Confiar ltda. seguridad

ENTORNOS **SEGUROS**

Políticas de **la Seguridad de la información**

OBJETIVO:

Definir los lineamientos básicos que normen la coordinación de responsabilidad de Seguridad de Información en la organización; para asegurar la integridad, disponibilidad y confidencialidad de la información.

1. PROPOSITO

El propósito es proporcionar a los empleados de CONFIAR SEGURIDAD LTDA servicios de alta calidad y al mismo tiempo desarrollar un comportamiento altamente ético y profesional en relación con el manejo y/o manipulación de los servicios y los recursos informáticos. Describir las reglas de uso y actividades que se entiende como violación al uso de los servicios y recursos, los cuáles se consideran prohibidos.

ALCANCE:

Esta política es de estricto cumplimiento para la organización en sus diferentes ubicaciones, procesos (estratégico, misionales y apoyo) como define el mapa de procesos de la organización, activos de información (físicos y/o digitales), la infraestructura (edificios, tecnología) y colaboradores (directos e indirectos).

2.POLITICAS:

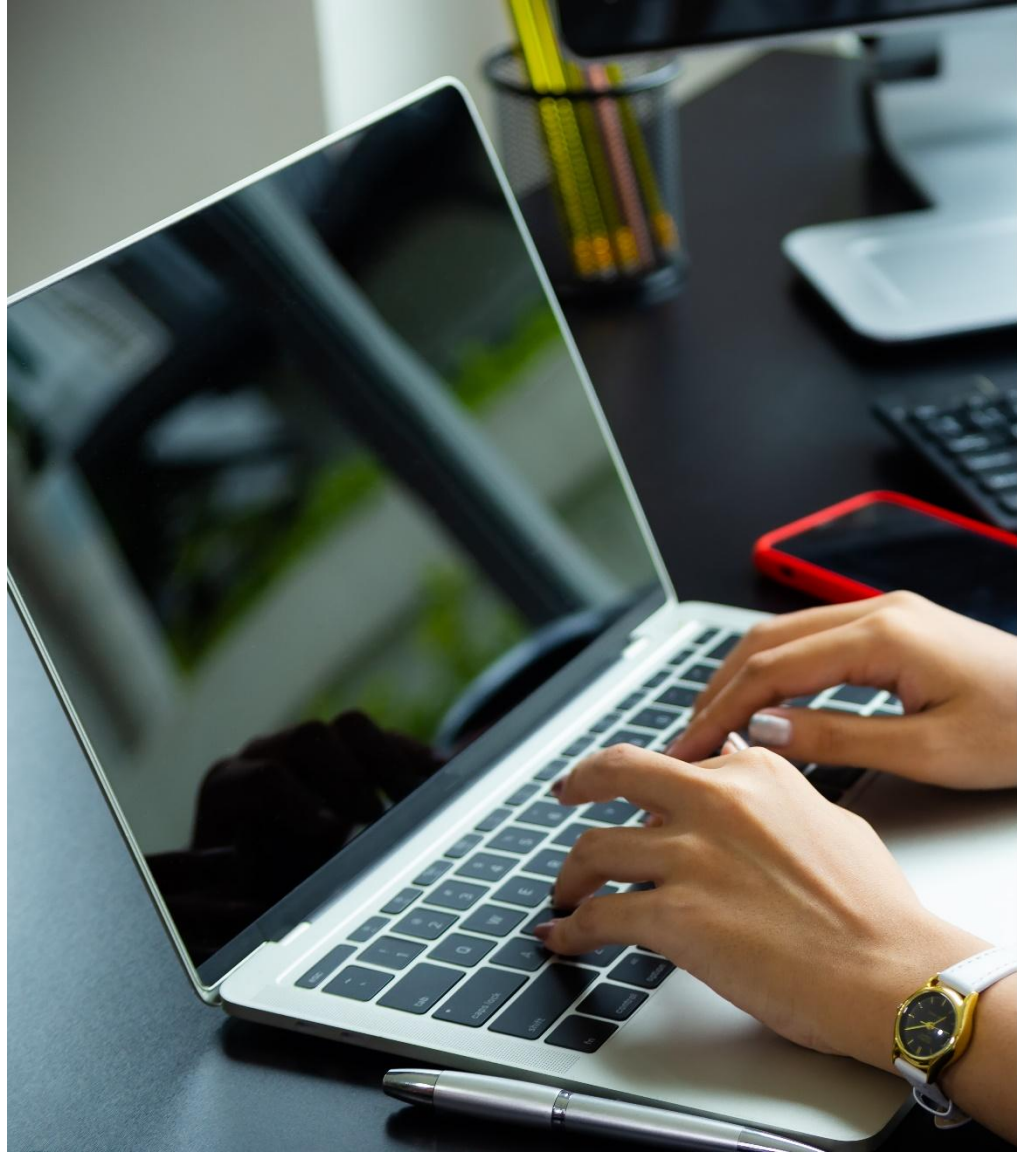
- El computador de escritorio, computador portátil y demás recursos informáticos asignados para su trabajo, los servicios asociados tanto internos como externos, el servicio de mensajes de correo electrónico, la Intranet, el acceso a Internet y los documentos y programas que existen en los mismos, son propiedad de CONFIAR SEGURIDAD LTDA y sólo podrán utilizarse para propósitos lícitos, prudentes, res y dentro de las funciones que le hayan sido encomendadas en su cargo u otras q adicionalmente pueda asignarle su jefe inmediato.

Políticas de la Seguridad de la Información

-Toda información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho que surja, se cree o modifique mediante el uso de uno de los computadores de escritorio, computadores portátiles y demás recursos informáticos propiedad de CONFIAR SEGURIDAD LTDA, será propiedad de la Empresa, aunque la información, dato, obra literaria o de arte, escrito, documento, programa, acción, privilegio, patente, derecho de autor o cualquier otro derecho haya surgido mediante el esfuerzo personal del usuario.

-La información contenida en los sistema digital de documentos, los documentos y programas exirecursos informáticos que se le han asignado para su trabajo, los servicios asociados tanto internos como externos, los mensajes de correo electrónico, información de la Intranet, imágenes del stentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones CONFIAR SEGURIDAD LTDA y concernientes al cargo desempeñado.

- En concordancia con las leyes, reglamentos y contratos en vigor, y sin perjuicio de las políticas y Políticas de CONFIAR SEGURIDAD LTDA, se reserva el derecho, en cualquier momento y sin previo aviso, de acceder, inspeccionar, leer, examinar, eliminar, guardar, escanear o usar todas las comunicaciones electrónicas enviadas, recibidas, almacenadas o transmitidas, haciendo uso de los recursos propios de la compañía con fines de auditoria. Igualmente se podrá controlar el uso que se le dé a los recursos informáticos.



Políticas de la Seguridad de la Información

USO ACEPTABLE DE LOS ACTIVOS DE INFORMACIÓN

Se entiende por uso aceptable de activos de información a utilizar de forma correcta, eficiente y segura los activos de información, independiente de su forma (física o lógica). Además, cualquier actividad de creación, asignación, destrucción, modificación, o procesamiento de este en cualquier formato que genere algún tipo de valor para la organización, para minimizar los riesgos asociados.

1.Todos los colaboradores de la organización deberán respetar los controles que atañen al uso de activos de información.

2.Se establece que los recursos tecnológicos proporcionados por la organización son para uso exclusivamente de carácter laboral. Sin embargo, se permite un uso mínimo de carácter personal, sin que este llegue a afectar directa o indirectamente a la operación. Todos los recursos tecnológicos de la organización se rigen por el marco normativo definido en este documento.

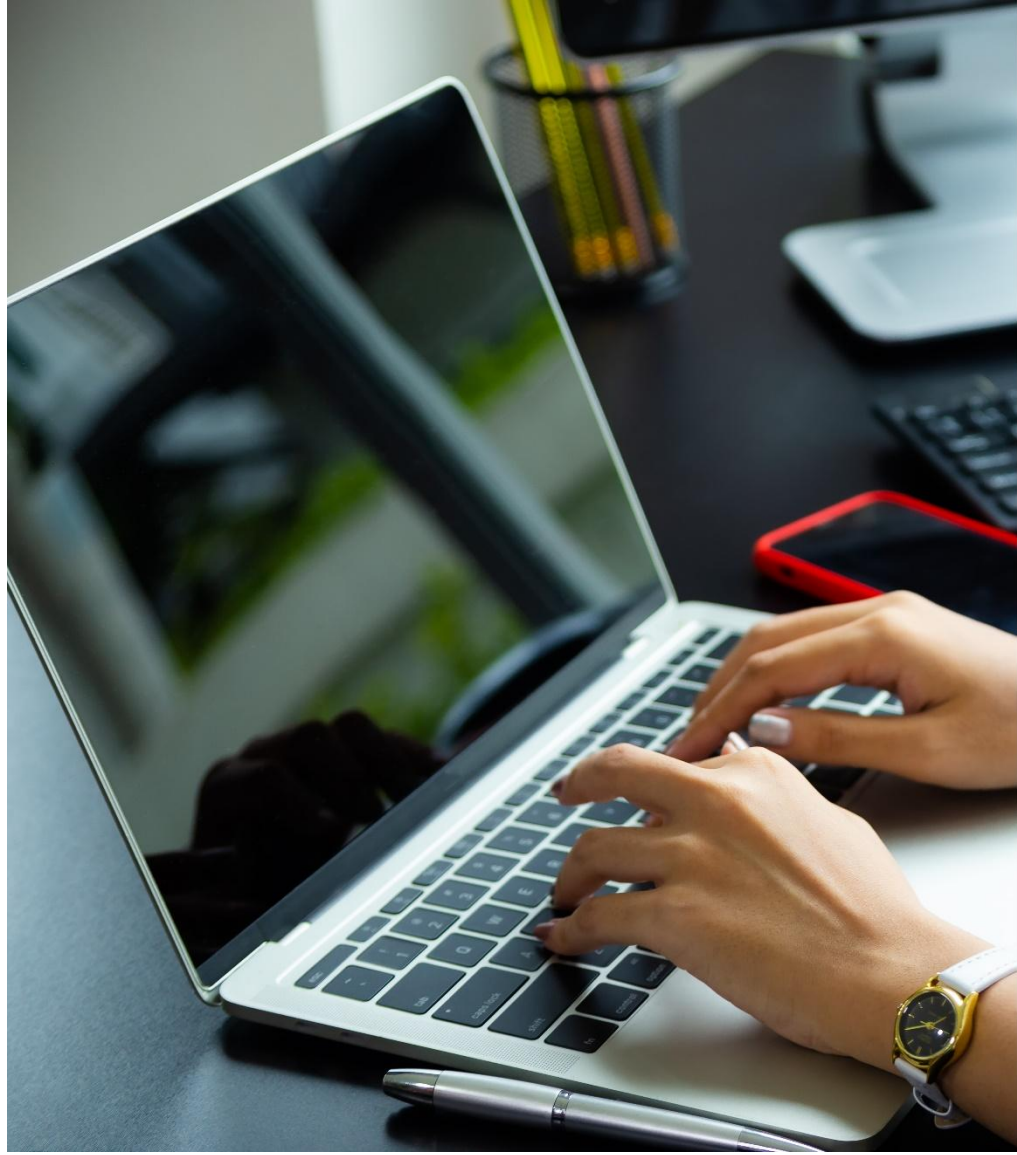
3. La organización se reserva el derecho de monitorear las actividades dentro de los recursos de cómputo acorde a sus intereses.

4.El uso aceptable de activos de información implica:

a.Usar el correo electrónico corporativo y software de comunicación interna solo para fines legítimos y autorizados.

b.Usar los recursos y/o sistemas de información solo para propósitos laborales y relacionado con las tareas asignadas.

c.Uso responsable de los recursos, sistemas de información, internet, servicios de red y almacenamiento.

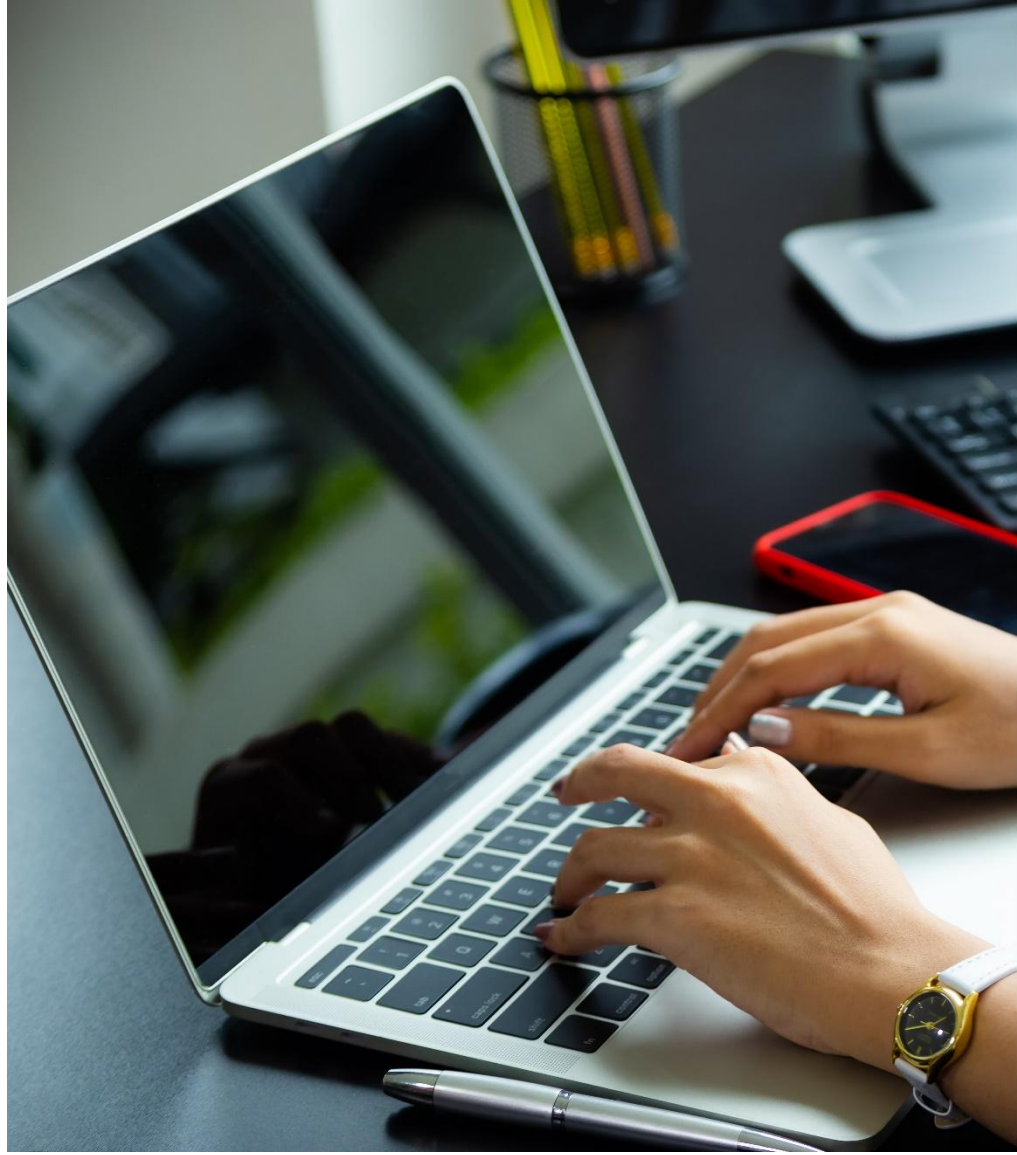


Confiar ltda. seguridad

Políticas de la Seguridad de la Información

d. Evitar daños temporales o permanentes en los activos de información causados por accidentes imprudenciales .
e. Evitar la pérdida temporal o total de activos de información causados por actividades negligentes u olvidos.

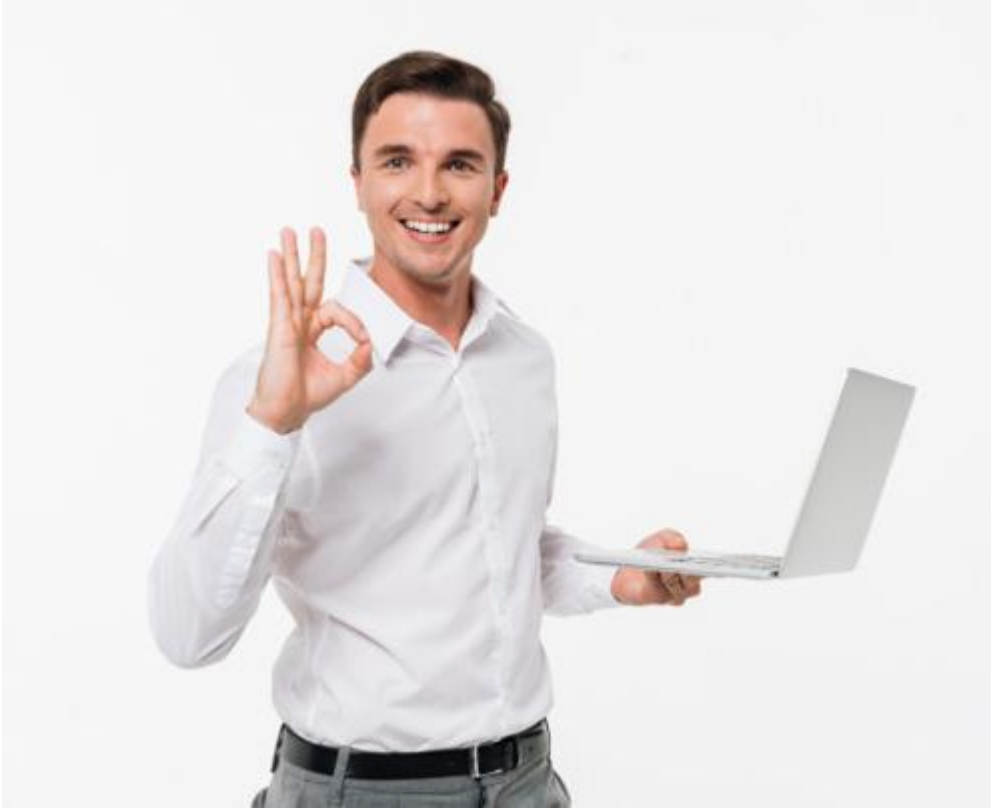
5.El uso inaceptable de activos de información implica:
a. Usar los recursos y/o sistemas de información para realizar actividades ilegales, como piratería, fraude o violación de derechos de autor.
b. Usar los recursos provistos para obtener, almacenar o transmitir material electrónico de cualquier índole que viole alguna ley bajo la jurisdicción local o regional.
c. Descargar archivos de internet de dudosa procedencia, esto puede causar daños irreparables al activo de información.
d. Alterar archivos o librerías propios del sistema operativo a través de la aplicación de parches no autorizados.
e. Se prohíbe deshabilitar o evadir las medidas de seguridad instaladas en los recursos tecnológicos de la organización.
f. Instalar software no autorizado.



Confiar ltda. seguridad

Políticas de la

Seguridad de la Información



-Se incluye la información relativa al uso de Internet, incluido, pero no limitado a los sitios visitados, las fechas, las horas y la duración de cualquiera de dichas visitas. Además, podrá efectuarse control sobre los puntos de acceso a las redes corporativas ya sean internos o externos.
-En la medida autorizada por la legislación, CONFIAR SEGURIDAD LTDA se reserva el derecho de emplear sistemas de control de contenidos, servicios de bloqueo de sitios que impidan el acceso a determinados sitios Web, así como otras herramientas electrónicas de gestión, como son, herramientas para monitorear el almacenamiento de archivos en los servidores.

-Hasta donde las leyes lo permitan, CONFIAR SEGURIDAD LTDA se reserva el derecho de revelar cualquier información o material obtenido por cualquiera medio

Confiar ltda. seguridad

Manejo de **Información confidencial**

Acuerdos de confidencialidad, de conexión a la red por parte de terceros y cumplimiento de las políticas de Seguridad de la Información.

ACCESO A REDES

Se entiende por red al conjunto de dispositivos conectados entre sí que permite el transporte de datos, con la finalidad de compartir diferentes tipos de recursos como servidores, dispositivos y además consumir servicios de red como son los sistemas de información, herramientas, aplicaciones, entre otras.

La organización debe garantizar que la red cuente con protección necesaria para dar cumplimiento a los principios de seguridad de la información (confidencialidad, disponibilidad e integridad) en el tránsito de los datos.

La organización debe segmentar / segregar la red cuando se requiera y, definir arquitectura e infraestructura que garantice los mínimos de seguridad a manera de aislar y apoyar en la prevención de intrusos malintencionados.

Confiar ltda. seguridad

Manejo de **Información confidencial**

Los activos de información que se conecten a la red de la organización deben contar con su respectiva identificación. Además, los equipos de índole personal no se deben conectar a la red de la organización, deben emplear la red para visitantes.

La administración de accesos a recursos de red es responsabilidad del área de IT.

Todos los usuarios de los recursos informáticos CONFIAR SEGURIDAD LTDA, empleados y personas suministradas por terceras partes, deben firmar un acuerdo de confidencialidad y de cumplimiento de las políticas de Seguridad Informática.

Política Dirigida a Todos los Usuarios:

Todo usuario debe firmar un acuerdo de confidencialidad y estará prohibido la divulgación de información confidencial a propios o terceros, para el uso de los recursos informáticos de CONFIAR SEGURIDAD LTDA.

Políticas de la

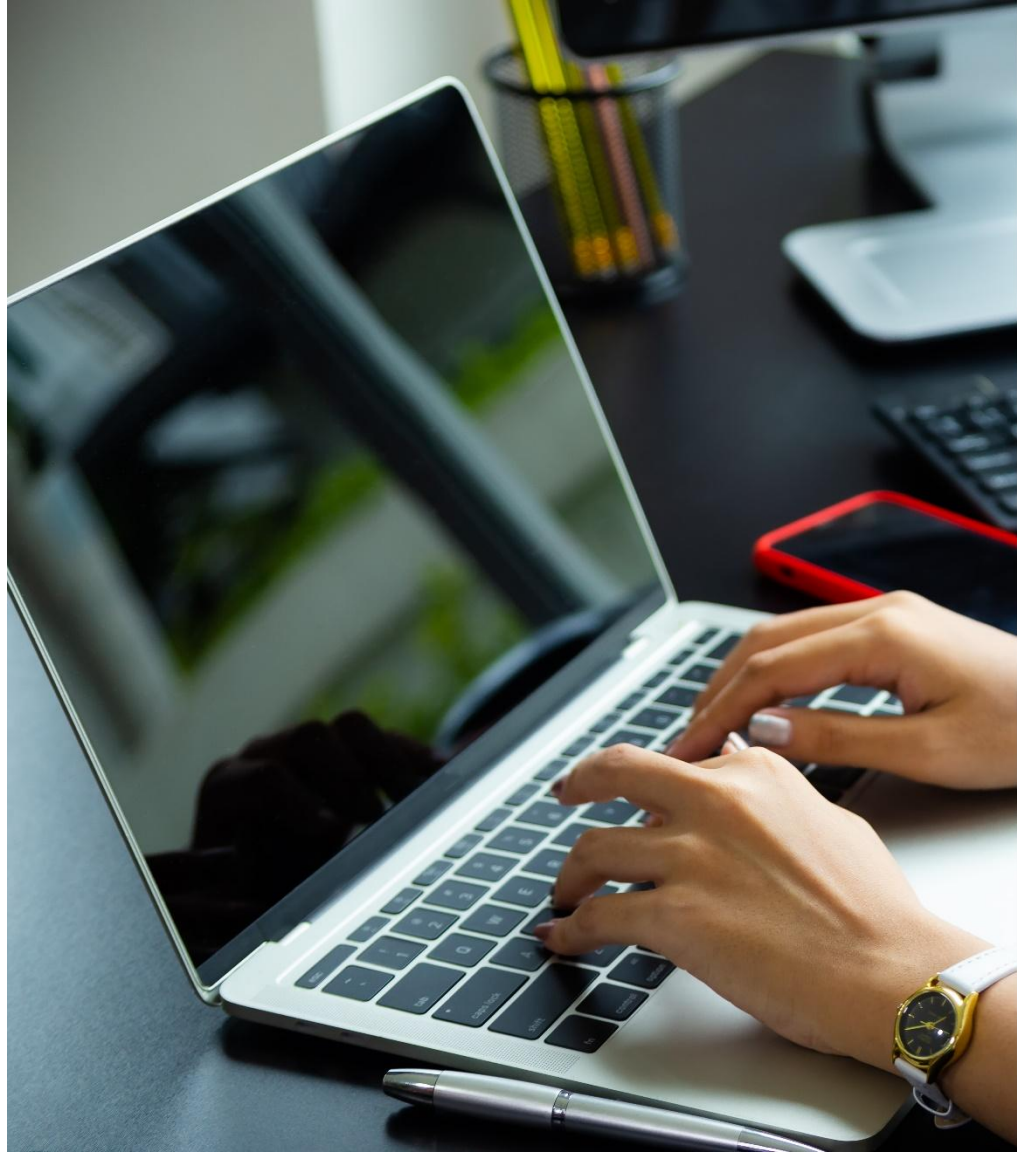
Seguridad de la información

Uso de computadores de escritorio, computadores portátiles y otros dispositivos.

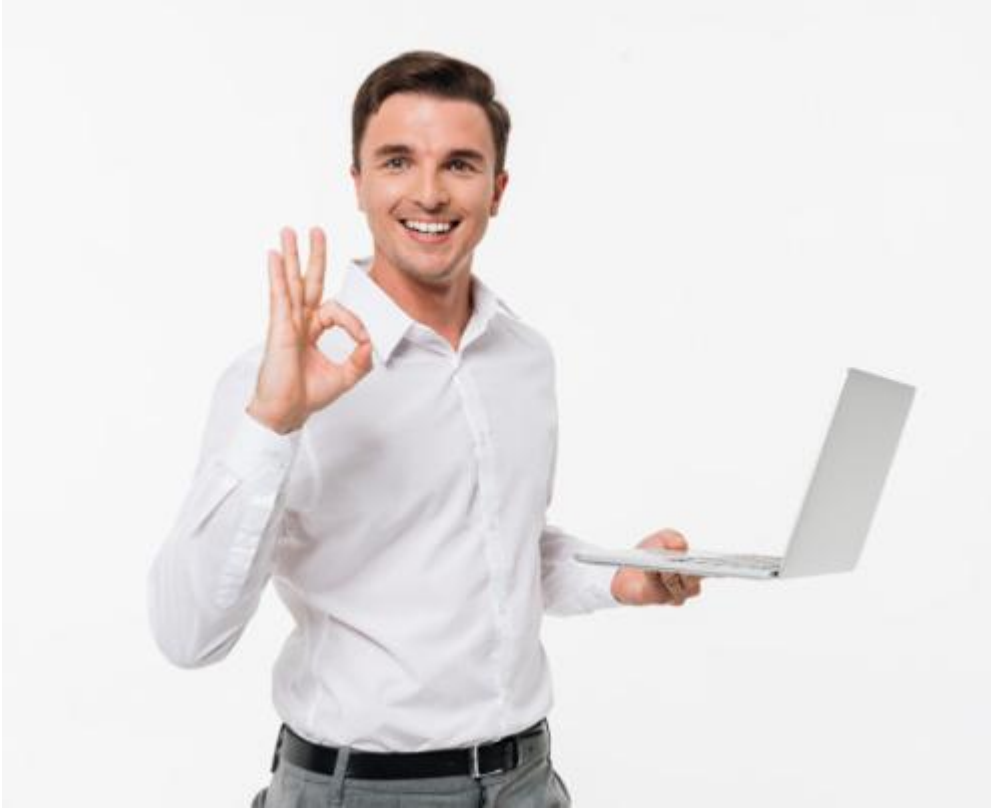
Los recursos informáticos son provistos por CONFIAR SEGURIDAD LTDA a los usuarios, con el único fin de desarrollar actividades relacionadas con el negocio y el trabajo asignado. Por lo anterior, estos recursos deben ser utilizados de manera adecuada y eficiente.

-La protección física de los computadores de escritorio, computadores portátiles y demás recursos informáticos, corresponde a las personas, a quienes se les asignaron, y es su deber notificar al departamento de sistemas sobre cualquier eventualidad que ocurra sobre dichos equipos. La notificación se debe realizar a través de correo electrónico corporativo.

-El éstos pueda hacer cualquier usuario, aún si a este se le ha asignado el recurso. Departamento de sistemas es el único autorizado para realizar movimientos y asignaciones de recursos informáticos, por lo que está totalmente prohibida la disposición que de



Políticas de la Seguridad de la Información



- Cuando un usuario inicie o termine su vinculación laboral con CONFIAR SEGURIDAD LTDA, sea trasladado a otra sede o seccional, o por alguna otra circunstancia deje de utilizar el computador de escritorio, computador portátil o el recurso informático asignado, deberá entregar dicho recurso formalmente al departamento de sistemas.

- Está prohibido el ingreso a las instalaciones de CONFIAR SEGURIDAD LTDA, de recursos informáticos que no sean propiedad de la entidad, computadores, dispositivos de almacenamiento magnéticos.

- El ingreso y salida de computadores de escritorio, computadores portátiles y demás recursos informáticos de las instalaciones de CONFIAR SEGURIDAD LTDA, deben seguir el procedimiento establecido en el manual de activos fijos.

- La decisión del tipo de recurso que deberá utilizar es tomada en conjunto con el director del área, la Dirección administrativa y el jefe del departamento de Sistemas.

Manejo de **Información confidencial**

ACTIVOS DE INFORMACIÓN

Los terceros no podrán usar ningún activo de información de la organización para su beneficio propio. Y se comprometen a no divulgar información sin autorización previa.

Los terceros deben acogerse a cumplir todo lo estipulado en este documento y los procedimientos asociados para cualquier activo de información propiedad de la organización.

Los terceros deben garantizar el uso apropiado de los activos de información, y delos pilares de seguridad de la información (confidencialidad, disponibilidad e integridad), así como los derechos de propiedad intelectual. Esto durante todo el desarrollo de sus labores y desarrollo del contrato.

En los dispositivos removibles de almacenamiento custodiados por el tercero que contenga información de la organización, se usarán métodos de cifrado para proteger esta información y esta solo será accedida por personal autorizado.

Los procesos, documentos, actividades, entre otros que realicen los terceros Durante la ejecución del contrato son de propiedad intelectual de la organización.

El tercero debe seguir los procedimientos establecidos por la organización, para la conservación, borrado seguro y/o destrucción final de los activos de información.

Confiar ltda. seguridad

Manejo de **Información confidencial**

Los terceros a los que se les asigne herramientas de trabajo como (PC, Celular, SimCard, entre otros) deben devolver estos activos de información cuando la organización lo requiera y/o en la finalización de relaciones comerciales.
Los terceros tendrán acceso solamente a información que esté relacionada con el contrato o necesaria para el desarrollo de sus labores que mantienen con La organización.

Políticas de la **Seguridad de la información**

Uso y protección de la información

CONFIAR SEGURIDAD LTDA debe facilitar los mecanismos para que la información que se maneja a través de los recursos informáticos sea veraz, integra, oportuna y fluya de manera adecuada dentro de la empresa y hacia los clientes, proveedores, socios comerciales, entidades de control y otras terceras partes interesadas, garantizando la protección de la misma de divulgación o modificación no autorizada.

Política Dirigida a: Todos los Usuarios

Los usuarios son responsables por el buen uso de la información de CONFIAR SEGURIDAD LTDA, sea que la obtengan de documentos, medios magnéticos o electrónicos. Los usuarios que se encuentren conectados a la red corporativa de CONFIAR SEGURIDAD LTDA, deben garantizar la oportunidad, veracidad, exactitud, confiabilidad y disponibilidad de la información electrónica que generan.

Políticas de la

Seguridad de la información

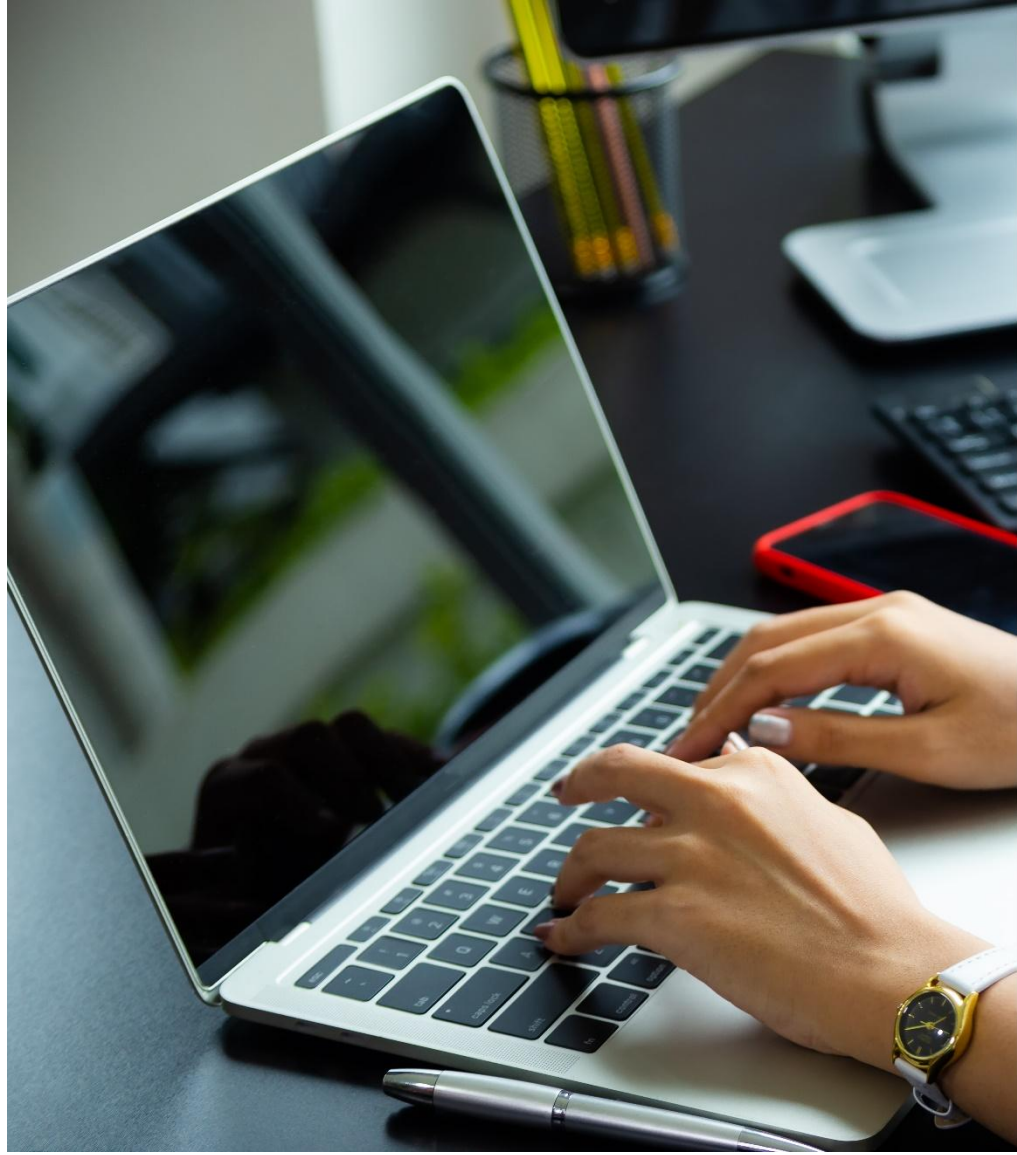
Se debe imprimir solo lo que es estrictamente necesario.

Se prohíbe hacer uso de las impresoras de CONFIAR SEGURIDAD LTDA. para la impresión de documentos no corporativos, es decir de tipo personal.

Verificar el equipo multifuncional o impresora y las áreas adyacentes para asegurarse de que no queden copias adicionales. Si encuentra copias adicionales destrúyalas.

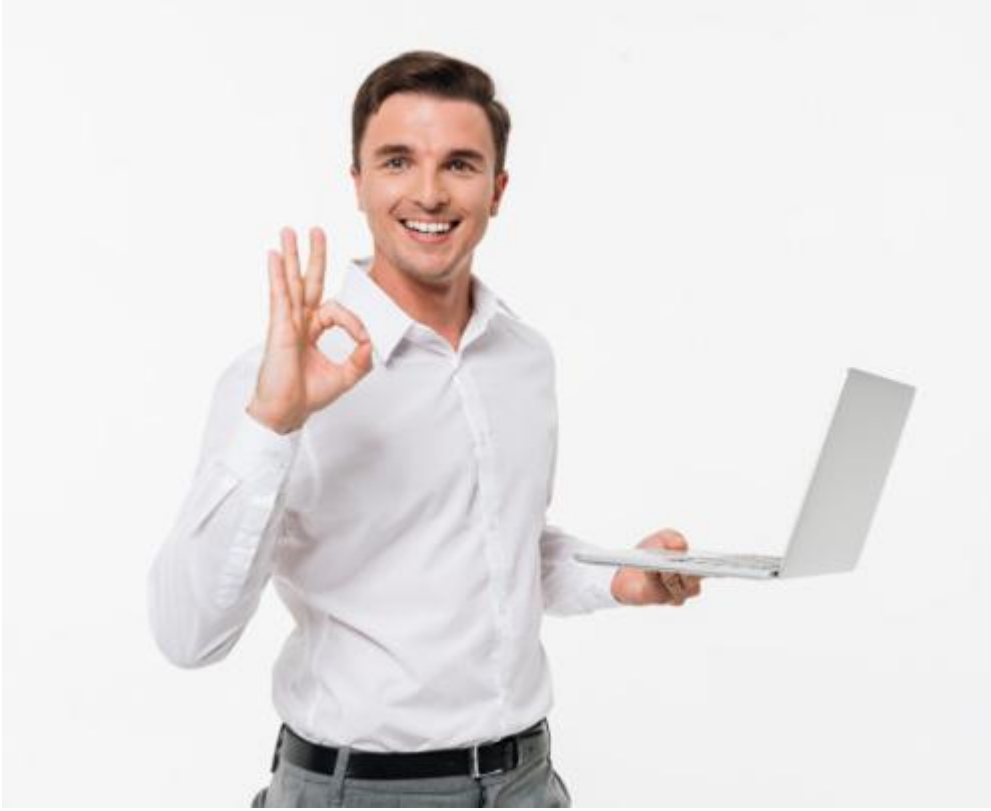
Gestión de cuentas de usuarios y contraseñas.

Cada usuario debe tener asignado un código de identificación y/o cuenta de usuario único y contraseñas, para el ingreso a los servicios informáticos a los cuales se le hayan dado privilegios de acceso, el cual no debe ser compartido con ninguna otra persona.



Políticas de la

Seguridad de la información



Protección frente a software malicioso

CONFIAR SEGURIDAD LTDA debe proteger sus recursos informáticos contra el acceso, modificación o daño permanente ocasionados por la contaminación y el contagio de software malicioso. Por tal razón, debe tomar las medidas necesarias para evitar que este tipo de contagio, en cualquiera de sus formas, se presente en los servidores, computadores de escritorio, computadores portátiles y en general, cualquier dispositivo que se conecte a las redes de la empresa.

Uso del correo electrónico

La cuenta de correo asignada es de carácter individual e intransferible, por lo tanto, ninguna persona bajo ninguna circunstancia, debe usar una cuenta de correo que no se le haya asignado explícitamente.

No se permitirá el envío ni el recibo de mensajes de correo electrónico con archivos anexos con las extensiones VCBS, MP3, CHM, SCR, EXE, SHS, OCX, HTA, BMP, PIF, DLL, VCF, GIF, BAT, INI, HTR, AVI, WMV. WMA, WAV, ACC, COM, INF, HTT, PPS, entre otros.

Confiar ltda. seguridad

Políticas de la **Seguridad de la información**

Se prohíbe enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a un tercero, identificarse como una persona ficticia o no identificarse.

Acceso a Internet

Los usuarios de CONFIAR SEGURIDAD LTDA a quienes se les otorgue el privilegio de navegación por Internet deben utilizarlo como una herramienta de consulta, para propósitos de las funciones del negocio, acatando y respetando las Políticas vigentes alrededor de su uso, se restringirán accesos a paginas web no laborales.

Copias de Respaldo

Todos los empleados de CONFIAR SEGURIDAD LTDA, al igual que los funcionarios suministrados por terceras partes, son responsables por la confiabilidad y oportunidad de la información que emiten o procesan y, es su deber identificar las fuentes de información que requieran protección electrónica e informar de éste requerimiento al departamento de sistemas de tal manera que ésta pueda aplicar los mecanismos que sean necesarios.

Confiar ltda. seguridad

Políticas de la **Seguridad de la información**

Se prohíbe enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a un tercero, identificarse como una persona ficticia o no identificarse.

Acceso a Internet

Los usuarios de CONFIAR SEGURIDAD LTDA a quienes se les otorgue el privilegio de navegación por Internet deben utilizarlo como una herramienta de consulta, para propósitos de las funciones del negocio, acatando y respetando las Políticas vigentes alrededor de su uso, se restringirán accesos a paginas web no laborales.

Copias de Respaldo

Todos los empleados de CONFIAR SEGURIDAD LTDA, al igual que los funcionarios suministrados por terceras partes, son responsables por la confiabilidad y oportunidad de la información que emiten o procesan y, es su deber identificar las fuentes de información que requieran protección electrónica e informar de éste requerimiento al departamento de sistemas de tal manera que ésta pueda aplicar los mecanismos que sean necesarios.

Confiar ltda. seguridad

Políticas de la **Seguridad de la información**

MANTENIMIENTO DE LOS EQUIPOS
El área encargada del mantenimiento de los activos de información debe definir un plan de mantenimiento donde se realicen revisiones y/o pruebas periódicas de acuerdo con las especificaciones del proveedor y/o fabricante. Esto para garantizarla integridad del activo.

El área encargada del mantenimiento de los activos de información debe mantenerlos registros de todas las actividades de mantenimiento (preventivo y/o correctivo).Además, se debe garantizar que esta actividad es desarrollada por personal que cuenta con estas habilidades y conocimiento.

Confiar ltda. seguridad

Políticas de la Seguridad de la información

APLICACIONES
Se entiende por aplicación un tipo de software diseñado para realizar un grupo de funciones, tareas o actividades coordinadas para el beneficio del usuario.

1.Se debe garantizar seguridad en las aplicaciones, con segregación de acceso y nivel de acceso a los datos funcionales de la aplicación..

2.La administración de accesos en aplicativos será responsabilidad del administrador de la aplicación.

3. Los lideres de proceso deben definir el listado de servicios de red a los que tendrá acceso cada uno de los colaboradores, de acuerdo con su cargo.

MENSAJERIA INSTANTANEA Y REDES SOCIALES
La información que se publique o divulgue -a título personal- por cualquier medio de internet por funcionarios, contratistas y proveedores, en redes sociales como -pero sin limitarse a los siguientes: Twitter®, Facebook®, YouTube®, blogs, Instagram, se considera fuera del
alcance del Sistema de Gestión de Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que lo genere.

El uso de WhatsApp con fines laborales debe ser aprobado por el departamento de TI o Seguridad de la Información.

Se prohíbe el uso de WhatsApp para compartir información clasificada como confidencial o sensible sin autorización previa.

Uso exclusivo para comunicación empresarial: WhatsApp solo debe utilizarse para conversaciones laborales y nunca para compartir información personal o confidencial sin autorización.

Privacidad y protección de datos: No se deben compartir datos sensibles o documentos estratégicos a través de WhatsApp sin cifrado adicional o autorización previa.

Evitar almacenamiento de información crítica: Se recomienda no almacenar conversaciones con datos sensibles en la aplicación; en su lugar, utilizar sistemas internos seguros.

Autenticación y seguridad de dispositivos: Los usuarios deben habilitar la verificación en dos pasos y emplear métodos de autenticación seguros en sus dispositivos móviles.

Confiar ltda. seguridad

Políticas de la Seguridad de la información

Uso responsable de multimedia: No se debe compartir material que pueda infringir derechos de autor o normas internas de la empresa.

No se debe enviar contraseñas, datos personales sensibles, información financiera o propiedad intelectual a través de WhatsApp.

DISPOSITIVOS Y ACCESO:

Se debe eliminar regularmente el historial de chats que contengan información comercial.

El uso de WhatsApp para tareas laborales solo está permitido en dispositivos móviles protegidos con contraseña o biometría.

En caso de pérdida o robo del dispositivo, se debe notificar inmediatamente al área de TI.

Se prohíbe el uso de WhatsApp Web en computadoras públicas o no autorizadas.

RESPONSABILIDADES

Todo contenido compartido debe mantener un lenguaje profesional.

Está prohibido el envío de mensajes no solicitados (spam), contenido ofensivo o discriminatorio.

El colaborador es responsable de las comunicaciones emitidas a través de su número.

Los Usuarios deben cumplir con las normas establecidas en esta política y reportar cualquier incidente de seguridad al departamento de TI

El incumplimiento de esta política puede derivar en acciones disciplinarias, incluyendo restricciones en el acceso a herramientas corporativas y medidas legales en casos graves de vulneración de datos.

SUPERVISION Y AUDITORIA

CONFIAR SEGURIDAD se reserva el derecho de auditar el uso corporativo de WhatsApp para asegurar el cumplimiento de esta política.

No se realizarán revisiones de contenido privado sin causa justificada y sin respetar la legislación vigente en materia de privacidad.

Confiar ltda. seguridad

CONTROL DE CAMBIOS

FECHA DEL CAMBIO	MOTIVO DEL CAMBIO	VERSION	QUIEN APRUEBA ELCAMBIO
17/09/2024	En la política de Seguridad de la información se incluye el uso de WhatsApp para tareas laborales	1	Gerencia General
16/05/2025	En la política de Seguridad de la información se incluye: objetivos, alcance de la política, mantenimientos, acceso a redes sociales y uso aceptable de los activos de la información	2	Gerencia General