# POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

**Contenido**

**Introducción**

Actualmente la información de PEOPLE CONTACT se ha reconocido como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. PEOPLE CONTACT, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computador, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

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 entiende como la preservación, aseguramiento y cumplimiento de las siguientes características de la información:

- **Confidencialidad:** los activos de información solo pueden ser accedidos y custodiados por usuarios que tengan permisos para ello.
- **Integridad:** El contenido de los activos de información debe permanecer inalterado y completo. Las modificaciones realizadas deben ser registradas asegurando su confiabilidad.
- **Disponibilidad:** Los activos de información sólo pueden ser obtenidos a corto plazo por los usuarios que tengan los permisos adecuados.

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 la presente política, por medio del **comité de sistemas de gestión**.

En todo caso, dicho comité, deberá revisar y en caso necesario, actualizar anualmente esta política.

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, normas, guías y procedimientos recomendados por el **comité de sistemas de gestión**.

## 3. Política de Seguridad de la Información

### 3.1. Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la empresa y por consiguiente debe ser debidamente protegida.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto sistema de información.

PEOPLE CONTACT establecerá los mecanismos para respaldar la difusión, estudio, actualización y consolidación tanto de la presente política como de los demás componentes del Sistema de Gestión de la Seguridad de la Información y alinearlos de forma efectiva con los demás sistemas de gestión.

### 3.2. Alcance

Esta política es de aplicación para todas las áreas que componen a PEOPLE CONTACT, a sus recursos y a la totalidad de los procesos internos o externos vinculados a la compañía a través de contratos o acuerdos con terceros.

### 3.3. Objetivos

a) Proteger, preservar y administrar objetivamente la información de PEOPLE CONTACT 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 los características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
b) 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.
c) 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.

### 3.4. Responsabilidad

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.
Las directivas de PEOPLE CONTACT aprueban esta Política y son responsables de la autorización de sus modificaciones.

El **Comité de Sistemas de Gestión** es responsable de revisar y aprobar el texto de la Política de Seguridad de la Información, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejora del Sistema de Gestión de Seguridad de la compañía. Es responsabilidad de dicho comité definir las estrategias de capacitación en materia de seguridad de la información al interior de PEOPLE CONTACT. Así mismo será el responsable de coordinar las acciones para impulsar la implementación y el cumplimiento de la presente Política.

El **equipo 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

Los **propietarios de activos de información** (ver su definición en el glosario) son responsables de la clasificación, mantenimiento y actualización de la misma; así como de documentar y mantener actualizada la clasificación efectuada, definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a 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.

El **Gerente de Talento Humano** será el 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 Sistemas de Gestión. De igual manera es responsable del control y seguimiento a las violaciones de la presente política de seguridad de la información.

**Los Líderes de Tecnología** 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.

El **Secretario General** verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con terceros. Asimismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

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 área de **Gestión de la Calidad** 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 establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

## 4. Identificación, clasificación y valoración de activos de información.

Cada dependencia bajo supervisión del Comité de Sistemas de Gestión, 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 **Gestión de la Calidad** 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.

## 5. 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 ó a quien este 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.

**5.1. 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.

Las Áreas de Gestión Humana y de Gestión de la Calidad 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.

La empresa hará la entrega oficial del equipo de cómputo en funcionamiento, con el respectivo software instalado y licenciado, 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 las mismas y las consecuencias a nivel interno y externo que sus actuaciones pueden generar.

**5.2. Responsabilidades del personal de PEOPLE CONTACT**

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.

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 a la normatividad legal vigente.

Si se demuestran perdidas económicas por causales de daños a los equipos por causa de mal uso de los mismos, 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 a la instancia correspondiente (Help Desk).

No se permite fumar, comer o beber mientras se está usando un PC.

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.

**5.3. Responsabilidades de Usuarios Externos y Contratistas**

Todos los usuarios externos que deban usar recursos de TI deben estar autorizados de acuerdo a 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 a la duración del contrato.

Para el caso de contratistas, el incumplimiento de la política de seguridad de la compañía será sancionado de acuerdo a 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.

## 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 los menos con:

- Controles de acceso y seguridad física.
- Sistema de detección de incendio.
- Controles de temperatura mediante un sistemas 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.

Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Comité de Sistemas de Gestión

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.

**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. Administración de las comunicaciones y operaciones

### 7.1. Reporte e investigación de incidentes de seguridad

El personal de PEOPLE CONTACT debe reportar con prontitud presuntas violaciones de seguridad, siguiendo los procedimientos establecidos para tal fin.

El Comité de Sistemas de Gestión debe preparar, mantener y difundir las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

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

### 7.2. Protección contra software malicioso y hacking.

Todos los sistemas informáticos deben ser protegidos teniendo en cuenta un enfoque multi-nivel que involucre controles humanos, físicos, técnicos y administrativos. El Comité de Sistemas de Gestión elaborará y mantendrá un procedimiento de gestión de incidentes que defina las acciones a seguir cuando se presente amenazas o ataques de software malicioso y hacking.

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 la 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.

**7.3. Copias de Seguridad**

Toda información que pertenezca a la matriz de activos de 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 a 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 a cronogramas definidos y publicados por el Área de Tecnología para los roles interesados.

**7.4. Administración de Configuraciones de Red**

La configuración de Routers, 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 Red LAN de comunicaciones y datos de la empresa.

**7.5. 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 a la legislación. (Sección 12 de esta Política)

**7.6. Internet y Correo Electrónico**

Las normas de uso de Internet y de los servicios de correo electrónico serán aprobadas por el Comité de Sistemas de Gestión y en todo caso este comité debe velar por el cumplimiento del código de ética de la compañía y el manejo responsable de los recursos de tecnologías de la información.

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 (Ares, Limewire, Kazaa, etc)
- El uso de mensajería instantánea como el Messenger para fines personales.
- Bajar instaladores de cualquier tipo, que influyan en la ocupación del canal de Internet.

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.

**7.7. 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 a 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 a la Oficina 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.

### 7.8. Impresoras Corporativas

Recomendaciones:

- En caso de atascos de papel, favor recurrir inmediatamente a Help Desk.
- 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. Control de Acceso

### 8.1. Categorías de Acceso

El acceso a los recursos de tecnologías de información institucionales debe estar restringido según los perfiles de usuario definidos por el Comité de Sistemas de Gestión.

Está prohibido violar los sistemas de acceso y/o suplantar la identidad de personas.

### 8.2. Control de Claves (Contraseñas) y Cuentas de Usuario

El acceso a información restringida debe estar controlado. PEOPLE CONTACT actualmente usa un sistema automatizado de autenticación que manejen credenciales o firmas digitales.

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.

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.

Las contraseñas del directorio activo deben ser de mínimo 8 caracteres y debe incluir los siguientes aspectos: Mayúsculas, minúsculas, números, caracteres alfanuméricos y especiales, esta contraseña no debe haber sido utilizada en las ultimas 12 ocasiones, no debe contener el nombre del usuario, esta contraseña se bloqueará automáticamente tras 5 intentos fallidos de inicio de sesión y se desbloqueara automáticamente a los 10 minutos, igualmente caducará cada 60 días y es obligatorio realizar el cambio de la misma antes de iniciar nuevamente sesión cumplido este plazo.

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.

**Cuentas de los usuarios**

- 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 Coordinador del área 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.

Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse del su cuenta y/o privilegios de la PBX y del Directorio Activo.

- 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 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, Gestión Humana, activos fijos y Nómina deberán firmar el certificado de paz y salvo.

### 8.3. Computación Móvil

PEOPLE CONTACT reconoce el alto grado de exposición que presenta la información y los datos almacenados en dispositivos portátiles (computadores portátiles, tabletas, celulares, discos duros extraíbles, memorias USB, etc.).

Corresponde al área de Gestión Humana elaborar, mantener e implementar planes de capacitación que propendan por la formación y mantenimiento de la conciencia en cuestión de seguridad de la información.

Los personas que estén autorizadas para realizar el uso de dispositivos móviles tales como computadores portátiles, Smartphone y tabletas con el fin de tener acceso a información de la empresa como correo electrónico deberá tener el equipo bloqueado con contraseña para que impida el acceso por personas no autorizadas.

En caso de incumplimiento de lo anterior, Gestión de Talento Humano iniciará un proceso disciplinario a las personas que no apliquen esta política.

### 8.4. Auditoria y Seguimiento

Todo uso que se haga de los recursos de tecnologías de la información en PEOPLE CONTACT debe ser seguido y auditado de acuerdo con los lineamientos definidos por el procedimiento establecido para tal fin.

### 8.5. Acceso Remoto y Telefonía Móvil

El acceso remoto a servicios de red ofrecidos por la Empresa debe estar sujeto a medidas de control definidas por el área de Tecnología, las cuales deben incluir acuerdos escritos de seguridad de la información.

Teniendo en cuenta las ventajas de la computación y telefonía móvil y el trabajo remoto, así mismo aumenta el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información organizacional, a continuación se establecen directrices que permitirán regular el uso de la computación y telefonía móvil y trabajo remoto.

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información organizacional, desde lugares diferentes a las instalaciones de PEOPLE CONTACT.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la empresa y deberán contemplar las siguientes directrices:

- La gerencia general debe autorizar por escrito a la persona usuaria de estos.

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información para portátiles y medios extraíbles
- Uso de software antivirus provisto por el área de Tecnología.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por el área de Tecnología.
- Realización de copias de seguridad periódicas. Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención, acerca de portar equipos móviles.
- No identificar el dispositivo con distintivos de PEOPLE CONTACT.
- No colocar datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.
- No conectarse a redes WiFi públicas.
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- Informar de inmediato al Área de Soporte sobre la pérdida o hurto del dispositivo, quien procederá al bloqueo del usuario.

Para dispositivos de comunicación móvil (telefonía celular) corporativos se aplicaran 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.

**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 general de PEOPLE CONTACT.

## 9. Adquisición, Desarrollo y Mantenimiento de Sistemas de Software

Para apoyar los procesos operativos y estratégicos, la Empresa debe hacer uso intensivo de las Tecnologías de la Información y las Comunicaciones. Los sistemas de software utilizados pueden ser adquiridos a través de terceras partes o desarrollados por personal propio.
PEOPLE CONTACT debe elegir, elaborar, mantener y difundir un método de desarrollo de software que incluya lineamientos, procesos, buenas prácticas, plantillas y demás artefactos que sirvan para regular los desarrollos de software internos en un ambiente de mitigación del riesgo y aseguramiento de la calidad.

Todo proyecto de desarrollo de software interno debe contar con un documento de Identificación y Valoración de Riesgos del proyecto. PEOPLE CONTACT no debe emprender procesos de desarrollo – o mantenimiento – de sistemas software que tengan asociados riesgos altos no mitigados.
Los sistemas de software adquiridos a través de terceras partes deben certificar el cumplimiento de estándares de calidad en el proceso de desarrollo.

## 10. Administración de Continuidad del Negocio

La Administración de Continuidad del Negocio debe ser parte integral del Plan de Administración de Riesgo de PEOPLE CONTACT.

## 11. Escritorio Limpio y Pantalla Limpia

### 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.

### 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.

**Protección en Impresoras**

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.

**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 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.

**12. Uso de controles criptográficos**

La empresa establece la presente Política de uso de controles criptográficos, a fin de determinar su correcto uso. Para ello se indica que:

**Se utilizarán controles criptográficos en los siguientes casos:**

- Accesos internos de la VPN (client to site)

- Bases de datos de los clientes y de los usuarios de los clientes
- Enlaces VPN Site to Site de acuerdo los requerimientos contractuales
- Sistema de archivos de equipos portátiles de los gerentes, directores y coordinadores
- Medios extraíbles Autorizados
- Carpetas FTP/ FTPS acceso Clientes Externos
- Grabadoras (Red Box – CTlog – WFO)
- Se tiene un procedimiento de criptografía en cual detalla los lineamientos para el cumplimiento de esta política.

**13. Política para la transferencia de información**

Los elementos conectados a la red deben tener las condiciones de seguridad (tanto de hardware y software) para garantizar que no afectarán la confidencialidad e integridad de la información actual de la organización al utilizar estos medios.
Por tal razón se tiene un procedimiento de Transferencia De Información En Las Redes en cual detalla los lineamientos para el cumplimiento de esta política.

**14. Cumplimiento**

Todo uso y seguimiento a los recursos de TI en PEOPLE CONTACT debe estar de acuerdo a las normas y estatutos internos así como a la legislación nacional en la materia.

**15. Referencias**


- ISO 27001:2013.Sistemas de gestión de Seguridad en la Información– Requerimientos.
- ISO/IEC 13335-1:2004. Tecnología de la información – Técnicas de seguridad – Gestión de seguridad en tecnología de información y comunicaciones – Parte 1: Conceptos y modelos para la gestión de seguridad en la tecnología de la información y comunicaciones.
- ISO/IEC TR 13335-3:1998. Lineamientos para la Gestión de Seguridad TI – Parte 3: Técnicas para la gestión de la seguridad TI.
- ISO/IEC 13335-4:2000.Lineamientos para la Gestión de la Seguridad TI – Parte 4: Selección de salvaguardas.
- ISO 14001:2004.Sistemas de gestión ambiental – Requerimientos con lineamiento para su uso.
- ISO/IEC TR 18044:2004.Tecnología de la información – Técnicas de seguridad – Gestión de incidentes en la seguridad de la información.
- ISO/IEC 19011:2002. Lineamientos para la auditoría de sistemas de auditoría y/o gestión ambiental.
- ISO/IEC Guía 62:1996.Requerimientos generales para los organismos que operan la evaluación y certificación/registro de sistemas de calidad.

- ISO/IEC Guía 73:2002. Gestión de riesgo –Vocabulario – Lineamientos para el uso en estándares .
- NIST SP 800-30.Guía de Gestión de Riesgo para los Sistemas de Tecnología de la Información.
- ISO 9001:2000.Sistemas de gestión de calidad – Requerimientos.

**16. 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 la misma, 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.

**Comité de Gerencia y Sistemas de Gestión**

El Comité de Gerencia y Sistemas de Gestión, es un cuerpo integrado por diferentes representantes de PEOPLE CONTACT, destinado a garantizar el apoyo manifiesto de las directivas a las iniciativas de seguridad.

Su función principal es definir, estructurar, recomendar, hacer seguimiento y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) de la Empresa. Depende directamente Gerencia General, y complementa el trabajo del Comité de Informática y Telecomunicaciones sirviendo como consultor técnico en temas relacionados con la seguridad de la información.

**Responsable de Seguridad Informática**

Coordinador general del Comité de Gerencia y Sistemas de Gestión. Su función principal es supervisar el cumplimiento de la presente Política y los lineamientos del SGSI.

**Grupo responsable de Seguridad Informática**

Grupos de apoyo creado en dependencias de PEOPLE CONTACT que manejan información sensible o crítica y que se encargan de velar por la operación del SGSI. Están conformados por funcionarios o contratistas de la dependencia que tengan formación en seguridad de la información.

**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.

**GIOVANY GÓMEZ**
**GERENTE GENERAL**
**PEOPLE CONTACT S.A.S.**