POLÍTICAS DE SEGURIDAD INFORMACIÓN, Y MEDIOS TECNOLOGICOS.

PEOPLE AND TRADE S.A.S

Tabla de contenido

1. INTRODUCCIÓN

La Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información.

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos.

Esta síntesis este documento tiene como finalidad dar a conocer las Políticas de Seguridad de la I, que deben aplicar y acatar los empleados y contratistas de ***PEOPLE AND TRADE S.A.S***, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

2. ALCANCE

Las políticas de seguridad informática, están orientadas a todos los usuarios y a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas, aplicadas y cumplidas por funcionarios de ***PEOPLE AND TRADE S.A.S*** como por los socios, contratistas, proveedores y agentes que apoyan directa o indirectamente la gestión y que utilicen la información generada y los equipos tecnológicos.

3. OBJETIVOS

Definir e implementar las políticas de seguridad informática que dan las pautas y directrices para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de ***PEOPLE AND TRADE S.A.S***, para su interiorización, aplicación y verificación permanente.

4. DEFINICIONES

Para los efectos del presente, se adoptarán las siguientes definiciones:

Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

Activos de Información: Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

Configuración Lógica: conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

Copia de respaldo o backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentesservicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Correo electrónico: Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

Dispositivos/Periféricos: Aparatos auxiliares e independientes conectados al computador o la red.

Espacio en disco duro: Capacidad de almacenamiento de datos en la unidad de disco duro.

Herramientas ofimáticas: Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Licencia de uso: Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Mantenimiento lógico preventivo: Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.

Mantenimiento físico preventivo: Actividad de impiez deelementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.

Medios de almacenamiento extraíble: Son aquellos soport de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Propiedad intelectual: Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.

Recurso informático: Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un Sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.

Servicio informático: Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

Servidor: Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos.

Software de gestión: Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada.

Software malicioso: Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.

UPS: Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

5. DOCUMENTOS DE REFERENCIA

a) Documentos de fundamentación Obligatoria:

Apartes de las mejores practicas de la norma ISO 27001:2022.

6. POLÍTICAS ORIENTADAS A USUARIOS

6.1. Gestión de activos de la Información:

a) Todos los empleados de planta o contratista que inicie labores en ***PEOPLE AND TRADE S.A.S***, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de Políticas de Seguridad Informática.

b) Los funcionarios que se desvinculen y los contratistas que culminen su vínculo contractual con ***PEOPLE AND TRADE S.A.S***, deberán hacer entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expedición de paz y salvo y/o liquidación de contrato.

c) Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a ***PEOPLE AND TRADE S.A.S***, por lo tanto, no se hará divulgación ni extracción de la misma sin previa autorización del Directivo competente.

d) No se realizará por parte de los funcionarios o contratistas copia no autorizada de información electrónica confidencial y/o software de propiedad o bajo licencia de ***PEOPLE AND TRADE S.A.S;*** El retiro de información electrónica perteneciente a ***PEOPLE AND TRADE S.A.S*** y clasificada como confidencial, se hará única y exclusivamente con la autorización del Directivo competente.

e) Ningún funcionario o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

f) Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

g) Al termino de cada contrato o convenio la información generada o compartida entre las partes deberá ser eliminada de forma segura del equipo asignado mediante herramientas que garanticen la no recuperación de la misma.

6.2. Gestión de Hardware y Software:

a) Se debe realizar el inventario de activos de tecnología y debe mantenerse actualizado cada vez que se realicen cambios en hardware o software.

b) Se deben asignar los activos de tecnología a los empleados o terceros necesarios para la ejecución de la labor contratada.

c) La instalación y desinstalación de software, configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal de *REPONSABLE DE TECNOLOGIA*, en el caso de ser un contratado con un tercero debe tener el acompañamiento y supervisión de *REPONSABLE DE TECNOLOGIA.*

d) El espacio en disco duro de los equipos de cómputo pertenecientes a ***PEOPLE AND TRADE S.A.S*** será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

e) Ningún funcionario o contratista podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la Gerencia.

f) Ningún funcionario o contratista podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

g) Ningún funcionario, contratista o tercero podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema de información, equipos de computo ni a la información allí contenida, o a una red de telecomunicaciones, salvo el personal autorizado de *REPONSABLE DE TECNOLOGIA* en aplicación de las políticas o medidas de seguridad.

h) No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de ***PEOPLE AND TRADE S.A.S*** para actividades que no estén relacionadas con las labores propias de La Entidad.

i) Los funcionarios y contratistas serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

j) Se deben mantener bloqueados en todos los computadores el acceso a todos los medios extraibles, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).

k) Se deben proteger los equipos con instalaciones de sistemas antivirus o suite de seguridad en funcionamiento, actualizado y debidamente licenciado.

6.3. Gestion de Cuentas de Acceso:

a) Todos los funcionarios y/o contratistas, deben tener un usuario de acceso al equipo de computo asignado y los sistemas de información dispuestos por la entidad, que amerite de acuerdo al cargo a ocupar.

b) Se debe establecer una matriz de roles y perfiles de acceso a la información.

c) El perfil de la cuenta de usuario a equipos de computo asignado a los funcionarios y/o contratista debe ser creado de acuerdo a los perfiles de acceso establecidos.

d) Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen.

e) Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con ***PEOPLE AND TRADE S.A.S***

f) Se deben inactivar las cuentas de usuarios de los empleados y/o funcionarios que terminen los vínculos labores y/o comerciales con la entidad.

g) Las contraseñas de acceso deben cumplir con los siguientes requisitos de complejidad:

h) La contraseña debe ser cambiada mínimo cada 30 dias, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

i) Se deben establecer mecanismos que permitan bloquear las cuentas al detectar ingresos erróneos de la contraseña.

j) Solamente puede solicitar cambio o restablecimiento de contraseña el funcionario o contratista al cual pertenece dicho usuario, o el jefe inmediato mediante solicitud enviada al correo electrónico del área del *REPONSABLE DE TECNOLOGIA*.

k) Todo funcionario o contratista que se retire de la Entidad de forma definitiva o temporal (superior a 3 dias), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

6.4. Uso de Unidades de Almacenamiento Extraíbles:

a) Los puertos USB de los equipos de los empleados deben ser bloqueados y/o restringidos para evitar la fuga de información.

b) Los funcionarios y contratistas que tengan información de propiedad de ***PEOPLE AND TRADE S.A.S*** en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

c) Toda información que provenga de un archivo externo a la Entidad o que deba ser restaurado tiene que ser analizado con la suite de seguridad vigente.

d) Con el fin de garantizar la confidencialidad e integridad de la información, ***PEOPLE AND TRADE S.A.S*** debe establecer sistemas y/o técnicas de cifrado para la protección de la misma, tanto en el servidor de archivos como en los medios usados en las copias de seguridad.

6.5. Correo Electrónico:

a) El correo electrónico corporativo es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de ***PEOPLE AND TRADE S.A.S***, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en ***PEOPLE AND TRADE S.A.S***,.

b) La información transmitida a través de las cuentas de correo electrónico corporativo no se considera correspondencia privada del empleado, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de ***PEOPLE AND TRADE S.A.S***

c) Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

d) Es responsabilidad del funcionario o contratista depurar su cuenta de correo periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

6.6. Internet:

a) No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Entidad.

b) El Servicio de internet provisto por ***PEOPLE AND TRADE S.A.S*** no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

c) No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la ***PEOPLE AND TRADE S.A.S*** o de las personas.

d) ***PEOPLE AND TRADE S.A.S*** se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet provistos.

6.7. Seguridad Física:

a) Es responsabilidad de los funcionarios y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con ***PEOPLE AND TRADE S.A.S,*** En caso de daño, pérdida o robo, se debe informar a la Gerencia General.

b) Los funcionarios y contratistas deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

c) Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas cerca o encima de de ellos.

d) Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

6.8. Derechos de Autor:

a) Ningún usuario, debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

6.9. Clasificación de la información:

a) Los documentos electrónicos resultantes de los procesos misionales y de apoyo de ***PEOPLE AND TRADE S.A.S***, se tratarán en base a la confidencialidad de la misma y el impacto para la Entidad en caso de pérdida o robo, asi:

- **Confidencial**: Acceso a la información que compete a la alta dirección.
- **Restringido**: Acceso a la información que compete a directores de área y empleados clave.
- **Interno**: Acceso a la información que compete a cualquier nivel jerárquico dentro la Entidad.
- **Público**: Todas las personas, dentro y fuera de la organización, tienen acceso.

b) Los activos de información asociados a cada sistema de información, serán identificados y clasificados por su tipo y uso siguiendo lo establecido.

6.10. Personal de Tecnologia:

a) El control de los equipos tecnológicos deberá estar bajo la responsabilidad de *REPONSABLE DE TECNOLOGIA*, así como la asignación de usuarios, claves y ubicación física.

b) *REPONSABLE DE TECNOLOGIA*, deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

c) *REPONSABLE DE TECNOLOGIA* será el encargado de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).

d) Las licencias de uso de software, instaladores (CD, cintas magnéticas u otros medios), manuales de usuarios, claves de acceso a consolas de administración y demas, estarán bajo custodia del gerente general.

e) *REPONSABLE DE TECNOLOGIA* es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del

programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

f) Todas las publicaciones que se realicen en el sitio WEB de ***PEOPLE AND TRADE S.A.S*** *www.peopleandtrade.com*, deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

g) El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. *REPONSABLE DE TECNOLOGIA* será la encargada de crear y asignar las cuentas de acceso y sus permisos, sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

h) La estandarización de los nombres de usuario estará compuesta de la siguiente forma: nombre del cargo, en caso de existir cargos con el mismo nombre o duplicidad, se usará un numero consecutivo al final del nombre.

i) Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los funcionarios o contratistas, debe aplicarse la inactivación del usuario al menos por 30 dias.

j) Sera el responsable de realizar la copia de seguridad a la información institucional y bases de datos, conforme a lo establecido en la política de copia de seguridad, así como en los casos extraordinarios: desvinculación de funcionario o contratista, envío de equipo para garantía, mantenimiento preventivo y/o correctivo de los equiposequipo.

k) Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Entidad, deberán ser salvaguardadas por *REPONSABLE DE TECNOLOGIA* en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

l) Sera el responsable de monitorear y mantener el estado de la suite de seguridad o sistema antivirus instalado en los equipos.

m) Es responsables de realizar mantenimiento lógico preventivo a los equipos de cómputo mínimo cada 3 meses y mantenimiento físico preventivo mínimo una vez por año, que incluya el cableado estructurado, igualemente deberá elaborar el plan de mantenimientos especificando un cronograma.

n) Se debera llevar control y registros de los mantenimientos lógicos y físicos, asi como también de los soportes ejecutados en cada equipo.

6.11. Directivos:

a) La Gerencia debe garantizar la capacitación a los funcionarios en el manejo del software de gestión, herramientas de ofimatica, plataformas y/o aplicativos implementados.

b) Deberá notificar a *REPONSABLE DE TECNOLOGIA* las novedades de vinculación y desvinculación de personal de ***PEOPLE AND TRADE S.A.S***, con el fin de crear o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

c) Deberan proveer las herramientas (Hardware, Software) necesarias en pro del mejoramiento continuo de los controles implementados para la seguridad de la información.

7. POLÍTICAS ORIENTADAS A LA CONTINUIDAD DEL NEGOCIO.

a) PEOPLE AND TRADE S.A.S, establecerá todas las medidas que estén a su alcance para que, en un tiempo óptimo, sus operaciones, clientes y partes interesadas continúen ejecutando los procesos y/o servicios críticos ante eventos desfavorables que afecten la continuidad de los mismos.

b) PEOPLE AND TRADE S.A.S, establece como premisa ante un incidente o catástrofe la preservación de la vida e integridad de sus empleados, contratistas y demás partes interesadas; y el restablecimiento de los servicios de manera priorizada de acuerdo con la criticidad para el negocio en un tiempo optimo.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

a) El portal web bajo el dominio *www.peopleandtrade.com* que posee la entidad y su contenido son propiedad de ***PEOPLE AND TRADE S.A.S,*** está prohibida su reproducción total o parcial, su traducción, inclusión, transmisión, almacenamiento o manipulación sin autorización previa y escrita de ***PEOPLE AND TRADE S.A.S***. Sin embargo, es posible la descarga material (texto, video, audio) relacionado al portal web y de sus redes, aplicaciones y/o servicios para uso personal, informativo, educativo, noticioso y no comercial, siempre y cuando se haga expresa mención de la propiedad intelectual de ***PEOPLE AND TRADE S.A.S.***

b) ***PEOPLE AND TRADE S.A.S*** no será responsable por el uso indebido que hagan los usuarios del contenido del portal web en cualquiera de las plataformas tecnológicas que dispone para su comunicación con externos, asi mismo no se responsabiliza por cualquier consecuencia derivada de incidentes o ataques de terceros a su infraestructura tecnológica y/o por alguna falla técnica o por cualquier exposición o acceso no autorizado, fraudulento o ilícito a su portal web y que puedan afectar la confidencialidad, integridad o disponibilidad de la información publicada o asociada con los contenidos y servicios que se ofrecen en este.

9. POLITICAS ORIENTADAS AL CIFRADO DE INFORMACION

Con el fin de garantizar la confidencialidad e integridad de la información, ***PEOPLE AND TRADE S.A.S*** debe proveer sistemas y/o técnicas de cifrado para la protección de la misma, tanto en los servidores de archivos como en los medios extraíbles usados en las copias de seguridad.

a) Directrices de seguridad para el área de Tecnologia.

- *El RESPONSABLE DE TECNOLOGIA* deberá configurar y administrar el sistema de cifrado, así como velar por el cumplimiento de la presente política y generar los reportes que se requieran.

b) Directrices de seguridad para el personal que trata la información

- Se deberán cifrar todas las unidades de disco en los equipos asignados a personal y/o terceros que tenga acceso a información confidencial y en particular los documentos importantes para la misión de la ***PEOPLE AND TRADE S.A.S***.

10. POLÍTICA DE ADMINISTRACIÓN DE COPIAS DE SEGURIDAD

a) Los documentos electrónicos resultantes de los procesos misionales y de apoyo de ***PEOPLE AND TRADE S.A.S***, se tratarán en base a la confidencialidad de la misma y el impacto que genere a la entidad en caso de pérdida o robo, así:

- **Confidencial**: Acceso a la información que compete a la alta dirección.
- **Restringido**: Acceso a la información que compete a directores de área y empleados clave.
- **Interno**: Acceso a la información que compete a cualquier empleado en cualquier nivel jerárquico dentro la empresa.
- **Público**: Todas las personas, dentro y fuera de la organización, tienen acceso.

b) Se deben establecer cronogramas para la realización periodica de las copias de seguridad.

c) Se deben establecer controles y registros sobre la realización de las copias de seguridad.

d) Se deben proteger los medios e información contenida en ellos, mediante mecanismos de cifrado fuertes.

e) Debera existir un responsable de los medios que contengan copias de seguridad.

f) Cada copia de seguridad realizada debe ser registrada con alguna nomenclatura que permita el control de las copias realizadas y facilite ubicación de los medios y futura restauración de la información en caso de desastre.

11. POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

a) El acceso de terceras personas a las instalaciones de ***PEOPLE AND TRADE S.A.S*** debe ser controlado y su ingreso a las diferentes dependencias debe ser autorizado por los funcionarios a cargo.

b) Se debe restringir el acceso directo a usuarios no autorizados al centro de telecomunicaciones en el cual esten ubicados los sistemas o equipos activos de red y/o servidores.

c) Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos activos de red y servidores.

d) Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

e) Se debe contar por lo menos con dos extintores de incendio adecuado y cercano al centro de telecomunicaciones.

f) Los equipos que hacen parte de la infraestructura tecnológica de ***PEOPLE AND TRADE S.A.S,*** tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

12. POLÍTICAS ENFOCADAS A LA MEJORA CONTINUA

a) Se realizarán auditorias internas al cumplimiento de las políticas a la cuales este documento hace referencia.

b) Se deben realizar revisiones periodicas al menos cada seis meses de los riesgos identificados y actualizarlos de acuerdo a la revisión.

c) Se deben desarrollar reuniones para evaluar y comentar los incidentes de seguridad con la Gerencia al menos cada seis meses.

d) Se debe realizar evaluaciones periodicas al cumplimiento de proveedores de servicios, al menos cada seis meses.

e) Se establecera un programa de formación, sensibilizacion y divulgación de este documento, sus futuras actualizaciones y/o modificaciones mediante diferentes medios de comunicación

f) Se deben establecer un programa de concientización sobre temas enfocados a la seguridad de la información y ciberseguridad, mediante diferentes actividades y medios de comunicación al menos cada tres meses.

13. CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

La *Gerencia General* de ***PEOPLE AND TRADE S.A.S***, los jefes de area y responsable de Tecnologia, son responsables de conocer, monitorear, mejorar y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

CONTROL DE CAMBIOS

VERSION	MODIFICACION	FECHA
1	Creación del documento	18/04/2025

REVISIONES Y APROBACIONES DEL DOCUMENTO

ELABORADO POR:	APROBADO POR:
Cristian Zuñiga R. *Ingeniero de Sistemas.* **Asesor de Tecnologia.**	**Yesika Campo V.** **Gerente General.**