POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Introducción.

Uno de los activos más valiosos para PEOPLE CONTACT es la información y a medida que los sistemas de información apoyan cada vez los procesos de misión crítica, se requiere contar con estrategias de alto nivel que permitan el control y la administración eficiente de los datos.

PEOPLE CONTACT, los sistemas y la red de información enfrentan amenazas de seguridad como: Fraude por computadora, espionaje, sabotaje, vandalismo, afectaciones naturales, robos, entre otras muchas que se han visto en creciente aumento. El crecimiento exponencial de los ataques por códigos maliciosos, ramsomware, phising y ataques de denegación de servicio hace que sean muy comunes en estos tiempos y cualquier empresa puede estar sujeta a este tipo de ataques.

Con la promulgación de la presente Política de Seguridad de la Información PEOPLE CONTACT formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales

1. Acerca de la Seguridad de la Información

La seguridad de la información se refiere a la práctica de proteger la **confidencialidad**, **integridad** y **disponibilidad** de la información frente a diversos riesgos, como accesos no autorizados, manipulación indebida o destrucción. El objetivo principal de la seguridad de la información es garantizar que los datos sensibles (tanto digitales como físicos) estén seguros y protegidos, de modo que las organizaciones puedan operar de manera eficaz y cumplir con las normativas y regulaciones aplicables. Dentro de los componentes clave de la seguridad de la información:

1. **Confidencialidad**: Garantizar que solo las personas autorizadas tengan acceso a la información. Esto implica limitar el acceso a los datos sensibles y protegerlos frente a accesos no autorizados o divulgaciones.

2. **Integridad**: Asegurar que la información sea precisa, completa y no haya sido alterada o manipulada de manera indebida. La integridad busca mantener los datos correctos y confiables durante todo su ciclo de vida.
3. **Disponibilidad**: Asegurar que la información esté accesible para los usuarios autorizados cuando la necesiten. Esto implica mantener los sistemas y datos operativos y funcionales en todo momento, minimizando interrupciones.

Para ello es necesario considerar aspectos tales como:

- **Autenticidad**: Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- **Posibilidad de Auditoría**: Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.
- **Protección a la duplicación**: Los activos de información son objeto de clasificación, y se llevan registros de las copias generadas de aquellos catalogados como confidenciales.
- **No repudio**: Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- **Legalidad**: Los activos de información cumplen los parámetros legales, normativos y estatutarios de la institución.
- **Confiabilidad de la Información**: Es fiable el contenido de los activos de información que conserven la confidencialidad, integridad, disponibilidad, autenticidad y legalidad.

2. Organización para la Seguridad de la Información

PEOPLE CONTACT garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, del cual hace parte integral esta política, la cual debe ser revisada y actualizada cada año.

Los líderes de dependencia o procesos hacen parte del grupo de responsables de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares.

3. Política de Seguridad de la Información

3.1. Objetivo

- Proteger, preservar y administrar objetivamente la información de PEOPLECONTACT junto con las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.

- Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la Empresa para asegurar su permanencia y nivel de eficacia

- Definir las directrices de PEOPLE CONTACT para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

3.2. Alcance

Esta política es aplicable a todos los empleados, contratistas, consultores y terceros que tengan acceso a los sistemas, redes o información de PEOPLE CONTACT. Se extiende a toda la infraestructura de Tecnología de la Información, equipos de comunicación, aplicaciones, datos y redes utilizadas por la organización.

3.3. Roles y Responsabilidades

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de PEOPLE CONTACT, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe

- **Equipo Directivo.**

El equipo directivo de PEOPLE CONTACT aprueban esta Política y son responsables de la autorización de sus modificaciones.

La Alta Dirección alineada con el equipo de tecnología serán los responsables de revisar y aprobar el texto de la Política de Seguridad de la Información, así como las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y la mejorara continua.

Así mismo será el responsable de coordinar las acciones para impulsar la implementación y el cumplimiento de la presente Política.

- **Departamento de Tecnología**

Será responsable de cumplir funciones relativas a la seguridad de los sistemas de información de la empresa, definidas dentro de la política de seguridad de la información.

Deben seguir los lineamientos de la presente política y cumplir los requerimientos que en materia de seguridad informática se establezcan para la operación, administración, comunicación y mantenimiento de los sistemas de información y los recursos de tecnología de PEOPLE CONTACT

- **Director de Talento Humano**

Será la responsable de notificar a todo el personal que se vincula contractualmente con la Empresa, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del Sistema de Gestión de la Seguridad de la Información. De igual forma, será responsable de la notificación de la presente Política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los Compromisos de Confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Calidad. De igual manera es responsable del control y seguimiento a las violaciones de la presente política de seguridad de la información.

- Director Jurídico

Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información

- **Director de planeación y mejoramiento continuo**

Es responsable de coordinar auditorías periódicas sobre los sistemas y actividades vinculadas con la gestión de activos de información y la tecnología de información. Es su responsabilidad informar sobre el cumplimiento e incumplimiento de las especificaciones y medidas de seguridad de la información establecida por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

- **Empleados**

Todos los empleados son responsables de proteger la información de la organización, seguir las políticas de seguridad, reportar incidentes de seguridad y usar la tecnología proporcionada de manera responsable y ética.

Los **propietarios de activos de información** (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de esta; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo con sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

Los **usuarios de la información** y de los sistemas utilizados para su procesamiento son responsables de conocer y cumplir la Política de Seguridad de la Información vigente

El incumplimiento de alguna o algunas de estas políticas por parte del empleado puede ser causal de terminación justificada del contrato de trabajo con PEOPLE CONTACT o con la temporal a la que se encuentre vinculado. “Validar cruzar reglamento interno de trabajo Articulo 55”

En caso de que se incurra en una falta grave PEOPLE CONTACT podrá entablar una demanda penal o civil cuando lo considere necesario y de acuerdo con la normatividad legal vigente.

Si se demuestran pérdidas económicas por causales de daños a los equipos por causa de mal uso de estos, los costos de reparación o de sustitución de estos serán cargados al empleado que así se le demuestre.

Para el desempeño de las funciones de los colaboradores PEOPLE CONTACT le proporcionará los recursos informáticos necesarios, los cuales deben ser cuidados, protegidos y aprovechados de una manera responsable y eficiente, siendo de carácter

confidencial y de buen manejo la información entregada por nuestros clientes, salvaguardándola y no comunicándola a personal no autorizado.

Sólo el personal autorizado (personal del área técnica) puede llevar a cabo cualquier tipo de mantenimiento tanto del hardware como del software y de la configuración de acceso a la red, al igual que las configuraciones de escritorio.

El usuario debe reportar cualquier tipo de daño del equipo tanto de hardware como de software por medio del aplicativo GLPI dispuesto por el área de soporte técnico para tal fin.

No se permite fumar, comer o beber mientras está en el puesto de trabajo. El almacenamiento de música, videos y películas en cualquier tipo de formato es una clara violación de los derechos de autor y una amenaza a la integridad, disponibilidad y confidencialidad de los equipos y la red, por lo cual está prohibida su grabación en los equipos de PEOPLE CONTACT.

PEOPLE CONTACT no se hará responsable por el almacenamiento y/o uso de información de carácter personal, que el empleado disponga en los equipos de cómputo de la empresa.

No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo que no sea un computador portátil fuera de la Compañía se requiere una autorización expresa del área de activos fijos. El retiro e ingreso de equipos portátiles se debe reportar al vigilante de cada sede.

Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

Cuando el usuario no esté en el puesto de trabajo, debe bloquear el equipo.

Nadie podrá solicitar restablecimiento de contraseña, apagar, ingresar o reiniciar un equipo (excluyendo los de los agentes de operación) sin previa autorización de la persona encargada de dicho equipo o en caso de ser urgente el uso del equipo, es necesario tener autorización por parte del jefe inmediato.

Los equipos personales asignados por PEOPLE CONTACT a cada empleado, deberán permanecer apagados fuera del horario de trabajo. Se debe solicitar autorización del jefe directo para dejar un equipo personal encendido en horario nocturno, fines de semana o periodos de vacacionales.

Solo se permitirá el acceso de computadores personales en caso de que las funciones del cargo lo requieran, para lo cual debe tener previa autorización del jefe inmediato y del responsable de tecnología.

Está prohibido el uso de cualquier medio extraíble (Disquetes, discos, USB, CD-ROM o cualquier otro medio de almacenamiento) sin que se tenga previa autorización, ya que estos son medio de transmisión de virus y fuga de información que puede ocasionar un incidente de ciberseguridad.

- **Responsabilidades de PEOPLE CONTACT**

Los procedimientos para modelar los perfiles del directorio activo y las características de cada uno de ellos deben ser mantenidos y actualizados por la dirección de tecnología.

El Reglamento Interno de Trabajo de la compañía debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

La empresa hará la entrega oficial del equipo de cómputo en funcionamiento, con el respectivo software instalado y con la licencia bien sea de pago o licencia GNU, de acuerdo con la actividad del usuario que trabaja en PEOPLE CONTACT.

Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

PEOPLE CONTACT define políticas de seguridad de la información, vela por su cumplimiento, sin embargo, es responsabilidad del personal el acatamiento de estas y las consecuencias a nivel interno y externo que sus actuaciones pueden generar

4. Gestión de la Información

4.1. Clasificación de la Información

La información de la organización será clasificada en diferentes niveles según su sensibilidad:

- **Pública:** Información que puede ser compartida con el público sin riesgo.

- **Interna:** Información para uso interno que no debe divulgarse fuera de la organización.
- **Confidencial**: Información sensible que solo debe ser accesible a un grupo limitado de personas.
- **Crítica:** Información cuya divulgación o pérdida podría causar graves perjuicios a la organización.

4.2. Identificación, clasificación y valoración de activos de información.

Cada dependencia debe elaborar y mantener un inventario de los activos de información que tengan a su cargo. Las características del inventario, donde se incorpore la clasificación, valoración, ubicación y acceso de la información, las especifica el área de mejoramiento continúo avalado por el representante por la dirección. Es responsabilidad del área de Tecnología garantizar la disponibilidad, integridad y confidencialidad de los datos que lo componen.

4.3. Seguridad de la información en el Recurso Humano

Todo el personal de PEOPLE CONTACT, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información y software asociado. El área de tecnología debe mantener un directorio activo completo y actualizado de tales perfiles.

Todo el personal de la Operación será monitoreado permanentemente tanto en las comunicaciones de voz, como los correos electrónicos y mensajes del chat que se tengan por los equipos y herramientas corporativas, ya que toda la información generada por estos medios pertenece a PEOPLE CONTACT S.A.S.

El **Representante de la Dirección** y/o el **Director de Tecnología** en conjunto con la **Dirección de Talento Humano** determina cuales son los atributos que deben definirse para los diferentes perfiles.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira o cambia de cargo, recae en el Líder de Área o a quien éste

designe; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

La política de seguridad Informática hace parte integral del contrato de trabajo suscrito entre la empresa y los diferentes trabajadores y en señal de aceptación suscriben documento mediante el cual acreditan que lo recibieron a satisfacción.

4.4. Protección de la Información

La información confidencial y crítica debe ser cifrada tanto en tránsito como en reposo. Se utilizarán protocolos seguros (por ejemplo, TLS/SSL para datos en tránsito y AES para datos en reposo).

4.5. Intercambio de Información con Organizaciones Externas.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por Control Interno, previa verificación por los propietarios de los activos de la información.

Toda la información institucional debe ser manejada de acuerdo con la legislación.

4.6. Copias de Seguridad

Toda información que pertenezca a la matriz de inventario de activos de la información de la compañía o que sea de interés para un proceso operativo o de misión crítica debe ser respaldada por copias de seguridad tomadas de acuerdo con los procedimientos. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.

El área de tecnología de PEOPLE CONTACT debe realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

Los registros de copias de seguridad deben ser guardados en el servidor.

El área de Tecnología debe tener las herramientas para administrar la información y registros de copias de seguridad.

Las copias de seguridad de información crítica deben ser mantenidas de acuerdo con cronogramas definidos y publicados por el Área de Tecnología para los roles interesados.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo con las políticas y estándares que para tal efecto elabore y se mantengan por parte delos responsables.

Las áreas de PEOPLE CONTACT tienen la responsabilidad de adoptar y cumplir las normas definidas para la creación y el manejo de copias de seguridad.

PEOPLE CONTACT no se hará responsable por el almacenamiento y/o uso de información de carácter personal, que el empleado disponga en los equipos de cómputo de la empresa.

4.7. Retención y Eliminación de Datos

La información será retenida solo durante el tiempo necesario para cumplir con sus fines. Después del periodo de retención, los datos se eliminarán de manera segura. Para eliminar datos sensibles, se utilizarán técnicas de borrado seguro o destrucción física, según corresponda.

5. Control de Acceso

5.1. Política de Acceso Mínimo

El acceso a los sistemas y a la información se concederá solo en función de las necesidades laborales de cada empleado, basándose en el principio de "mínimo privilegio". Cada empleado o contratista recibirá acceso únicamente a la información que necesite para desempeñar sus funciones.

Los procedimientos para modelar los perfiles del directorio activo y las características de cada uno de ellos deben ser mantenidos y actualizados por la dirección de tecnología.

El acceso a sistemas de cómputo y los datos que contienen es responsabilidad exclusiva del personal encargado de tales sistemas. PEOPLE CONTACT debe propender por

mantener al mínimo la cantidad de cuentas de usuario que el personal y terceros deben poseer para acceder a los servicios de red

5.2. Gestión de Identidades

Cada empleado o contratista debe contar con una identificación única (ID de usuario) para acceder a los sistemas. El uso compartido de cuentas está prohibido, y las credenciales deben mantenerse seguras en todo momento.

Cuando un usuario recibe una nueva cuenta, declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta. El área de Tecnología enviará todas las recomendaciones y políticas a la cuenta de correo del colaborar cuando sea entregada la misma.

La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el jefe inmediato de la persona que solicita y el director de tecnología.

No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de los sistemas.

Se prohíbe el uso de cuentas anónimas o de invitado (Guest) y todos los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas Unix/Linux no deben entrar inicialmente como "Root", sino primero empleando su propio ID y luego mediante "Set Userid" para obtener el acceso como "Root". En cualquier caso, debe registrarse en la bitácora todos los cambios de ID.

Toda cuenta del dominio quedará automáticamente suspendida después de 60 días de inactividad.

El área de Tecnología debe elaborar, mantener y actualizar el procedimiento y las guías para la correcta definición, uso y complejidad de claves de usuario.

El proceso administrativo y disciplinario en caso de suplantación a través de clave de acceso del personal de tecnología o de aquellos que conozcan los claves de otras personas en el desarrollo de su labor será más estricto a conllevará mayores sanciones.

Como requisito para la liquidación contractual del personal de la Empresa, las áreas de Tecnología, Talento Humano, activos fijos y Nómina deberán firmar el certificado de paz y salvo.

5.3. Autenticación

El control de las contraseñas de red es responsabilidad del Área de Tecnología. Dichas contraseñas deben ser codificadas y almacenadas de forma segura. Las claves de administrador de los sistemas deben ser conservadas por el Área de Tecnología y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie

Se deben utilizar contraseñas seguras para el acceso a todos los sistemas de PEOPLE CONTACT, cumpliendo con los siguientes requisitos:

- Longitud mínima de 8 caracteres.
- Uso de caracteres alfanuméricos y especiales y uso de mayúsculas y minúsculas.
- Cambio obligatorio de contraseñas cada 60 días.
- No debe contener el nombre del usuario.
- Al momento de cambiarla no debe haber sido utilizada en al menos 12 veces anteriores la misma contraseña
- Luego de 5 intentos fallidos la cuenta se bloqueará

El control de las contraseñas de red es responsabilidad del Área de Tecnología. Dichas contraseñas deben ser codificadas y almacenadas de forma segura.

Las claves de administrador de los sistemas deben ser conservadas por el Área de Tecnología y deben ser cambiadas en intervalos regulares de tiempo y en todo caso cuando el personal adscrito al cargo cambie.

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, deberá cambiarla inmediatamente. No deben usarse contraseñas que sean idénticas o substancialmente similares a contraseñas previamente empleadas. El directorio activo no permite el uso de contraseñas anteriores. Esto aplicará dependiendo del sistema de validación que tienen las diferentes plataformas.

Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con ese usuario y contraseña

La contraseña inicial emitida a un nuevo usuario sólo será válida para la primera sesión. En ese momento, el usuario debe cambiar otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switches, etc., deben cambiarse antes de poner en servicio el equipo.

Para prevenir ataques, cuando el software del sistema lo permita, se limitarán a 5 el número consecutivo de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada quedará suspendida Si se trata de acceso remoto por VPN, la sesión debe ser inmediatamente desconectada.

Las contraseñas de acceso remoto por VPN no se podrán configurar de forma automática. Si no ha habido ninguna actividad como máximo en 5 minutos en una Terminal, PC o estación de trabajo el sistema automáticamente suspenderá la sesión. El re-establecimiento de la sesión requiere que el usuario proporcione nuevamente su contraseña.

Adicionalmente, para sistemas críticos, se requiere la autenticación de dos factores (2FA).

5.4. Revocación de Accesos

Cuando un empleado deja de trabajar en la organización, o cambia de rol, todos sus accesos a sistemas de información deben ser revocados o modificados inmediatamente según el formato TH.NO.F90.

5. Uso Aceptable de los Sistemas

5.1. Uso de Equipos y Recursos de TI

Los recursos tecnológicos de la organización, incluidos computadores, redes, y acceso a internet, deben utilizarse exclusivamente para fines laborales. Queda prohibido el uso de estos recursos para actividades ilícitas, inapropiadas o que pongan en riesgo la seguridad de la organización.

5.2. Uso de Dispositivos Personales (BYOD)

En caso de permitir el uso de dispositivos personales para el trabajo, los empleados deben seguir las pautas de la organización para la seguridad de estos dispositivos. Esto incluye:

- Mantener los dispositivos actualizados con los parches de seguridad.
- Instalar software de seguridad (antivirus, cortafuegos).
- Asegurar que los datos de la organización almacenados en estos dispositivos estén cifrados.

5.3. Responsabilidades de Usuarios Externos y Contratistas

Todos los usuarios externos que deban usar recursos de TI deben estar autorizados de acuerdo con los lineamientos establecidos en el procedimiento de acceso a terceros.

Los usuarios externos que requieran acceso a la red LAN o recursos internos deben aceptar el conocimiento y cumplimiento por escrito de los términos y condiciones de uso de la información y recursos de TI de PEOPLE CONTACT. Las cuentas de usuarios externos deben ser de perfiles específicos y tener caducidad de acuerdo con la duración del contrato.

Para el caso de contratistas, el incumplimiento de la política de seguridad de la compañía será sancionado de acuerdo con las cláusulas contractuales con este.

Las empresas de empleos temporales serán responsables de dar buen uso y difundir la información al personal en misión enviado para las diferentes campañas.

5.4. Usuarios invitados y servicios de acceso público.

El acceso y uso a cualquier tipo de recurso de información y TI no es permitido a usuarios invitados no registrados, salvo el acceso a internet destinado para tal fin.

5.5. Uso de Correo Electrónico

El correo electrónico corporativo solo debe ser utilizado para fines laborales. Está prohibido enviar información confidencial por correo sin cifrado, y se desaconseja el uso de correos personales para actividades laborales.

Responsabilidades de los usuarios con respecto al uso del correo:

- Los usuarios son responsables de todas las actividades realizadas con las cuentas de correo electrónico proporcionadas por PEOPLE CONTACT S.A.S.
- Esta responsabilidad supone el cuidado de los recursos que integran dicha cuenta y, particularmente, de los elementos, como la contraseña, que pueden permitir el acceso de terceras personas al correo, o a otros recursos personales que utilicen ese identificador.
- Cada usuario será el directamente responsable por la copia de seguridad de los .PST de su e-mail corporativo.
- En caso de retiro de la compañía el colaborador deberá entregar la copia de los .PST que tenga.

- Si se sospecha que la cuenta está siendo utilizada por una tercera persona, hay que avisar inmediatamente al grupo de Tecnología o a la cuenta "**soporte@peoplecontact.com.co".**

No está permitido:

- Los mecanismos y sistemas que intenten ocultar la identidad del emisor de correo.
- La suplantación de identidad de otra persona en el envío de mensajes de correo electrónico.
- Difusión del contenido inadecuado: Contenido ilegal por naturaleza.
- Difusión a través de canales no autorizados: Uso no autorizado de una cuenta ajena para reenviar correo propio.
- Difusión masiva no autorizada: correo SPAM.
- Ataques con objeto de imposibilitar o dificultar el servicio: Pueden dirigirse a un usuario o al propio sistema de correo.
- Abrir archivos de remitentes sospechosos.

- El tamaño máximo del mensaje que se debe y puede enviar utilizando el servidor de correo de PEOPLE CONTACT S.A.S. es de 10 MB.
- Máximo de destinatarios por correo: 20 (utilizar mejor las listas).
- Enviar información de la empresa sin autorización de la persona correspondiente.

5.6. Uso de Internet

Internet es un recurso importante para la obtención de información, sin embargo, cuando se usa para fines distintos a los laborales significa:

- Uso inapropiado de los recursos informáticos de la empresa.
- Pérdida de tiempo y, por tanto, ineficiencia en el desempeño del colaborador.
- Fuente de contaminación de virus, lo cual puede afectar el desempeño general de la red y por tanto de nuestros sistemas de información.

Por lo tanto, no es permitido:

- Acceder a páginas con contenido pornográfico y que no tengan que ver con las tareas asignadas por PEOPLE CONTACT S.A.S.
- Bajar videos con contenido pornográfico.
- Tener software Peer to Peer instalado

- El uso de mensajería instantánea como el whatsapp, Messenger, Instagram, Twitter para fines personales.
- Bajar instaladores de cualquier tipo, que influyan en la ocupación del canal de Internet.

5.7. Instalación de Software

Todas las instalaciones de software que se realicen sobre sistemas de PEOPLE CONTACT deben ser aprobadas por el Área de Tecnología, de acuerdo con los procedimientos establecidos.

No se permite la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas. El Área de Tecnología debe desinstalar cualquier software ilegal y registrar este hecho como un incidente de seguridad que debe ser investigado.

Corresponde al proceso de Tecnología mantener una base de datos actualizada que contenga un inventario del software autorizado para su uso e instalación en los sistemas informáticos de la compañía.

En conclusión, no es permitido:

- Copiar software (programas, Música, videos, libros, etc.).
- Instalar software. El personal de soporte es el único que puede instalar software en la empresa, con previa autorización de los líderes de Tecnología.
- Desinstalar programas, borrar archivos o cambiar configuraciones, sin autorización del personal del Área de Tecnología.
- Reconfigurar el software, hacer intentos de reconfigurar cualquier aplicativo ya instalado en el equipo del usuario.

Teniendo en cuenta que la empresa está sujeta a sanciones de tipo penal y civil por el uso de software no licenciado, es deber de los empleados de PEOPLE CONTACT el estricto cumplimiento de este numeral.

6. Seguridad Física y del entorno

6.1. Acceso

Se debe tener acceso controlado y restringido a los cuartos de servidores principales y a los cuartos de comunicaciones. El área de Tecnología elaborará y mantendrá las normas, controles y registros de acceso a dichas áreas.

6.2. Seguridad en los equipos

Los centros de cómputo donde se ubiquen los servidores y equipos de procesamiento de datos que contengan información y servicios corporativos deben estar protegidos por lo menos con:

- Controles de acceso y seguridad física.
- Sistema de detección de incendio.
- Controles de temperatura mediante un sistema de aire acondicionado.
- Controles para minimizar el riesgo de inundación.
- Sistemas eléctricos regulados y respaldados por fuentes de potencia ininterrumpida (UPS).

Toda información corporativa en formato digital debe ser mantenida en servidores aprobados por el área de Tecnología. No se permite el alojamiento de esta información en servidores externos sin que haya una aprobación por escrito por parte de la gerencia de PEOPLE CONTACT.

Los empleados de PEOPLE CONTACT serán responsables de almacenar la información de la compañía únicamente en los servidores de la empresa o los medios dispuestos por esta para tal fin.

El Área de Tecnología debe asegurar que la infraestructura de servicios de TI esté cubierta por mantenimiento y soporte adecuados de hardware y software.

El mantenimiento a computadores será llevado a cabo por personal de la empresa, el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información de la compañía. Solamente el área de tecnología hará cualquier tipo de mantenimiento tanto del hardware como del software y de la configuración de acceso a la red, al igual que las configuraciones de escritorio.

No está permitido:

- La instalación de ningún servicio que intervenga directamente con el cableado que alimenta las tomas.
- La manipulación por parte de los usuarios en cualquier tipo de conexión.
- Sin excepción, las conexiones deberán ser realizadas por el personal autorizado del área de tecnología.

- El diseño, la administración y el mantenimiento de las redes son responsabilidad del área de tecnología.
- Intervenir o modificar las redes de cableado, marcaciones de tomas, puertas o ductos.
- Golpear o forzar tubos y/o canaletas. La instalación de cables, derivaciones de voz o datos por parte de los usuarios.

7. Respuesta a Incidentes de Seguridad

7.1. Detección de Incidentes

Los incidentes de seguridad pueden ser detectados por los mecanismos que posee PEOPLE CONTACT, como:

- El Antivirus correspondiente (ESET) y sistemas de monitoreo de la red (FORTINET)
- Herramientas de detección de intrusiones (IDS/IPS)
- Informes de los empleados de PEOPLE CONTACT que experimentan actividad anómala como mensajes de error, ralentización extrema, accesos no autorizados o comportamiento no esperado de los dispositivos.
-

7.2. Notificación del Incidente

Todos los empleados de PEOPLE CONTACT y los sistemas de detección deben notificar inmediatamente cualquier actividad sospechosa usando los canales de comunicación establecidos (correo, teléfono, sistemas de tickets) al Área de Tecnología siguiendo los procedimientos para tal fin.

En conformidad con la ley, PEOPLE CONTACT podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos y en todo caso notificando previamente a los afectados por esta decisión.

7.3. Protección contra software malicioso y hacking (ciberseguridad)

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos, técnicos y administrativos.

En todo caso y como control mínimo, las estaciones de trabajo de PEOPLE CONTACT deben estar protegidas por software antivirus con capacidad de actualización automática en cuanto a firmas de virus. Los usuarios de las estaciones no están autorizados a deshabilitar este control.

Los equipos con sistema operativo Windows deberán tener instalado el antivirus corporativo. El cual deberá actualizarse diariamente.

PEOPLE CONTACT a través del área de Tecnología podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o detrimentos en el desempeño.

El Área de Tecnología debe tener información con alertas de seguridad reportadas por organismos competentes y actuar en conformidad cuando una alerta pueda tener un impacto considerable en el desempeño de los sistemas informáticos.

8. Administración de las comunicaciones y operaciones

8.1. Administración de Configuraciones de Red

La configuración de Reuters, Switches, Firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red; debe ser documentada, respaldada por copia de seguridad y mantenida por el Área de Tecnología.

Todo equipo de TI debe ser revisado, registrado y aprobado por el Área de Tecnología antes de conectarse a la Red LAN de comunicaciones y datos de la empresa.9.2. Plan de Mitigación

Para cada riesgo identificado, se debe desarrollar un plan de mitigación que pueda incluir medidas técnicas (actualizaciones de software, cifrado) o cambios organizacionales (capacitación, nuevos procedimientos).

8.2. Impresoras Corporativas

Las impresoras deben estar en sitios seguros y de poco tránsito de personas para protegerlas contra el acceso no autorizado.

Cualquier información impresa, debe ser retirada de la impresora en forma inmediata, evitando el acceso a esta información por personas no autorizadas.

Cuando sea posible y se trate de información sensible, debe implementarse el control de impresión con el uso de clave por usuario.

Recomendaciones:

- En caso de atascos de papel, favor recurrir inmediatamente a soporte técnico.
- Las impresoras no deben ser conectadas a la energía regulada.

No es permitido:

- Utilizar las impresoras para fines no laborales (trabajos personales).
- Para impresiones tipo borrador usar papel reciclable que esté grapado o en mal estado.
- Emplear papel de tamaño y tipo diferente al admitido por la impresora como: Papel demasiado delgado (papel de directorio telefónico).

8.3. Acceso Remoto y Telefonía Móvil

8.3.1. Acceso Remoto

Trabajo remoto

El trabajo remoto deberá ser avalado por el jefe de área a la cual depende el colaborador que solicite el permiso y autorizado por el gerente.

Requisitos de Conexión

Todo acceso remoto a los sistemas y recursos corporativos debe realizarse a través de una VPN segura aprobada por la organización.

Es obligatorio el uso de autenticación multifactor (MFA) para acceder remotamente a los sistemas.

Las conexiones remotas deben cumplir con los estándares de cifrado especificados por el Área de Tecnología, utilizando protocolos como IPSec o SSL/TLS.

Restricciones de Acceso

Solo los usuarios autorizados podrán tener acceso remoto a la red corporativa.

El acceso remoto solo debe utilizarse para tareas laborales y no para fines personales.

Se prohíbe el acceso remoto desde redes públicas no seguras (cafés, aeropuertos, etc.) sin el uso de VPN.

Supervisión y Monitoreo

Todas las conexiones remotas serán monitoreadas y auditadas para detectar actividades sospechosas o no autorizadas.

Cualquier actividad sospechosa será investigada y el acceso podrá ser suspendido en caso de detectar posibles violaciones de seguridad.

8.3.2. Uso de Dispositivos Móviles

Requisitos de Seguridad para Dispositivos Móviles

Los dispositivos móviles que se utilicen para acceder a recursos corporativos deben estar protegidos con contraseñas fuertes, bloqueo biométrico o métodos de autenticación aprobados.

Todos los dispositivos deben tener habilitado el cifrado de datos para proteger la información almacenada.

Se debe instalar software de seguridad aprobado por la empresa, como antivirus y aplicaciones de administración de dispositivos móviles (MDM - Mobile Device Management).

Uso Adecuado de Dispositivos Móviles

Los dispositivos móviles solo deben utilizarse para acceder a sistemas y aplicaciones corporativas aprobadas.

Se prohíbe el almacenamiento de información sensible o confidencial en dispositivos móviles sin cifrado.

No se permite el uso de redes Wi-Fi públicas sin protección para acceder a sistemas corporativos sin usar una VPN.

En caso de pérdida o robo de un dispositivo móvil, se debe notificar inmediatamente al Área de Tecnología para que se tomen las medidas necesarias, como la desactivación remota o el borrado de datos del dispositivo comprometido.

Mantenimiento y Actualización de Dispositivos

Los dispositivos móviles utilizados para el acceso a la red corporativa deben estar actualizados con los últimos parches de seguridad y versiones de software.

Los dispositivos que no cumplan con las actualizaciones de seguridad pueden ser bloqueados hasta que se pongan al día.

Para dispositivos de comunicación móvil (telefonía celular) corporativos se aplicarán los controles antes mencionados y los detallados a continuación:

La gerencia general debe autorizar por escrito los planes de voz y/o datos que paga la empresa y que usan los colaboradores.

Toda cuenta de correo corporativo en dispositivos móviles deberá ser autorizada por la Dirección de Tecnología de PEOPLE CONTACT.

El área de tecnología es la única que puede configurar las cuentas de correo de PEOPLE CONTACT en cualquier tipo de dispositivo móvil y la contraseña no se indicará al usuario.

Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.

No hablar de asuntos confidenciales cerca de personas que no requieran conocer dicha información.

9. Escritorio Limpio y Pantalla Limpia

9.1. Escritorios Limpios

Cada vez que un trabajador se ausenta de su lugar de trabajo debe bloquear su estación de trabajo, guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.

Al finalizar la jornada de trabajo, el funcionario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

9.2. Pantallas Limpias y Cierre de Sesión por Inactividad

Las estaciones de trabajo y equipos portátiles deben tener aplicado el bloqueo del escritorio automáticamente como máximo a los 5 minutos de inactividad del usuario en el equipo. Al regresar el funcionario se solicitará nuevamente usuario y contraseña para ingresar al equipo.

La pantalla de autenticación a la red de la empresa debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información.

El usuario deberá tener el cuidado de no almacenar documentación o información sensible en el escritorio (Pantalla inicial) de la estación de trabajo, se recomienda el uso de carpetas.

Cada vez que el usuario se ausente de su lugar de trabajo deberá bloquear la estación de trabajo de forma que proteja el acceso a las aplicaciones y servicios de la empresa. Para ello se recomienda presionar botón Windows + Letra L. Al volver el usuario, el sistema solicitará nuevamente usuario y contraseña para ingresar al equipo.

Una vez que el funcionario ha terminado su jornada laboral, deberá apagar el equipo, de lo contrario este se apagará automáticamente entre las 21:00 y las 23:00 según las políticas establecidas de ahorro de energía.

9.3. Salas y Tableros o Acrílicos Limpios

Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado.

Después de las reuniones en que se utilicen tableros o acrílicos, estas deben quedar limpias de la información que se ha expuesto en ellas.

En caso de que se utilice una estación de trabajo para presentaciones, si éste fuera de uso común, debe eliminarse la información antes presentada.

Luego de utilizar salas de reuniones con proyección estos deberán apagarse.

10. Capacitación en Seguridad de la Información

10.1. Capacitación Regular

Las Áreas de Talento Humano y Mejoramiento Continuo se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

11. Cumplimiento Legal y Normativo

11.1. Cumplimiento de Regulaciones

La empresa debe cumplir con todas las normativas de seguridad de la información y protección de datos aplicables, como el Reglamento General de Protección de Datos (GDPR), ISO/IEC 27001 y otras legislaciones locales o internacionales.

11.2. Auditorías

Se realizarán auditorías periódicas para lo cual se llevará a cabo el programa de auditoria por los entes de control para garantizar que la política de seguridad de la información esté siendo cumplida y para identificar áreas de mejora.

12. Consecuencias del Incumplimiento

12.1. Sanciones

El Reglamento Interno de Trabajo de la compañía debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

Revisión y Actualización de la Política

12.2. Revisión Anual

Esta política será revisada al menos una vez al año, o cuando sea necesario debido a cambios tecnológicos, normativos o estructurales.

13. Referencias

- **ISO 27001:2022. Sistemas de gestión de Seguridad en la Información Requerimientos.**
- **NIST SP 80030.**Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.
- **ISO/IEC 27001:2022** — Establece los **requisitos** para implementar un SGSI (Sistema de Gestión de Seguridad de la Información). Es la norma **certificable**.
- **ISO/IEC 27002:2022** — Proporciona un **catálogo de controles** y buenas prácticas de seguridad para aplicar los requisitos de la 27001.
- **ISO/IEC 27005:2022** — Guía para la **gestión de riesgos de seguridad de la información**, complementa la 27001.
- **ISO/IEC 27017:2015** — Controles de seguridad para **servicios en la nube** (Cloud Computing).
- **ISO/IEC 27018:2019** — Protección de **datos personales en la nube**.
- **ISO/IEC27035 (Partes 1 y 2)** — Gestión de **incidentes de seguridad de la información**.
- **ISO/IEC 27701:2019** — Extensión de la 27001 para **gestión de privacidad y datos personales (SGPI)**.

14. Términos y Definiciones

Información

Toda forma de conocimiento objetivo con representación física o lógica explícita.

Activo de Información

Datos o información propiedad de la Empresa que se almacena en cualquier tipo de medio y que es considerada por la misma como sensitiva o crítica para el cumplimiento de los objetivos misionales.

Sistema de Información

Conjunto ordenado de elementos cuyas propiedades se relacionan e interaccionan permitiendo la recopilación, procesamiento, mantenimiento, transmisión y difusión de información utilizando diferentes medios y mecanismos tanto automatizados como manuales.

Propietario de Activos de Información

En el contexto de la norma NTC 27001, un propietario de activos de información es cualquier persona o entidad a la cual se le asigna la responsabilidad formal de custodiar y asegurar un activo de información o un conjunto de ellos.

Tecnología de la Información

Conjunto de hardware y software operados por la entidad o por un tercero en su nombre, que componen la plataforma necesaria para procesar y administrar la información que requiere la entidad para llevar a cabo sus funciones.

Evaluación de Riesgos

Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de esta, la probabilidad de que ocurran y su potencial

impacto.

Administración de Riesgos

Proceso de identificación, control y reducción o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Responsable de Seguridad Informática

Líder de Telecomunicaciones y Soporte. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

Incidente de Seguridad Informática

Un incidente de seguridad informática es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad, disponibilidad, legalidad o confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Cadena de custodia

En el ámbito de la seguridad de la información, la cadena de custodia es la aplicación de una serie de normas y procedimientos tendientes a asegurar, depositar y proteger cada

activo de información para evitar la pérdida de integridad, disponibilidad o confidencialidad.