecto en el cual participa la organización o sus agentes.

7.7. Criterio para Inteligencia y la Gestión de Ciber amenazas

La dirección de proyectos de tecnología será la responsable de implementar sistemas y procesos de monitoreo continuo a efectos de identificar amenazas potenciales, incluyendo la vigilancia de redes, sistemas y actividades sospechosas dentro y fuera de la infraestructura de COSERVIPP Ltda. A su vez, deberá clasificar las ciber amenazas según su nivel de riesgo e impacto potencial, con el fin de priorizar la respuesta y gestionar adecuadamente los recursos de protección de la información.

7.8. Gestión y Control de Accesos y Perfiles de usuario

La dirección de proyectos de tecnología será la encargada de administrar y otorgar accesos y perfiles de usuario, los accesos a los sistemas y la asignación de perfiles de usuario se realizarán en función de las responsabilidades y necesidades específicas de cada rol.

7.9. Gestión de relación con los Proveedores y Terceros

La dirección de proyectos de tecnología llevará a cabo una evaluación de seguridad previo a la formalización de la relación con cualquier proveedor o tercero, que verifique el cumplimiento de estándares mínimos en la protección de la información suministrada o susceptible de ser suministrada al momento de la suscripción contractual.

De otro lado, quienes se vinculen como proveedores y terceros y además cuenten con acceso a los sistemas de información de la organización, deberán notificar de inmediato a la compañía en caso de surgir cualquier incidente de seguridad que comprometa la integridad de la información de la empresa. Al finalizar la relación contractual, el proveedor o tercero deberá devolver y/o restringir de forma segura todos los datos de la compañía en su poder. Este proceso debe ser documentado y certificado para asegurar la protección de la información.

7.10. Gestión de los usuarios en relación con el uso de los activos de la información.

COSERVIPP Ltda. se reserva el derecho de monitorear el uso de los activos de información para asegurar el cumplimiento de la política de seguridad, siempre respetando la normativa vigente en materia de privacidad y

protección de datos, ello, por cuanto la infracción de la Política de Seguridad de la Información y ciberseguridad y demás que hayan sido establecidas por la compañía, constituirá una falta disciplinaria como quiera que la inobservancia de los procedimientos para la salvaguarda y buen uso de la información será causal de investigación y eventual sanción de conformidad a los criterios de graduación establecidos en el Reglamento Interno de Trabajo.

Los empleados recibirán acceso únicamente a los activos de información necesarios para cumplir con sus funciones, conforme al principio de privilegio mínimo. Por lo tanto, los accesos a los activos de información se revisarán y ajustarán regularmente para asegurar su adecuación. Cuando un empleado finalice su relación laboral, se procederá a la revocación inmediata de sus accesos a los sistemas y activos de información, asegurando la devolución de los dispositivos y la protección de la información.

8. USO DE LA TECNOLOGÍA, PROCESAMIENTO Y SEGURIDAD DE LA INFORMACIÓN EN COSERVIPP LTDA

8.1. CONTROL DE ACCESO A LA INFORMACIÓN Y SISTEMAS

- **Administración del Control de Acceso:** El acceso a la información y sistemas será gestionado por personal autorizado, respetando los perfiles de usuarios y prioridades del negocio.
- **Control de Acceso al Usuario:** El acceso sólo se permitirá con justificación formal por el usuario propietario y autorización escrita del administrador responsable.
- **Protección de Equipos**:
  - Los equipos desatendidos deben estar protegidos física y lógicamente.
  - Los usuarios son responsables de la información y uso de herramientas tecnológicas.
  - Los puertos de comunicación (ej. USB) deben estar bloqueados, salvo excepciones autorizadas por la gerencia general.
- **Control de Acceso a la Red**: Similar a otros accesos, debe ser administrado por el personal autorizado y respetando los perfiles de usuarios.
- **Restricción de Acceso a la Información:** Las restricciones deben basarse en niveles de acceso adecuados a los roles y minimizar riesgos de seguridad.
- **Monitoreo de Acceso y Uso**: Todos los accesos a recursos tecnológicos deben ser registrados y monitoreados.
- **Acceso a Activos de Información:** Debe ser controlado y autorizado formalmente, asegurando la disponibilidad solo para personal previamente autorizado por el director de proyectos de tecnología.
- **Control de Usuarios Remotos:** Acceso limitado a usuarios remotos pertenecientes al área de tecnología
- **Seguridad de Aplicaciones**: Cada aplicación debe tener un Administrador de Seguridad calificado y autorizado.
- **Claves de Máximos Privilegios**: Estas claves tendrán un nivel de clasificación alto y deben ser administradas con estrictos mecanismos de control.

8.2. PROCESAMIENTO DE INFORMACIÓN Y DOCUMENTOS

8.2.1. Redes.

- **Arquitectura y Configuración de la Red:** La red está diseñada y configurada para satisfacer las necesidades del negocio, garantizando un alto rendimiento.
- **Administración de la Red:** Solo personal calificado y autorizado puede gestionar la red, cumpliendo con los acuerdos de servicio y priorizando las necesidades del negocio.
- **Administración de Plataformas de Seguridad**: Las plataformas de seguridad de la red deben ser administradas exclusivamente por personal calificado y autorizado, conforme a los mismos principios de servicio y prioridades.
- **Acceso Remoto a la Red:** El acceso remoto a la red está autorizado solo a usuarios pertenecientes al área de tecnología

8.2.2. Operaciones y Administración de Sistemas

- **Administración de Sistemas**: La gestión de los sistemas debe ser realizada por personal calificado y autorizado, siguiendo las normas de seguridad y acuerdos de servicio.
- **Control de Distribución de Información**: Los propietarios de la información deben establecer controles para asegurar la distribución adecuada de información a personas autorizadas.
- **Revisión de Registros de Eventos**: Los registros de eventos de error y seguridad deben ser revisados y documentados de manera continua por personal calificado.
- **Programación de Operaciones de Sistemas:** Las operaciones deben ser planificadas y autorizadas por personal calificado, siguiendo los protocolos de seguridad.
- **Cambio y Mantenimiento de Programación:** Cualquier modificación debe contar con la aprobación del área de tecnología y seguir las políticas de control de cambios.
- **Sincronización de Relojes de Sistemas:** Los relojes de los sistemas deben estar sincronizados entre las distintas plataformas.
- **Atención de Fallas de Sistemas:** Solo personal calificado y autorizado debe gestionar fallas en los sistemas, siguiendo los acuerdos de servicio.
- **Contratación de Servicios Externos:** La contratación de servicios externos debe cumplir con los requerimientos mínimos exigidos por el procedimiento de proveedores y contratistas del área de logística y ser aprobada por la gerencia administrativa.

8.2.3. Correo Electrónico e Internet

- **Correo Electrónico:** Solo el personal autorizado debe usar el correo de la empresa con fines laborales, respetando los procedimientos de uso, almacenamiento y retención.
- **Internet:** Su uso está permitido para apoyar labores diarias; terceros requieren aprobación de seguridad tecnológica**.**
- **Descarga de Archivos:** Solo se permite descargar información relacionada directamente con el rol laboral y para actividades del negocio.

- **Firmas Digitales:** Para COSERVIPP ltda., este ítem se considera la digitalización del manuscrito y solo se hace uso de la misma, con previa autorización del titular para intercambiar información**.**

8.2.4. Dispositivos de Transmisión de la Información

- **Administración de Dispositivos**: Los dispositivos de transmisión de información deben ser gestionados y controlados de manera segura por el área de tecnología.
- **Uso de Dispositivos**: Solo se permite el uso de dispositivos de transmisión de información con autorización formal del director de proyectos de tecnología.

8.2.5. Manejo de la Información

- **Transferencia e Intercambio:** Requiere autorización formal del propietario de la información, en concordancia con las políticas de seguridad.
- **Administración de Bases de Datos:** Solo personal autorizado puede gestionar las bases de datos, respetando la seguridad y acuerdos de servicio.
- **Cambios de Emergencia:** Solo personal autorizado puede realizar cambios urgentes sin comprometer la seguridad de la información.
- **Estructuras de Información**: Solo personal autorizado administra directorios y carpetas, siguiendo los acuerdos con el propietario.
- **Preservación de Información:** Debe realizarse conforme a las tablas de retención, asegurando la integridad y cumplimiento normativo.
- **Nuevas Bases de Datos**: Su creación y control está a cargo del personal autorizado y/o jefe de proceso, en concordancia con la actual política.

8.2.6. Respaldo, Almacenaje y Recuperación

- **Respaldo:** El respaldo de los datos e información se realizan de manera automática siempre y cuando se encuentren almacenados en los repositorios autorizados.
- **Recuperación:** La recuperación de datos se realiza por personal autorizado bajo la petición del propietario de la información.

8.2.7. Seguridad de la Información

- **Manejo de Información:** Se implementarán mecanismos para que empleados y terceros conozcan sus compromisos legales y corporativos en el manejo de información.
- **Intercambio con Terceros:** Toda información compartida con terceros requiere autorización formal cumpliendo la normativa de actual política.
- **Protección contra Riesgos:** La empresa debe proteger toda su información en cualquier formato para mantener su integridad, confidencialidad y disponibilidad.
- **Control de Acceso:** Se protegerá el acceso a la información mediante autenticación e identificación adecuadas.

8.2.8. Manejo y Procesamiento de Otra Información

- Eliminación de Información: La eliminación de datos en medios a desincorporar debe ser autorizada y realizada por personal autorizado, siguiendo políticas de gestión archivística.
- Uso de Dispositivos de Copiado: Solo personal autorizado puede utilizar dispositivos de copiado para fines del negocio.
- Escritorio Despejado: Todo el personal debe mantener los escritorios libres de información clasificada a la vista, tales como: claves de acceso, nombres de usuario, contraseñas, entre otros.
- Movilización de Información: La transferencia de información fuera de la empresa requiere autorización formal y medidas de custodia.

9. SENSIBILIZACIÓN Y COMUNICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

COSERVIPP Ltda. proporcionará información clara sobre la Política de Seguridad de la Información y ciberseguridad y los procedimientos asociados, procurando que los empleados, contratistas, proveedores, colaboradores y demás partes interesadas, conozcan sus responsabilidades específicas y los protocolos a seguir, poniendo a su disposición, todo el material físico y digital que facilite el acceso a recursos, guías, normas y procedimientos de seguridad de la información, para que así puedan consultar y actualizar sus conocimientos sobre la política y las mejores prácticas encaminadas a la protección de los activos de la información de la empresa.

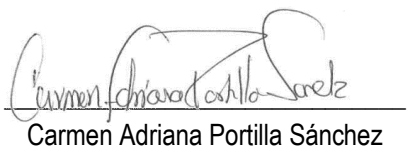
La Dirección de proyectos de tecnología adelantará campañas de concientización en seguridad de la información mediante boletines informativos, correos electrónicos, talleres, seminarios o estrategias similares, para recordar la importancia de la seguridad en el manejo de la información y mantener al personal informado sobre posibles amenazas y nuevas prácticas.

10. APROBACIÓN Y REVISIÓN DE LA POLÍTICA

La presente política será revisada de manera periódica, al menos una vez al año, o cuando se presenten cambios significativos en el entorno normativo, en la estructura organizacional, o en los sistemas y activos de información, con el fin de garantizar su vigencia, pertinencia y alineación con los nuevos requerimientos internos y externos.

Esta política ha sido aprobada y firmada, con vigencia a partir del 21 de Abril del 2025.

.



Carmen Adriana Portilla Sánchez

Gerente General

11. FORMATOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIFICACIÓN
NA	NA

12. CONTROL DE CAMBIOS

VERSION	CAMBIO	FECHA
4	En el marco de esta actualización del presente documento, se elimina la codificación **PO-GTI-001**, correspondiente a la antigua *Política de Gestión de la Tecnología de la Información,* integrando sus disposiciones en una nueva estructura normativa con los requisitos legales vigentes, los principios de seguridad de la información (confidencialidad, integridad, disponibilidad y trazabilidad) y las necesidades estratégicas e institucionales en materia de ciberseguridad y protección de la información.	21/04/2025