1. OBJETIVO

El objetivo principal de esta política del Sistema de Gestión de Seguridad de la Información (SGSI) en WEARE DEV S.A.S es establecer un marco sólido y coherente para salvaguardar la información de la organización y de sus clientes. Este conjunto de directrices busca garantizar la confidencialidad, integridad y disponibilidad de los datos mediante la implementación de medidas de seguridad física y lógica, así como la promoción de una cultura de seguridad entre los colaboradores.

A través de la aplicación de esta política, se busca lograr los siguientes objetivos específicos:

a) Promover la conciencia y el compromiso de todos los Colaboradores de WEARE DEV S.A.S con respecto a la seguridad de la información, asegurando que comprendan la importancia de proteger los activos de datos de la organización y de sus clientes.
b) Establecer controles adecuados para regular el acceso físico y lógico a los recursos informáticos, asegurando que solo las personas autorizadas tengan acceso a la información según sea necesario para realizar sus funciones laborales.
c) Garantizar la protección de los equipos de cómputo y de comunicaciones, así como de las instalaciones físicas de la organización, mediante la implementación de medidas de seguridad física y la promoción de prácticas seguras por parte de los usuarios.
d) Establecer procedimientos claros para la administración de operaciones de cómputo, incluyendo el almacenamiento seguro de información sensible y la gestión adecuada de la instalación de software.
e) Regular el uso de privilegios de acceso y cuentas privilegiadas, asegurando que solo las personas autorizadas tengan los permisos necesarios para realizar tareas específicas dentro del entorno informático de la organización.

Al alcanzar estos objetivos, se espera fortalecer la postura de seguridad de WEARE DEV S.A.S y mitigar los riesgos asociados con posibles amenazas a la seguridad de la información, protegiendo así los intereses de la organización y de sus clientes.

2. ALCANCE

La política de seguridad de la información en WEARE DEV S.A.S abarca a todos los Colaboradores, contratistas, consultores y terceros que acceden a los recursos informáticos y a la información de la organización. Esta política se aplica en todas las instalaciones de WEARE DEV S.A.S, incluyendo sus oficinas principales, sucursales y cualquier otro lugar donde se realicen actividades relacionadas con la compañía.

Las directrices establecidas en esta política son de aplicación obligatoria para todos los usuarios de los recursos informáticos de la organización, independientemente de su cargo o función. Esto incluye, pero no se limita a, directivos, personal administrativo, personal de TI, personal de operaciones y cualquier otro colaborador que utilice sistemas informáticos en el curso de sus responsabilidades laborales.

La política de seguridad de la información en WEARE DEV S.A.S se enfoca en la protección de la información en todas sus formas, incluyendo datos electrónicos, físicos y verbales. Además, esta política aborda aspectos clave de la seguridad de la información, como el acceso físico y lógico, la protección de equipos, la gestión de contraseñas, la administración de operaciones de cómputo y el control de acceso a la red.
Es responsabilidad de todos los usuarios adherirse a esta política y cumplir con las directrices establecidas en ella. Cualquier violación de esta política será tratada con seriedad y puede resultar en medidas disciplinarias, incluida la revocación de privilegios de acceso, acciones legales o terminación del empleo, según la gravedad de la infracción.

3. DEFINICIONES

- **Política:** declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Disponibilidad:** propiedad de ser accesible y utilizable a solicitud de una entidad autorizada.
- **Confidencialidad:** propiedad por la que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados.
- **Información documentada:** se refiere a la información necesaria que una organización debe controlar y mantener actualizada tomando en cuenta y el soporte en que se encuentra. La información documentada puede estar en

cualquier formato (audio, video, ficheros de texto etc.) así como en cualquier tipo de soporte o medio independientemente de la fuente de dicha información. en general la información documentada se refiere a:

- Al sistema de gestión y sus procesos
- Información necesaria para la actividad de la propia
- Evidencias o registros de los resultados obtenidos en cualquier proceso del sistema de gestión o de la organización

- **Evento:** ocurrencia o cambio de un conjunto particular de circunstancias
  - Un evento puede ser repetitivo y puede tener varias causas.
  - Un evento puede consistir en algo que no sucede.
  - Un evento puede ser clasificado como un “incidente” o “accidente”.

- **Seguridad de información:** preservación de la confidencialidad, integridad y disponibilidad de la información. Además, hay que considerar otras propiedades, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucrados.

- **Continuidad de la seguridad de la información:** procesos y procedimientos para garantizar la continuidad de las operaciones de seguridad de la información

4. RESPONSABILIDADES

La aplicación de la política está bajo la responsabilidad de todos los colaboradores y el liderazgo de la misma estará bajo el líder del proceso administrativo y financiero.

5. PRINCIPIOS

- La responsabilidad sobre la seguridad de la información será compartida y publicada para que todos los colaboradores la conozcan.
- WeAre Dev protegerá la información derivada de la operación de sus procesos, en su creación, procesamiento y transmisión de la misma.
- WeAre Dev implementará controles de acceso de la información documentada.

- WeAre Dev garantizará la disponibilidad de la información documentada que se encuentre en su dominio, para dar continuidad a la operación de los servicios.

6. LINEAMIENTOS

6.1. Gestión con instituciones de seguridad de la información

La gestión con instituciones de seguridad de la información tiene como objetivo establecer y mantener un contacto con organizaciones especializadas que puedan proporcionar apoyo para la implementación y mantenimiento del SGSI.

Considerando los requisitos de las partes interesadas y las regulaciones aplicables, **WEARE DEV S.A.S** mantiene contacto con las **SOINFCO S.A.S y SOPHOS SECURITY** para la comunicación y reporte de los incidentes de seguridad:

Organizaciones	Contacto
SOINFCO S.A.S	Teléfono: +57 324 202 1660 Correo electrónico: soporte@soinfco.com
SOPHOS SECURITY	Teléfono: 1 (833) 886-6005 Correo electrónico: support@sophos.com

Para asegurar la concientización y el conocimiento de los colaboradores, la compañía también mantiene contacto con grupos de interés especial que les permite capacitarse y estar actualizados sobre las mejores prácticas, nuevas amenazas, alertas y/o vulnerabilidades de seguridad.

Compañía | Institución	Medio de contacto
Hackmetrix	Blog, Hacknews (notificaciones sobre vulnerabilidades) Hackmeets (foros sobre temas de seguridad de la información).

ACRONIS	Gestión de vulnerabilidades
SOPHOS	Gestión de seguridad endpoint

6.2. Gestión de protección de datos personales

WeAre Dev comprende la importancia de la protección de datos personales y el cumplimiento de las normativas de seguridad aplicables al SGSI.
La seguridad implementada para la protección de datos de identificación personal es de manera general y consistente para toda la información de la compañía, sin distinción de la que contiene o no datos personales.
Con lo anterior garantiza que se permee la integridad, confidencialidad y disponibilidad en los datos personales que gestiona.

Además, WeAre DEV implementa los siguientes métodos de enmascaramiento de datos para garantizar su protección:

- ➔ Cifrado.
- ➔ Anulación o eliminación de caracteres.
- ➔ Variación de números y fechas.
- ➔ Sustitución (cambiar un valor por otro).
- ➔ Sustitución de los valores por su hash.

En caso de que sea necesario eliminar el vínculo y asociación del titular con sus datos personales, se implementan los lineamientos establecidos en la presente política ayudan, en diferentes niveles, con la prevención de fuga de datos.

6.3. Gestión de los dispositivos móviles y el trabajo

La gestión de los dispositivos móviles y el teletrabajo tiene como objetivo asegurar el buen uso por parte de los colaboradores o partes externas, de los activos y la información de la compañía que procesan.

Garantizamos que todos nuestros colaboradores se sientan seguros y respaldados mientras utilizan dispositivos móviles y disfrutan de la flexibilidad del teletrabajo.

Esta política busca establecer pautas claras para que puedan aprovechar al máximo estas herramientas, manteniendo al mismo tiempo la seguridad y la integridad de nuestra compañía. Queremos que cada miembro de nuestro equipo se sienta empoderado y protegido, sabiendo que están contribuyendo al éxito de la compañía desde cualquier lugar donde se encuentren. Para ello se aplican los siguientes controles:

- ➔ **seguridad de los dispositivos móviles:** Es responsabilidad de cada Colaborador proteger su dispositivo móvil mediante el uso de contraseñas robustas y mantenerlos actualizados con las últimas actualizaciones de seguridad. se requiere notificar de inmediato a la dirección de TI en caso de extravío o robo de un dispositivo móvil para que se tomen las medidas de seguridad adecuadas, como el bloqueo remoto o la eliminación segura de datos. Al ocurrir un robo o extravío, el colaborador debe informar de inmediato a su jefe directo y a las autoridades pertinentes.
- ➔ **Propósito y uso:** Los dispositivos móviles proporcionados por la compañía son herramientas destinadas exclusivamente para el desempeño de tareas laborales. Están diseñados para facilitar la comunicación, el acceso seguro a recursos corporativos y el aumento de la productividad de nuestros Colaboradores Actualizar el sistema operativo y aplicaciones de forma regular.
- ➔ **Instalación de aplicaciones:** Queda estrictamente prohibida la instalación de aplicaciones no autorizadas en los dispositivos móviles proporcionados por la compañía. Esto incluye aplicaciones de terceros no aprobadas por el departamento de TI.
- ➔ **Actualizaciones y mantenimiento:** Todos los dispositivos móviles deben mantenerse actualizados con las últimas versiones de software y parches de seguridad proporcionados por el departamento de TI de manera regular.
- ➔ **Conexiones a Redes Wi-Fi:** Se exige a los Colaboradores utilizar redes Wi-Fi seguras y evitar conectarse a redes públicas no protegidas mientras utilicen los dispositivos móviles de la compañía.
- ➔ **Responsabilidad del Colaborador:** Cada Colaborador es responsable de proteger la información confidencial de la compañía almacenada en su dispositivo móvil y de utilizarlo de manera responsable y ética en todo momento.
- ➔ **Monitoreo y cumplimiento:** El departamento de TI se reserva el derecho de monitorear el uso de los dispositivos móviles proporcionados por la compañía para garantizar el cumplimiento de esta política y proteger la seguridad de los datos corporativos.

- ➔ **Educación y capacitación:** Se ofrecerá capacitación regular a los Colaboradores sobre las mejores prácticas de seguridad en el uso de dispositivos móviles y la importancia de proteger la información confidencial de la compañía.

6.3.1. Consistencia con la clasificación de la información

Al trabajar de forma remota o en movimiento, los colaboradores y partes externas se aseguran que la información es manejada de manera coherente respecto a su clasificación asignada, y de acuerdo con lo establecido en esta política.

6.3.2. Lineamientos de seguridad sobre el entorno

WEARE DEV S.A.S establece las siguientes medidas de seguridad para proteger sus activos de información en cualquier tipo de entorno:

- ➔ Garantizar un nivel de privacidad adecuado y asegurar que personas externas no puedan ver documentos, archivos o pantallas en los que se pueda visualizar información confidencial.
- ➔ Implementar los lineamientos establecidos en el procedimiento de “WAD-Procedimiento de escritorio limpio” definida por la compañía.

6.4. Gestión de los recursos humanos

La gestión de los recursos humanos tiene como objetivo seleccionar a las personas más adecuadas, mantener e incluso reforzar sus competencias, conocimientos, habilidades y comportamientos éticos y garantizar la seguridad de la información de la compañía.
Para esto, WEARE DEV S.A.S realiza las siguientes actividades:

- ➔ Diseña e implementa un Procedimiento de Preselección y Selección de Personal que:
  - ◆ Valora el talento de las personas.
  - ◆ Respeta la igualdad de oportunidades y no promueven la discriminación de ningún tipo.

- ◆ Asegura que la selección de personal se realiza con base en los criterios profesionales del candidato y alineados a las necesidades reales de la organización.
- ◆ Cumple con la legislación laboral vigente.
- ◆ Garantiza la confidencialidad y protección de los datos personales.

➔ Realiza la investigación de los candidatos de acuerdo a las regulaciones aplicables para validar la información proporcionada en la solicitud de empleo, como lo puede ser:

- ◆ Los datos de identificación de la persona.
- ◆ Las referencias personales, familiares y laborales.

Y una vez seleccionados los candidatos adecuados, se diseña e implementa un Proceso de Contratación y Desvinculación de Personal que:

➔ Asegura el establecimiento de los términos y condiciones de la relación laboral en el contrato acordado con el colaborador, incluyendo aquellos relacionados con las sanciones administrativas, la desvinculación y la devolución de todos los activos provistos por la compañía completando y firmando el Formato de Devolución de Equipos.

- ◆ Puede ocurrir el caso en que personal interno o externo incurra en alguna desviación o incumplimiento de los lineamientos de seguridad establecidos por la compañía, lo cual será motivo de sanciones administrativas e incluso legales, las cuales quedan por escrito en los contratos celebrados. Esto involucra un proceso disciplinario que considera:

  - La identificación de la actividad o comportamiento inapropiado, o la violación de las políticas internas de la organización.
  - La investigación adecuada para determinar la causa y el impacto de lo ocurrido.
  - La definición de las acciones disciplinarias apropiadas a implementar, las cuales pueden incluir una advertencia verbal, por escrito, una suspensión temporal, una terminación del contrato, una acción legal o una combinación de estas medidas.
  - El registro y documentación de las acciones disciplinarias tomadas.
  - La detección de intentos o accesos a sitios web clasificados en categorías inapropiadas o restringidas

- ➔ Formaliza un compromiso de confidencialidad y lealtad con el colaborador para proteger la información de la compañía.
- ➔ Brinda la inducción y concientización pertinente a los colaboradores sobre sus responsabilidades de seguridad de la información y los riesgos asociados a sus funciones, así como también de la misión y visión de la compañía.
    - ◆ Para esto además implementa un programa anual de capacitación y concientización sobre seguridad de la información para todos los colaboradores, tanto internos como externos.
- ➔ Proporciona las políticas y procedimientos pertinentes que deben ser de conocimiento del colaborador para su lectura y comprensión.
- ➔ Entrega anualmente la política de seguridad de la información a toda la compañía para su lectura y comprensión.
- ➔ Otorga los accesos y permisos pertinentes de acuerdo al puesto asignado, siguiendo los lineamientos establecidos en esta política y el Procedimiento de Gestión de Accesos definido por la compañía.

6.5. Gestión y clasificación de los activos de información

Los activos de información de la compañía y los recursos que le dan soporte son identificados, inventariados y clasificados en función de los requerimientos del negocio y del programa de seguridad de la compañía.
WeAre Dev establece una adecuada gestión de sus activos y su clasificación, por medio de las siguientes acciones:

- ➔ La identificación y mantenimiento de un inventario de activos de información que abarca todos los dispositivos y medios extraíbles utilizados para las actividades de la compañía, ya sean de su propiedad o de los colaboradores.
- ➔ La asignación de propietarios de los activos de información.
- ➔ La clasificación de la información en función a sus niveles de confidencialidad, integridad y disponibilidad.
- ➔ El acceso, manejo y tratamiento adecuado de los activos de información acorde a su clasificación asignada.

WeAre Dev establece las siguientes categorías de clasificación:

- ➔ **Información confidencial o sensible:** Es aquella con el mayor nivel de importancia y/o custodia dentro de la organización. Su afectación puede traer consecuencias graves al negocio.
- ➔ **Información organizacional o interna:** Es aquella con un nivel de importancia y/o custodia moderada dentro de la organización.
- ➔ **Información pública:** Es aquella con un nivel de importancia y/o custodia mínimo e incluso nulo dentro de la organización.

La compañía realiza la clasificación de su información dentro de los registros del módulo de Activos de la plataforma Hackmetrix.

6.5.1. Etiquetado de los activos de información

La compañía realiza la clasificación de su información dentro de los registros del módulo de Activos de la plataforma Hackmetrix.

WeAre Dev SAS etiqueta sus activos de información con base en su clasificación asignada para identificarlos fácil y rápidamente.

Los métodos para el etiquetado de la información que pueden ser utilizados por la empresa son:

- ➔ **Versionado**, es decir indicando la clasificación de la información dentro del control de versiones que se encuentra en la documentación.
- ➔ **Marca de agua,** incluyendo en la documentación un sello o leyenda que indique su clasificación.
- ➔ **Encabezado o pie de página**, incluyendo en la parte superior o inferior dentro de la documentación la clasificación de la información correspondiente en todas las hojas que contenga.
- ➔ **Carpeta lógica**, etiquetando una carpeta creada dentro de un equipo de cómputo o dispositivo con la clasificación de la información que tendrán todos los archivos depositados en ella.
- ➔ **Diapositiva,** indicando la clasificación de la información en la primera diapositiva o portada del documento correspondiente.

Nota importante: Toda la información que no cuente con un etiquetado explícito será considerada como información organizacional.

6.5.2. Intercambio de información con partes externas

WeAre Dev implementa políticas, procedimientos y controles formales para proteger el intercambio de información a través de los distintos medios de comunicación y acorde con la clasificación de la información a intercambiar.
La compañía define los lineamientos del intercambio de información en su Política de Tratamiento de la Información.

6.5.3. Saneamiento/ Destrucción de activos y eliminación de información

WEARE DEV S.A.S reconoce la necesidad de sanear, destruir o eliminar los activos y la información que ya no se consideren necesarios para la organización.
Nuestra política de seguridad de la información se centra en salvaguardar la confidencialidad y privacidad de nuestros Colaboradores y clientes mediante un proceso de borrado seguro de información en dispositivos electrónicos. Esta política se aplica a todos los miembros del equipo que manejan datos sensibles y confidenciales. Buscamos garantizar que ningún dato sensible quede expuesto a riesgos de filtración o acceso no autorizado. Nuestro objetivo es cumplir con regulaciones y leyes de protección de datos, como GDPR, HIPAA y CCPA. Implementamos métodos como la sobreescritura múltiple de datos, el formateo seguro y la destrucción física de medios para garantizar la eliminación completa y confiable de datos. El borrado seguro ofrece ventajas en términos de cumplimiento normativo y protección de la confidencialidad, pero también presenta desafíos como el tiempo necesario y los costos asociados. La política incluye la importancia de seguir las mejores prácticas y la necesidad de capacitación continua para todo el personal.

La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se elimina de forma segura por medio de:

- ➔ Sobreescritura electrónica.
- ➔ Borrado criptográfico.
- ➔ Herramientas de borrado seguro que estén previamente autorizadas y configuradas correctamente.

➔ Eliminación de versiones, copias y archivos temporales de todas las ubicaciones donde se encuentren.

Además, define los siguientes métodos de saneamiento y destrucción para garantizar que la reutilización o eliminación de activos y la información contenida en ellos sea segura:

Tipo de activo de información	**Saneamiento (o borrado seguro)**	**Destrucción**
Papel	No aplica.	Triturado del papel
Dispositivos móviles	- Restablecimiento del dispositivo a estado de fábrica - Uso de cifrado con Sophos Device Encryption y posterior formateo del dispositivo	No aplica en casos del equipo ser reutilizado, en caso de daño del equipo se procede a realizar su disposición final con previa destrucción de placa base
Equipo de cómputo	- Sanear equipo de cómputo utilizando aplicativos de borrado seguro. - Desconfiguración de cuenta de correo y otros sistemas organizacionales. - Limpieza de exploradores (temporales, cookies, etcétera). - Formateo de equipo a bajo nivel	En ocasiones donde el equipo no será reutilizado, se hace destrucción de dispositivos de almacenamiento y posterior disposición final del elemento

7. Gestión de los riesgos de seguridad

La gestión de los riesgos de seguridad dentro de la organización tiene como objetivo facilitar la identificación y evaluación de los eventos potenciales que podrían provocar la pérdida, ya sea operativa o tecnológica, que afecten la confidencialidad, integridad y/o disponibilidad de la información.
Otro de sus objetivos es establecer y priorizar planes de tratamiento adecuados que minimicen el impacto de los riesgos dentro de las operaciones de la compañía.

WeAre Dev establece un proceso formal dentro de su Metodología de Gestión de Riesgos que contempla lo siguiente:

- ➔ El alcance del proceso de gestión de riesgos y su necesidad de adaptación al contexto más actual de la compañía.
- ➔ La implementación de métodos para la identificación y evaluación de los riesgos de seguridad de la información.
- ➔ El análisis y decisión de los planes de tratamiento de riesgo.
- ➔ La definición del umbral de tolerancia y los criterios de aceptación de los riesgos.
- ➔ La evaluación y aceptación del nivel de riesgo residual.
- ➔ La planificación y evaluación periódica de los riesgos, la cual se realiza por lo menos una vez al año o cuando ocurran cambios significativos dentro de la compañía.

WeAre Dev además garantiza que los riesgos de seguridad se abordan de manera efectiva en la gestión de proyectos y durante todo su ciclo de vida, considerando los siguientes aspectos:

- ➔ La evaluación y tratamiento de los riesgos de seguridad de la información debe realizarse en una fase temprana del ciclo de vida del proyecto y con revisiones periódicas.
- ➔ Se debe evaluar y monitorear el progreso y efectividad del tratamiento de los riesgos.

8. Gestión de los accesos

En el mundo actual, donde la seguridad de la información y la protección contra amenazas cibernéticas son de suma importancia, nosotros en WEARE DEV S.A.S entendemos la necesidad de proteger nuestros recursos de tecnología de la información (TI). Es por eso que hemos implementado una política de control de acceso de TI enfocada en la ciberseguridad, con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de nuestros datos. La razón detrás de esta política es asegurarnos de que solo el personal autorizado tenga acceso a los sistemas e información de nuestra compañía.

Al seguir principios como el otorgamiento del mínimo privilegio y la autenticación robusta, buscamos reducir los riesgos asociados con accesos no autorizados. En WEARE DEV S.A.S, reafirmamos nuestro compromiso con la seguridad de la información, reconociendo la importancia del control de acceso de TI para proteger nuestros activos. Nos preparamos para enfrentar los desafíos de seguridad cibernética con resiliencia y determinación, asegurando la continuidad de nuestras operaciones y fortaleciendo la confianza de nuestros clientes y partes interesadas.
Nuestro objetivo general es establecer un marco integral de control de acceso de TI que proteja nuestros recursos y datos contra amenazas cibernéticas, garantizando confidencialidad, integridad y disponibilidad. Nuestros objetivos específicos incluyen implementar políticas basadas en principios de seguridad reconocidos internacionalmente y reducir el riesgo de accesos no autorizados.

Esta política se aplica a todos los Colaboradores, contratistas, proveedores y terceros que acceden a nuestros sistemas y datos. Incluye aspectos como autenticación y autorización, gestión de identidades y privilegios, implementación de medidas de seguridad, supervisión y registro de actividades, formación y concienciación del personal, y revisión periódica de la política y procedimientos.

Nuestras acciones están guiadas por principios como el otorgamiento del mínimo privilegio, autenticación fuerte, supervisión y actualización. Nuestros procedimientos detallados abarcan desde identificación y autenticación hasta gestión de accesos. Además, hemos establecido responsabilidades claras para nuestro equipo de IT, gerentes, usuarios y gestión humana. Es importante tener en cuenta que el incumplimiento de estas políticas puede tener serias implicaciones

para la seguridad de nuestra información y la reputación de nuestra organización. Por lo tanto, tomaremos las medidas apropiadas para abordar cualquier violación y proteger los activos de WEARE DEV S.A.S.

Los siguientes controles son implementados y monitoreados para garantizar la actual política:

- **Control de autenticación robusta:** Implementar medidas de autenticación multifactorial para verificar la identidad de los usuarios antes de permitirles el acceso a sistemas críticos y datos sensibles.
- **Control de asignación de privilegios:** Aplicar el principio de menor privilegio para garantizar que los usuarios solo tengan acceso a los recursos y datos necesarios para realizar sus funciones laborales.
- **Control de revisión y actualización de accesos:** Realizar revisiones periódicas de los permisos de acceso asignados a usuarios para reflejar cambios en las funciones laborales y minimizar riesgos de seguridad.
- **Control de gestión de contraseñas:** Establecer un proceso de gestión de contraseñas que permita a los usuarios cambiarlas regularmente y garantizar su seguridad mediante técnicas de cifrado y almacenamiento seguro.
- **Control de supervisión y registro de actividades:** Implementar herramientas de supervisión de acceso y actividad para registrar todas las interacciones de los usuarios con los sistemas y recursos de TI.
- **Control de revisión y aprobación de solicitudes de acceso:** Establecer un proceso formalizado para solicitar nuevos accesos, modificar permisos existentes o revocar accesos no autorizados, gestionado por el departamento de IT o personal designado.
- **Control de comunicación de cambios en accesos:** Comunicar de manera oportuna cualquier cambio en los accesos asignados a los usuarios afectados, garantizando que estén informados sobre sus permisos y responsabilidades.
- **Control de concienciación y formación:** Implementar un programa de formación y concienciación sobre seguridad de la información y control de acceso de TI dirigido a todos los Colaboradores, contratistas y terceros.
- **Control de revisión de procedimientos:** Realizar revisiones periódicas de la política y los procedimientos para garantizar su efectividad y relevancia en un entorno cambiante de ciberseguridad.
- **Control de auditoría interna y externa:** Coordinar auditorías internas y externas para evaluar la efectividad de los controles de acceso de TI y garantizar el cumplimiento de las políticas de seguridad de la información.

9. Gestión de contraseñas e información de autenticación

En nuestro firme compromiso con la seguridad de la información, hemos creado la Política de Gestión de Contraseñas e Información de Autenticación para garantizar la protección adecuada de nuestros sistemas y recursos. Esta política se aplica a todos los miembros de nuestra comunidad, incluyendo colaboradores, contratistas, proveedores y terceros que acceden a los activos de nuestra organización.
Nuestro objetivo principal con esta política es salvaguardar la seguridad y confidencialidad de las contraseñas e información de autenticación. Al reducir el riesgo de accesos no autorizados, podemos proteger la integridad de nuestros datos y mantener la confianza de nuestros clientes y colaboradores.

- ➔ Las contraseñas deben cumplir con criterios de seguridad específicos, incluyendo longitud, complejidad y evitando información fácilmente identificable. Queda prohibido almacenarlas en medios inseguros como documentos no cifrados o correos electrónicos.
- ➔ Cada usuario debe tener una contraseña única para cada cuenta o sistema. Se recomienda el uso de autenticación multifactorial, especialmente para acceder a sistemas críticos o datos sensibles.
- ➔ Los usuarios deben cambiar sus contraseñas periódicamente según la política establecida. También deben cambiarlas inmediatamente si se sospecha que han sido comprometidas.
- ➔ Se proporcionará formación regular sobre buenas prácticas de seguridad en el manejo de contraseñas. Los usuarios serán informados sobre los riesgos asociados con contraseñas débiles o compartidas, así como las consecuencias del incumplimiento de esta política.

La dirección de IT es responsable de implementar y hacer cumplir esta política. Los gerentes y supervisores deben asegurar que sus equipos cumplan con esta política. Los usuarios son responsables de cumplir con las directrices establecidas y de informar cualquier incidente de seguridad relacionado.
El incumplimiento de esta política puede resultar en medidas disciplinarias, incluida la suspensión o terminación del acceso a nuestros sistemas y recursos, dependiendo de la gravedad de la violación.

10. Gestión de la criptografía

La gestión de la criptografía tiene como objetivo proporcionar un nivel más alto de seguridad de la información para que ésta no pueda ser leída por personas no autorizadas.

Y para esto, WEARE DEV S.A.S utiliza métodos criptográficos que protegen la confidencialidad e integridad de su información, no solo durante su almacenamiento, sino también durante su transferencia y recepción.
Esta política establece los lineamientos para garantizar la protección de la información sensible almacenada en dispositivos mediante la implementación del cifrado de discos utilizando Sophos Device Encryption utilizando además los métodos que son aplicados en los siguientes elementos:

- ➔ Credenciales de accesos.
- ➔ Información compartida por medios no oficiales como correos electrónicos
- ➔ Información y repositorios de backups.
- ➔ Información interna restringida para la mayoría de los colaboradores.
- ➔ Bases de datos.
- ➔ Registros de usuarios.
- ➔ Información de carácter personal.

Además, para ejecutar un protocolo de seguridad de criptografía eficiente, WEARE DEV S.A.S considera lo siguiente:

- ➔ El establecimiento y gestión de las claves públicas y privadas, lo cual se realiza siguiendo el Procedimiento de Gestión de Claves Públicas y Privadas definido por la compañía.
- ➔ La autenticación de los usuarios.
- ➔ La aplicación de cifrado de mensajes y métodos de no repudio.

La organización establece que los métodos criptográficos a implementar son:

Activo de información	Método criptográfico	Especificaciones

Página web de la compañía	Certificado	Protocolo de transferencia de hipertexto seguro (HTTPS)
Almacenamiento de información en la nube	Cifrado simétrico	AES
Accesos a plataformas en trabajo remoto.	VPN	OpenVPN
Mensajería por correo electrónico confidencial	Cifrado asimétrico	Estándar Open PGP
Cifrado de dispositivos	Cifrado AES256	Cifrado para almacenamiento extraíble y local

11. Gestión de la seguridad física

La gestión de la seguridad física tiene como objetivo proteger adecuadamente las instalaciones de la compañía y sus activos de información.

Para esto, WEARE DEV S.A.S implementa las siguientes medidas de seguridad:

- ➔ Perímetro de seguridad física de las instalaciones y oficinas de la organización, considerando la protección contra amenazas externas y ambientales.
- ➔ Las instalaciones y oficinas de la compañía cuentan con los señalamientos pertinentes de seguridad para identificar salidas de emergencia, rutas de evacuación, extintores, etcétera.
- ➔ Las instalaciones y oficinas de la compañía son monitoreadas continuamente con herramientas como videovigilancia, guardias de seguridad y alarmas.
- ➔ Controles de acceso físico que generan registros de las entradas y salidas de colaboradores y visitantes.

- ◆ Estos registros contienen fecha, hora de entrada y de salida, y en caso de ser proveedores o visitantes, el motivo de visita.

➔ Tanto los colaboradores como los visitantes deben portar una identificación visible mientras se encuentren en las instalaciones de la compañía.
➔ Aseguramiento de los activos de información, oficinas, instalaciones y centros de procesamiento de datos de la compañía con accesos biométricos, credenciales de acceso y/o puertas con códigos de acceso.
➔ Mantenimiento periódico del suministro de electricidad y agua, de los servicios de telecomunicaciones, alcantarillado, ventilación, aire acondicionado, etcétera.
➔ Designación de áreas para entrega y carga de material.
➔ Seguridad en el cableado estructurado.
➔ Mantenimiento periódico de los equipos y los procedimientos adecuados para autorizar su retiro de las instalaciones de la compañía.
- ◆ El mantenimiento de los equipos solo es realizado por personal autorizado.

➔ Separación de las instalaciones de procesamiento de información de las demás áreas de la compañía.

12. Gestión de la tecnología y las operaciones

La gestión de la tecnología y las operaciones considera todos los procesos operativos con el objetivo de garantizar la implementación de la seguridad de la información en las operaciones y servicios del negocio.
WEARE DEV S.A.S establece los lineamientos para estos procesos dentro de la Política de Tecnología y Operaciones de TI.

13. Gestión de la seguridad en los sistemas y aplicaciones

La gestión de la seguridad en los sistemas, aplicaciones, plataformas o cualquier otra herramienta usada por la compañía tiene como objetivo implementar y controlar la seguridad en todos los entornos que soportan los servicios y operaciones del negocio.
Y para esto, WEARE DEV S.A.S implementa, configura y utiliza los siguientes sistemas:

➔ Servicio de seguridad en correos electrónicos: Sophos Email Gateaway
➔ Antimalware: Sophos intercept X Advanced with MDR

- ➔ Antivirus: Sophos intercept X Advanced with XDR
- ➔ Firewall: Mikrotik

La correcta instalación y configuración de los sistemas mencionados anteriormente abarcan los siguientes elementos:

- ➔ Sistemas operativos.
- ➔ Redes y dispositivos de red.
- ➔ Estaciones de trabajo y dispositivos móviles.
- ➔ Sistemas de almacenamiento.
- ➔ Bases de datos.
- ➔ Correo electrónico e internet.
- ➔ Aplicaciones en general.
- ➔ Aplicaciones web.
- ➔ Soluciones de seguridad.
- ➔ Sistemas, servicios y aplicaciones de nube.

Además, WEARE DEV S.A.S implementa las medidas de hardening proporcionadas por los proveedores y las contenidas en la Documentación de Hardening de la organización.

Esto permite:

- ➔ La detección de programas informáticos no autorizados.
- ➔ La detección de sitios web maliciosos o sospechosos.
- ➔ La reducción de explotación de vulnerabilidades técnicas.
- ➔ La validación automatizada y periódica de los sistemas utilizados en los procesos críticos de la organización.
- ➔ El escaneo de archivos, datos, descargas, páginas web, etcétera para validar que no sean maliciosos.

Los lineamientos que se aplican a nivel de sistema operativo y de aplicaciones se encuentran definidos en la Política de Seguridad por Capas de la compañía.

13.1. Filtrado web

WEARE DEV S.A.S gestiona y restringe el acceso a todos sus colaboradores y personal externo que trabaje con activos y/o información de la organización de los siguientes tipos de sitios web para reducir y evitar la exposición a contenido malicioso:

- ➔ Sitios que tienen una función de carga de información que no está autorizada por la organización.
  - ◆ La carga de información a sitios web debe estar justificada por razones comerciales válidas.
- ➔ Sitios maliciosos conocidos o sospechosos que distribuyen malware o contenido de phishing.
- ➔ Servidores de mando y control.
- ➔ Sitios maliciosos identificados a partir de inteligencia de amenazas (ver sección 3.21 Gestión de la inteligencia de amenazas de seguridad).
- ➔ Sitios web que comparten contenido ilegal.

- ➔ Sitios clasificados en categorías inapropiadas, tales como:
  - ◆ Contenido para adultos.
  - ◆ Servicios de anonimización como proxies, VPNs o túneles no autorizados.
  - ◆ Juegos de azar en línea.
    - ◆ Drogas
    - ◆ Phishing
    - ◆ Hacking
    - ◆ Alcohol y tabaco
      - ◆ Sitios de mensajería no requeridos para fines laborales.
      - ◆ Cualquier otra categoría que represente un riesgo para la seguridad o que no esté alineada con los intereses de la organización.

13.2. Gestión de los registros de eventos (logs)

La gestión de los registros de eventos también llamados logs, tiene como objetivo registrar y monitorear las actividades realizadas en los sistemas de información de la compañía para la detección de acciones inusuales o accesos no autorizados a tiempo que permitan la prevención de incidentes de seguridad.

WEARE DEV S.A.S establece los lineamientos para esto en la Política de Gestión de Logs y aplica las acciones definidas en el Procedimiento de Gestión de Logs.

14. Gestión de las vulnerabilidades técnicas

La gestión de vulnerabilidades técnicas tiene como objetivo revisar constantemente los sistemas de información para identificar vulnerabilidades y posibles brechas de seguridad que puedan ser explotadas para perjudicar a la organización, y de esta manera dar solución a ellas en el modo y momento adecuado.
Dado esto, WEARE DEV S.A.S establece lo siguiente:

- ➔ Se realiza Ethical Hacking periódicamente
- ➔ El Procedimiento de Gestión de Vulnerabilidades establecido por la compañía contempla:
  - ◆ La verificación periódica de la publicación de vulnerabilidades por parte de los fabricantes de tecnología.
  - ◆ La realización periódica de escaneos de vulnerabilidades.
  - ◆ La priorización de atención para las vulnerabilidades con respecto a su criticidad e impacto.
  - ◆ La definición de plazos para reaccionar y dar resolución a las vulnerabilidades técnicas reportadas o identificadas.
  - ◆ La generación de un plan de remediación con plazos establecidos y su seguimiento.
  - ◆ La validación de la remediación por medio de retest de vulnerabilidades.
- ➔ Para mitigar la explotación de posibles vulnerabilidades se deben mantener los sistemas actualizados en sus últimas versiones, incluyendo la instalación de los parches pertinentes.
- ➔ La instalación de software en dispositivos propiedad de la compañía debe limitarse a actualizaciones y parches de seguridad. No se permite la instalación de nuevo software para uso personal y cuya procedencia es desconocida o sin licencia.

15. Gestión de la seguridad en las redes

La gestión de la seguridad en las redes tiene como objetivo proteger la información y el tráfico de datos transmitidos por redes internas o externas, y para ello WEARE DEV S.A.S implementa las siguientes medidas:

- ➔ Se restringen las conexiones con redes que no sean confiables.
- ➔ Se segregan en distintas redes los servicios, usuarios y sistemas de información de la compañía.
- ➔ El acceso público directo entre internet y los sistemas de la organización se realiza solo por medio de una VPN.
- ➔ Se aplican medidas de seguridad para la protección de la información transferida por medio de la mensajería electrónica contra acceso no autorizado, asegurando el correcto direccionamiento, usando canales de comunicación seguros y garantizando la disponibilidad e integridad de la información.
- ➔ Se documentan, comunican e implementan una Política de Tratamiento de la Información y un Procedimiento de Transferencia de Información por Medios Extraíbles para administrar los equipos de red, los medios extraíbles y las transferencias de información.
- ➔ Se documenta, comunica e implementa una Política de Seguridad por Capas donde se establecen las medidas aplicadas a nivel de red.
- ➔ Las transacciones en la página web de la organización se ejecutan de manera segura utilizando los protocolos de seguridad pertinentes.
    - ◆ Algunos de los protocolos aplicados son el uso de certificados, firma electrónica, autenticación de usuarios, protocolos de cifrado de comunicaciones entre las partes involucradas, etcétera.

16. Gestión del ciclo de vida del desarrollo

La gestión del ciclo de vida del desarrollo tiene como objetivo mantener un control adecuado de los cambios y adecuaciones, así como del mantenimiento e implementación de medidas de seguridad durante todas las fases que contempla el desarrollo de software.
Para esto, WeAre Devaplica las siguientes acciones:

- ➔ Se cuenta con una segregación de ambientes para el desarrollo, pruebas y producción con el fin de minimizar los riesgos latentes en los procesos de gestión de cambios. Además, se definen los requisitos para el paso entre cada uno de los ambientes y los derechos de usuario responsables de ello.
  - ◆ Para la ejecución de las pruebas, no se utilizan datos productivos de clientes.
- ➔ Se documenta, comunica e implementa una Política de Desarrollo Seguro donde se establecen los lineamientos de seguridad pertinentes.
- ➔ Se documenta, comunica e implementa una Metodología de Ciclo de Vida de Desarrollo donde se establecen todas las actividades y controles de seguridad realizados por la compañía durante el desarrollo.
- ➔ Se documenta, comunica e implementa un Procedimiento de Gestión de Cambios Productivos donde se establece el proceso formal para el control de los cambios aplicados en los pasos a producción.
  - ◆ Los lineamientos establecidos para la gestión de cambios productivos se encuentran dentro de la Política de Tecnología y Operaciones de TI.

17. Gestión de las relaciones con los proveedores

La gestión de las relaciones con los proveedores tiene como objetivo asegurar un nivel apropiado de calidad y seguridad en los servicios y/o productos obtenidos por partes externas, así como garantizar la seguridad de los activos e información de la compañía a los que tienen acceso.

Para esto, WeAre Dev implementa las siguientes medidas:

- ➔ Se mantiene una lista de los proveedores de la compañía y se realiza una evaluación semestralmente y anualmente de sus servicios, la cual se documenta en la Matriz de Evaluación de Proveedores.
  - ◆ Esta evaluación proporciona información relevante para la toma de decisiones sobre la contratación y/o renovación de proveedores, y para las evaluaciones de riesgo de la organización.
- ➔ Se cuenta con un contrato por escrito con cada proveedor, el cual incluye sus responsabilidades asociadas a la seguridad de la información y acuerdos de confidencialidad y el compromiso de cumplir con las políticas de seguridad de la información de WeAre Dev.
- ➔ El contrato también define los acuerdos de niveles de servicio, las responsabilidades legales y derechos de propiedad intelectual vigentes, y las regulaciones de protección de la información de carácter personal.
- ➔ Se definen los requerimientos mínimos de seguridad para proteger la información según su clasificación asignada, y el tipo de acceso y permisos a otorgar con base en las necesidades del proveedor y del negocio.
- ➔ Se le comunican las políticas y procedimientos operativos aplicables al proveedor para cumplir con todos los requisitos de seguridad establecidos por la compañía.
- ➔ Se gestiona adecuadamente la comunicación y el impacto de los posibles cambios que puedan presentarse en los contratos con proveedores, en sus servicios o cualquier aspecto dentro de la organización que afecte directa o indirectamente la relación con ellos.
- ➔ Se solicita al proveedor la comunicación y propagación de los requisitos de seguridad de WeAre Dev a lo largo de la cadena de suministro, en caso de que subcontraten y/o adquieran productos y/o servicios de otras partes externas para la prestación de su propio servicio.
- ➔ Se solicita al proveedor información relacionada a seguridad, configuraciones y buenas prácticas para el uso correcto de su producto y/o servicio.

17.1. Servicios de nube

Además de los lineamientos previamente establecidos para la gestión de las relaciones con los proveedores, que también aplican a los proveedores de

servicios en la nube, WeAre Dev establece los siguientes criterios para implementar adecuadamente la seguridad en los servicios de la nube.

Criterios generales

- ➔ El uso de servicios en la nube debe ser exclusivo para el cumplimiento de las funciones laborales de cada colaborador.
  - ◆ No está autorizado el uso de servicios en la nube para fines personales.
- ➔ Está prohibido el uso de los servicios de correo electrónico y almacenamiento en la nube con fines personales que no tengan que ver con la compañía.
  - ◆ Se debe tener activado el filtro antispam para asegurar que los correos maliciosos son identificados y que no lleguen a la bandeja de entrada, así como también se debe instalar una tecnología de cifrado y firma digital para proteger la información confidencial y asegurar la autenticidad de la compañía como remitente en los correos electrónicos.
- ➔ Se debe verificar y dar mantenimiento a las redes creadas sobre la infraestructura del proveedor de servicios de nube.
- ➔ Se debe realizar monitoreo a los logs de transferencia de datos hacia la nube.
- ➔ Los procesos no deben ejecutarse en una nube virtualizada de alguno de los múltiples inquilinos de los servicios de la compañía.
- ➔ Si se requiere el almacenamiento de información clasificada como reservada, sensible o confidencial y/o información de carácter personal, ésta debe permanecer cifrada para evitar su divulgación o acceso no autorizados.
- ➔ Al contratar servicios en la nube se debe validar la protección de los datos en tránsito, incluyendo:
  - ◆ Los datos que se mueven desde la infraestructura tradicional a los proveedores de nube, incluyendo público/privado, interior/exterior y otras combinaciones.
  - ◆ Los datos que migran entre los proveedores de nube.
  - ◆ Los datos que se mueven entre instancias (u otros componentes) en una nube determinada.

Criterios relacionados a los riesgos de seguridad

- ➔ En los procesos de contratación y uso de servicios en la nube se deben identificar, evaluar y gestionar los riesgos de seguridad asociados al tratamiento de información, acceso a información personal, riesgos legales, técnicos, de continuidad y todos los asociados a la transmisión de información por medio de la nube.

- ➔ Al contratar servicios de nube se deben contemplar y tratar los riesgos de pérdida de continuidad, disponibilidad e integridad por fallas en las plataformas para generar los procesos de recuperación correspondientes.
- ➔ No se deben utilizar servicios en la nube cuyo análisis de riesgo indique niveles no tolerables para la organización.
    - ◆ Los resultados del análisis y evaluación de riesgos son determinantes para aceptar o rechazar el uso de servicios en la nube, ya sean de pago o gratuitos.

Criterios relacionados a las capacidades, respaldos y gestión de cambios

- ➔ Los servicios de nube deben cumplir con los lineamientos de capacidad, respaldos y gestión de cambios establecidos en la Política de Tecnología y Operaciones de TI de la compañía.
- ➔ Los servicios de nube deben ser incluidos en el Procedimiento de Gestión de Backups, y Procedimiento de Gestión de Cambios Productivos establecidos por la compañía para que cumplan con todos los requisitos de seguridad pertinentes.
- ➔ Los cambios deben aprobarse siguiendo el Procedimiento de Gestión de Cambios Productivos y con la utilización de sandbox y pistas de lanzamiento.
- ➔ La compañía recibe notificaciones sobre los cambios sustanciales que el proveedor realiza y que afecten al cliente en la forma en que se entrega el servicio.

18. Gestión de incidentes de seguridad

La gestión de incidentes de seguridad tiene como objetivo llevar un adecuado análisis, registro y tratamiento de los incidentes de seguridad que puedan afectar las operaciones o servicios de la compañía.

Para esto, WEARE DEV S.A.S define los siguientes lineamientos:

- ➔ Todos los colaboradores, clientes y proveedores deben reportar a la organización la identificación de posibles incidentes de seguridad y la ocurrencia de ellos.
- ➔ Se deben analizar, definir y registrar soluciones para todo incidente de seguridad reportado o detectado, siguiendo el Procedimiento de Gestión de Incidentes de Seguridad establecido por la compañía.

- ➔ Se deben asignar a los responsables más adecuados para atender y resolver los incidentes de seguridad y otras posibles vulnerabilidades detectadas.
- ➔ Se debe registrar toda la información relevante sobre los incidentes de seguridad, incluyendo su impacto, frecuencia y forma de resolución aplicada.
    - ◆ Esto tiene como objetivo recolectar datos sobre su comportamiento y crear una base de conocimiento a la que se pueda consultar ante la ocurrencia de eventos similares en el futuro.

Adicionalmente, la organización habilita un canal de comunicación por medio de correo a los siguientes destinatarios para denunciar de manera anónima cualquier violación a las políticas de seguridad de la organización, o cualquier anomalía que pueda generar un incidente de seguridad.

- soporte@soinfco.com
- itdirector@wearedev.co

19. Gestión de la continuidad del negocio

La gestión de la continuidad del negocio tiene como objetivo asegurar que las operaciones de la compañía se mantengan funcionando adecuadamente aún durante eventos de crisis o de desastre.

Para esto, WEARE DEV S.A.S define los siguientes lineamientos:

- ➔ La documentación, comunicación e implementación de planes de continuidad y recuperación ante desastres que garanticen la restauración de los servicios o elementos interrumpidos por eventos inesperados, y su correcto funcionamiento una vez levantados.
- ➔ La asignación de los responsables adecuados, con el conocimiento y capacitación pertinentes para la ejecución adecuada de los planes definidos por la compañía.
- ➔ El aseguramiento de los recursos necesarios para la ejecución adecuada de los planes ante un evento inesperado.
- ➔ El mantenimiento de los planes, considerando la aplicación de pruebas y la mejora continua, siguiendo los lineamientos establecidos en el Plan de Recuperación ante Desastres y el Plan de Continuidad definidos por la compañía.

20. Gestión del cumplimiento

La gestión del cumplimiento tiene como objetivo mantener a la compañía alineada a las diferentes regulaciones y normativas a las que está sujeta.

Para esto, WEARE DEV S.A.S realiza lo siguiente:

- ➔ Identifica y documenta los requisitos, regulaciones y normativas aplicables al giro de negocio y a la compañía en general dentro de la Matriz de Evaluación de Requisitos Legales y Contractuales.
- ➔ Verifica que los acuerdos con los colaboradores, clientes y proveedores cumplan con las pautas de las regulaciones aplicables, así como también que se identifiquen los riesgos de seguridad de la información derivados del servicio prestado o asociados a la relación con cada una de estas partes.
- ➔ Establece las políticas y procedimientos necesarios para adherirse a los requisitos regulatorios y normativos.
- ➔ Realiza revisiones de cumplimiento y auditorías internas del SGSI de manera anual.

21. Gestión de la inteligencia de amenazas de seguridad

WEARE DEV S.A.S implementa la inteligencia de amenazas para la examinación y análisis de datos e información relevante sobre posibles nuevas amenazas y vulnerabilidades, lo cual aporta valor en la toma de decisiones sobre el control de ellas, saber cómo prevenirlas, detectarlas y remediarlas a través del servicio de SOC que provee Sophos MDR.
Esto se realiza siguiendo el Procedimiento de Gestión de Inteligencia de Amenazas establecido por la organización, y tiene los siguientes objetivos:

- Mejora de procesos internos.
- Implementación de una gestión de riesgos de seguridad más eficiente que genere decisiones más sólidas e informadas.
- Mayor comprensión de los puntos débiles de la organización que permita la priorización adecuada de las decisiones a tomar.
- Amplio conocimiento en las amenazas que apoye la proactividad y la aplicación de medidas preventivas que impidan la ocurrencia de un ciberataque.

La información obtenida como resultado de la inteligencia de amenazas debe ser compartida en un formato comprensible a todas las personas pertinentes, partes

interesadas e incluso con otras organizaciones para mejorar los procesos y sus resultados.

22. DESCRIPCIÓN DE LA POLÍTICA

WeAre Dev comprende la importancia que tiene un eficaz manejo de la información documentada y se compromete a con la aplicación de la política y sus lineamientos en seguridad de la información, por el cuál desea que todas sus partes interesadas tengan certeza que se realiza un adecuado tratamiento, acceso, distribución, conservación y protección de la información.

Por medio de la cual determina los lineamientos para garantizar el eficaz manejo de la información documentada de WeAre Dev y aplica para todos sus colaboradores.

<u>Gestión de activos</u>

- El área administrativa deberá realizar semestralmente la verificación y actualización de los activos de información.
- El área administrativa deberá clasificar sus activos de acuerdo al impacto que tengan en sus operaciones.
- El permiso de uso de medios removibles tales como USB, tarjetas SD entre otros únicamente está permitido para los siguientes casos:

    - Cuando se requiera extraer información de códigos fuentes, documentos corporativos, información sensible de la compañía y no se cuente con acceso alguno al drive o al correo electrónico corporativo, y sea necesario presentarla a una parte interesada.

      Para dichos casos el colaborador se debe dirigir al líder administrativo y deberá validar el caso pertinente y asignará al analista de TI para realizar la apertura de los puertos.

- Todos los colaboradores una vez se retiren de la compañía deberán hacer entrega de todos los activos que le fueron suministrados, tales como equipos de cómputo, teclado, mouse, USB, celulares, sillas, escritorios, diademas, descansa pies, ventiladores y demás activos que se tengan asignados.

Control de acceso

- En el archivo de “Matriz de activos” reposarán los datos correspondientes a: área, CECO, correos, usuarios, contraseñas, número de licencia Windows, número de licencia office, estado de antivirus y/o cualquier otra información u observación referente a datos destinados para cada colaborador en términos de seguridad de la información.
- Los usuarios y las contraseñas asignadas a cada colaborador son personales e intransferibles, y por ningún motivo deben prestarse, compartirse o divulgarse.
- Las contraseñas deberán ser cambiadas por cada colaborador semestralmente y se deberá informar al área administrativa y financiera el cambio de estas.
- El acceso a la información se llevará de manera planificada, haciendo uso del archivo “matriz de activos” donde se establecerá qué colaboradores tendrán acceso a la información pertinente a cada proceso de acuerdo a la estructura organizacional definida. Además, se deberá especificar en el archivo de estructura documental el tipo de permisos que tiene el colaborador, bien sea de lectura, de edición o revisión.
- Todos los colaboradores tendrán acceso a las páginas principales, y se bloquearán aquellas páginas web que no estén alienadas con la cultura de WeAre Dev.
- El acceso a la información de las partes interesadas y de WeAre Dev debe realizarse por los medios previstos y autorizados.

Retención y almacenamiento

- El almacenamiento de la información relacionada con el cliente deberá ser retenida durante 2 años.
- La información relacionada a las partes interesadas o de WeAre Dev debe ser almacenada en lugares determinados por el cliente o por la compañía, de acuerdo a los lineamientos que sean aplicables y tomando como referencia las políticas definidas.
- La información del cliente y de la compañía no debe ser divulgada por emails, mensajes adjuntos o cualquier otro medio en el que la compañía o el cliente no haya determinado.
- La compañía podrá disponer de los archivos eliminados treinta (30) días después de la eliminación en la siguiente ruta: Google Drive/Papelera. Después de los días nombrados la información será borrada permanentemente.
- WeAre Dev asegurará 1 BackUp al mes de la información albergada en las Unidades Compartidas con el fin de promover la conservación de la misma.

Privacidad y confidencialidad

- La política de la confidencialidad y tratamiento de datos personales será tratada de acuerdo a lo estipulado en la ley vigente (1581 del 2012).
- La información almacenada y tratada deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- El tratamiento de los datos personales sólo podrá ser tratado por personas autorizadas por el titular o de acuerdo a la norma vigente.
- Todos los colaboradores y clientes de WeAre Dev deben entender y firmar la cláusula de confidencialidad, que puede estar de manera independiente al contrato o inmersa en él.
- Todos los colaboradores que tengan una relación directa con los clientes deben aplicar y dar cumplimiento a las políticas de seguridad y confidencialidad del cliente.
- Se prohíbe la divulgación de la información de WeAre Dev tal como salarios, estrategias, tarifas comerciales, información financiera, metodologías, howknow. Dicha información debe permanecer confidencial.
- Toda la información que sea de naturaleza reservada debe guardarse y no debe ser comunicada, expuesta, compartida o divulgada por ningún medio, o cualquier tercero.
- La información que se derive de operaciones con el cliente, será considerada información sensible y su tratamiento está sujeto a los lineamientos del cliente y a los propios de WeAre Dev.
- En caso de pérdida de la información los colaboradores deberán reportar el evento ante el jefe inmediato, en caso de que pertenezca al cliente se llevaran a cabo los lineamientos establecidos por él, y si pertenece a WeAre Dev, debe ser escalado al líder del proceso administrativo y a su vez contar con el concepto jurídico de ser necesario.
- Todos los colaboradores de WeAre Dev deben mantener confidencialidad de toda la información a la que se tenga acceso, de cualquiera de las partes interesadas de la compañía.
- La información que sea confidencial y no sea necesaria para uso inmediato o posterior debe ser destruida.
- Todos los correos difundidos desde WeAre Dev deben contener la firma de cada colaborador junto al siguiente apartado: "En cumplimiento con nuestras políticas de seguridad de la información, le recordamos que toda la información contenida en este correo es confidencial y está destinada únicamente para el destinatario especificado. Cualquier divulgación, copia, distribución o uso no autorizado de esta información está estrictamente prohibido. Agradecemos su colaboración en la protección de la información y le exhortamos a tomar medidas de seguridad apropiadas para proteger su propia información confidencial."

- WeAre Dev abarca en su página web la política de privacidad de datos personales, la cual también se encontrará en las Unidades Compartidas Colaboradores WeAre Dev y Contratistas WeAre Dev

Seguridad

- La información debe tratarse evitando en todo momento la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Todas las personas que tratan la información de datos personales deben garantizar la reserva de la información.
- Todos los equipos de cómputo deberán contar con software antivirus, para asegurar la protección de la información.
- La información digital o física que se considere confidencial debe mantenerse debidamente salvaguardada y en ningún caso expuesta.
- Los dispositivos de seguridad otorgados por los clientes tal como tokens o tarjetas de acceso deben mantenerse en lugares seguros y bajo llave.
- No está permitido el almacenamiento de información que sea ilegal.
- No se permite extraer información de los equipos de cómputo a dispositivos móviles, tales como USB, discos duros, celulares u DVD´s, CD o cualquier otro dispositivo de almacenamiento.
- Todos los softwares que sean instalados en los equipos deben contar con las licencias legales adquiridas.
- Si se requiere instalar softwares libres, cada jefe inmediato deberá analizar la necesidad de instalación de acuerdo a las necesidades del proyecto en el que se encuentre.
- No se debe manipular el funcionamiento del software antivirus por ningún motivo.
- No se debe almacenar información personal en los equipos de cómputo, tales como fotos, aplicaciones, juegos etc.
- Si se ausenta del puesto de trabajo, los equipos de cómputo deben permanecer bloqueados.
- Los colaboradores no deben acceder a sitios web con contenido terrorista, pornográfico, violento o que viole políticas de derechos de autor.
- Si sospecha que el contenido de un correo es de dudosa procedencia, contiene información falsa o no le genera confianza por favor no acceder a él.
- La información que sea impresa y sea confidencial, por ningún motivo debe ser dejada en la impresora.
- Todos los equipos de cómputo utilizados para la operación de los servicios deben contar con restricción de acceso a los puertos USB, micro USB y tarjetas SD u otro sistema de almacenamiento.

Verificación

- El programa establecido para las auditorías internas deberá incluir la verificación de la aplicación de los lineamientos de seguridad de la información.
- La compañía podrá monitorear y verificar la aplicación de la política de la información y sus lineamientos.

Disponibilidad

- WeAre Dev contará con un plan de contingencia y continuidad con el que generará las actividades pertinentes para la prevención, preparación, respuesta y recuperación de la información documentada que soporta el sistema de gestión de la información.
- Los niveles de disponibilidad de los servicios e información acordados entre la compañía y cliente, proveedores y/o terceros se dispondrán de acuerdo a lo establecido contractualmente y a los tiempos de recuperación objetivos establecidos en el plan de contingencia y continuidad.
- La compañía proveerá en las oficinas de WeAre Dev el servicio de internet, que solo deberá ser utilizado para fines laborales.

Gestión de eventos

Pasos:

- Se deberá reportar inmediatamente ocurrido, todos aquellos eventos que afecten directamente la continuidad de la prestación de los servicios de la operación.
- Se deberá reportar los eventos a su jefe inmediato, y a su vez el jefe inmediato reportará el incidente al líder del proceso administrativo.
- Se utilizará el correo electrónico como medio para el reporte de incidentes.
- Una vez sea reportado el incidente, el líder del proceso administrativo deberá realizar el registro en la matriz ACPM y en caso de que se materialicen algunos de los eventos descritos en el plan de continuidad y contingencia se deberá activar el mismo.

Formación

- La alta dirección otorgará los recursos suficientes para el desarrollo de los programas, planes u otros, que sean necesarios para capacitar a los colaboradores acerca de los lineamientos de seguridad de la información.

- Debe ser responsabilidad de los colaboradores participar activamente de los espacios de formación sobre la seguridad de la información y cumplir a cabalidad con los lineamientos expuestos en el presente documento.

Excepciones

- Los colaboradores que presten servicios directamente al cliente, acatarán los lineamientos de seguridad de la información del tercero siempre y cuando dichos estándares abarquen más aspectos y condiciones en pro de la seguridad de la información.

23. CONTROL DE CAMBIOS

CONTROL DE DOCUMENTOS				
FECHA	**ELABORADO**	**REVISADO**	**APROBADO**	**CONTROL DE CAMBIOS**
30/11/2022	CEO	CEO	CEO	Versión 01
16/03/2023	Líder Administrativa(o) y Financiera(o)	Directora HSEQ	Directora HSEQ	Versión 02 actualización de excepciones y datos en matriz de control de seguridad de la información
13/03/2024	Analista IT	Líder TD	Directora HSEQ	Versión 03: Ampliación de nivel de detalle en cada componente de gestión de la política
26/07/2024	Analista IT	Líder TD	Directora HSEQ	Versión 04 Inclusión clasificación de la información
26/05/2025	Auxiliar TD	Líder TD	Directora HSEQ	Versión 05 actualización de contenido 6.4 gestión de los recursos humanos y 13.1 filtrado web