



**TI-ES-01**

**POLÍTICA DE SEGURIDAD DE LA  
INFORMACIÓN**

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

seguridad en cómputo.

- Mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.
- Monitorear constantemente el envío de documento sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de red.
- Revisar aleatoriamente los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Comunicar al Gerente General los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.
- Verificar el grado de seguridad del software adquirido e instalado en los equipos.

### 5.5 Uso de Dispositivos Móviles Corporativos

- El área de Tecnología debe establecer las configuraciones aceptables para los dispositivos móviles corporativos que hagan uso de los servicios.
- El área de Tecnología cuando lo crea conveniente debe instalar un software de antivirus tanto en los dispositivos móviles corporativos que hagan uso de los servicios provistos por parte de People Marketing S.A.S.
- No se deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega por parte de los usuarios.
- Los usuarios deben evitar usar los dispositivos móviles corporativos en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas.
- Contar con las actualizaciones de las aplicaciones que utiliza el dispositivo móvil para su funcionamiento y aquellas que contribuyan a los servicios que ofrece la empresa.
- Se debe evitar hacer uso de redes inalámbricas de uso público, así como desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos.
- Se debe evitar conectar los dispositivos móviles corporativos asignados por puerto USB a cualquier computador público.
- Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles corporativos asignados.
- El área de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

### 5.6 Uso de Dispositivos Móviles Personales

- People Marketing S.A.S ha establecido dentro del reglamento interno de trabajo: *Art. 43 Son obligaciones especiales del trabajador: “N°24. Abstenerse de usar el celular para asuntos personales, en las áreas donde está expresamente prohibido o dentro de la jornada laboral”.*

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

- El uso de los dispositivos móviles personales, está permitido para los cargos Gerenciales, Directivos, Coordinadores y aquellos quienes la organización apruebe como necesarios para la ejecución de tareas específicas.
- La autorización del uso de los dispositivos móviles personales, será informada en el proceso de ingreso del personal a la compañía, previa revisión de las funciones y responsabilidades de su cargo.

#### 5.7 Uso de Conexiones Remotas

- El área de Tecnología debe restringir las conexiones remotas; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma de People Marketing S.A.S o de sus clientes y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores público.
- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- Reservar las direcciones de entrada (direcciones IP o direcciones Web) al igual que las credenciales que les han sido otorgadas para su resguardo.
- Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones de People Marketing S.A.S

#### 5.8 Uso de Servicio de Internet

- El acceso a Internet es provisto a los usuarios de People Marketing S.A.S para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la empresa, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el área de Tecnología
- El área de Tecnología puede bloquear y denegar algunos accesos a páginas para optimizar el ancho de banda de Internet para su total aprovechamiento.

#### 5.9 Uso de Correo Electrónico

- Se debe hacer uso del correo electrónico, acatando todas las disposiciones de seguridad diseñadas para su utilización y evitar el uso o introducción de software malicioso a la red corporativa.
- El correo electrónico es de uso exclusivo, para los empleados y contratistas de la People Marketing.S.A.S
- Todo uso indebido del servicio de correo electrónico, será motivo de llamado de atención
- El usuario será responsable de la información que sea enviada con su cuenta.
- El administrador de la red corporativa, se reservará el derecho de monitorear las cuentas de usuarios, que presenten un comportamiento sospechoso para la seguridad de la red.
- El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

- El usuario debe tener en cuenta que el correo electrónico por capacidad solo envía archivos de capacidad máximo de 15 MB por lo que hace no optimo el envío del mismo
- El personal de Help Desk realizar la verificación de tamaño de buzón
- El responsable en el área de Tecnología deberá cancelar o suspender las cuentas de los usuarios previa notificación, cuando se le solicite mediante un correo electrónico explícito por directores o coordinadores en los siguientes casos:
  - a. Si la cuenta no se está utilizando con fines institucionales
  - b. Si pone en peligro el buen funcionamiento de los sistemas
  - c. Si se sospecha de algún intruso utilizando una cuenta ajena

#### 5.10 Administración de Autenticación de Equipo Tecnología – Data Center

- El acceso físico al Data Center solo puede ser ejecutado por el analista HelpDesk o el Director del área de Tecnología e Infraestructura. Las personas que ocupen estos cargos deben firmar un acuerdo de confidencialidad cada año que oficializa la responsabilidad de los accesos al Data Center.
- El acceso al Data Center solo puede ser realizado mediante control biométrico registrado por las personas responsables. En caso del cese de personal de uno de estos cargos como parte de su proceso de cese la persona debe registrar la huella de su reemplazo y la persona en reemplazo eliminar la huella del responsable anterior.
- Además, existe una tarjeta de emergencia para acceso único sellada bajo llave con permisos de la Gerencia General.
- Para accesos de proveedores o personal de mantenimiento se deben llenar los datos personales el cuaderno de visitas (nombres y apellidos, tipo de documento, numero de documento, fecha de ingreso, fecha de salida y responsable encargado) por una de las personas responsables. La única forma de ingreso es a través de un usuario responsable.
- Las medidas de seguridad física son:
  - Temperatura: Termómetro digital y ventilación
  - Vigilancia: Cámaras de seguridad con grabación de hasta 3 días
  - Energía Eléctrica: UPS de 6 kva
  - Contra incendios: Dispositivos extinguidores CO2
  - Elevamiento: Rack elevado y cableado superior
- Estas medidas de seguridad tienen una revisión mensual de disponibilidad. Los extintores deben tener una recarga y revisión anual de acuerdo a las políticas de Seguridad y Salud en el Trabajo.
- La UPS de People Marketing garantiza al menos 30 minutos de disponibilidad, adicional a ello la UPS del local en el que se encuentra People Marketing garantiza 24 horas de disponibilidad.
- La UPS garantiza disponibilidad únicamente en el circuito cerrado eléctrico de People Marketing etiquetado físicamente como UPS-6.

#### 5.11 Administración de Autenticación de Equipo Tecnología – Servicios Cloud

- El acceso a la consola de administración de AWS solo lo realiza el Director de Tecnología e Infraestructura y el acceso a los servicios de Microsoft o Google Suite solo lo realiza el Director de Tecnología e Infraestructura y el Analista de Help Desk. Ambas con doble factor.
- La única persona responsable de la creación de servidores virtualizados en AWS es el Director de Tecnología e Infraestructura. Estos servidores cuentan con seguridad para conexiones SSH y sólo accesible por Grupos de claves (.pem) con encriptación RSA.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

- Las bases de datos en AWS requieren de una conexión encriptada por SSL por lo cual solo los sistemas que cuenten con las llaves de SSL pueden conectarse a esas bases de datos. Los usuarios requieren también una llave de SSL además de los permisos de autenticación en MySQL.

#### 5.12 Administración de Autenticación de Usuarios Finales – Software y redes

- Todo equipo informático de People Marketing debe estar registrado en el Directorio Activo de People Marketing.
- En el Directorio Activo, el analista Help Desk o el Director de Tecnología e Infraestructura debe crear los usuarios y contraseñas de los usuarios con la funcionalidad de cambio de contraseña en la primera sesión.
- Las credenciales iniciales se entregan en el acta de entrega de accesos como parte del proceso de inicio de labores del personal.
- Durante el proceso de cese de personal el analista de Help Desk o el Director de Tecnología e Infraestructura debe de inhabilitar el usuario antes de firmar el acta de salida de la persona.
- Los usuarios finales tienen políticas administradas en el Directorio Activo de People Marketing las cuales prohíben las siguientes funcionalidades:
  - Instalación de aplicaciones sin usuarios administradores
  - Creación de usuarios
  - Restricción de páginas web y puertos
  - Cambios de contraseñas

#### 5.13 Administración de Autenticación de Usuarios Finales – Instalaciones y puestos de trabajo

- Solo el personal clave autorizado por la Gerencia General cuenta con acceso biométrico a las oficinas de People Marketing dentro de los cuales se encuentra el Director de Tecnología e Infraestructura y el analista Help Desk.
- Para el personal de Call Center, el analista Help Desk o el Director de Tecnología e Infraestructura debe de configurar la huella de acceso principal y secundaria para el acceso biométrico a la zona de Call Center. Esta configuración hace parte del proceso de ingreso de personal dentro del acta de entrega.
- El acceso al local de People Marketing se configura a través de la administración dle local mediante comunicación por correo y autenticación diaria por documento de identidad.
- En caso de olvido o extravío de información de la cuenta personal, para brindarse al usuario que lo necesite, siempre y cuando lo solicite por la plataforma de People Marketing S.A.S

#### 5.14 Contraseñas

- Los códigos de usuario y contraseñas o los mecanismos de acceso, son de uso personal e intransferible, por lo tanto los colaboradores son responsables de todas las actividades llevadas a cabo con su código de usuario y su contraseña personal.
- Las contraseñas se crean con mínimo siete caracteres, combinados entre letras mayúsculas, minúsculas, números y caracteres especiales tales como \*, &, \$, @, <, >, entre otros.
- En la selección de la contraseña, elegir una de fácil memorización, hecha con ayuda de acrónimos (formada al unir las letras iniciales de las palabras de una frase) o de asistencias mnemónicas (técnicas para facilitar el recuerdo de algo), que la hagan difícilmente reconocible a otros. Excluir términos como nombres propios, nombres de producciones, palabras del diccionario, aún si son terminados con números.
- El usuario deberá renovar su contraseña y colaborar en lo que sea necesario, a solicitud del área de tecnología e infraestructura

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

- Memorizar la contraseña creada. Evitar anotar la contraseña en papeles pegados al computador o dispuestos bajo el teclado, en gavetas o carteras. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.
- Evitar hacer uso de información personal para construir la contraseña, tales como nombres (propios o de familiares), nombre de usuario (username o login), nombres de mascotas, número telefónico, dirección o fechas de cumpleaños.
- Evitar emplear la misma contraseña para todos los aplicativos y equipos. De esta forma si un sistema está comprometido, los demás podrán estar fuera de peligro inmediato
- Las palabras comunes invertidas son contraseñas poco fiables. Ejemplo: "nauj". El invertirlas no agrega complejidad para los posibles intrusos.
- Evitar utilizar repeticiones de más de dos caracteres en la contraseña.
- Evitar el uso de palabras de idiomas extranjeros como contraseña. Los programas de descifrado verifican con diccionarios de muchos idiomas.
- Para seleccionar la clave piense en una frase (de un libro, de una película, una frase común, etc.), seleccione un número de un hecho memorable, cambie la frase a un acrónimo (incluyendo la puntuación) si la frase es muy larga o use la misma frase si la considera corta, e incluya el número, agregue un poco de complejidad sustituyendo letras por símbolos. Por ejemplo, punto (.) por asterisco (\*), la letra 'a' por arroba '@', la letra 's' por signo pesos "\$", etc., añada un poco más de complejidad colocando mayúscula al menos a una letra. Ejemplo: AmOL@\$Contr@\$eña\$1810.
- El usuario podrá definir su contraseña y será responsable de la confidencialidad de la misma.
- Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.
- Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.

#### 5.15 Backup

- Se realiza el backup de la información en la nube a través de la infraestructura AWS de People Marketing S.A.S para todos los sistemas realizados por People Marketing y basados en AWS.
- El respaldo de información de cada equipo informático es responsabilidad de cada funcionario, por lo cual en caso de pérdida de documentos trabajados que no hayan sido almacenados en la nube no son responsabilidad del área de Tecnología e Infraestructura.
- Para dar un segundo respaldo de la información el analista de Help Desk realiza backup a los siguientes servidores o IP



	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

#### 5.17 Antivirus de la Red

- Deberán ser utilizadas en la implementación y administración de la Solución Antivirus por parte del área de Tecnología e Infraestructura
- Todos los equipos de cómputo de People Marketing S.A.S. deberán tener instalada la Solución Antivirus.
- Todos los usuarios de People Marketing S.A.S no deberán desinstalar la solución antivirus de su computador pues ocasiona un riesgo de seguridad ante el peligro de virus.
- Se debe contactar al área de Tecnología e Infraestructura
  - a) Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la empresa.
  - b) Cuando sus archivos resulten con daños irreparables por causa de virus.
  - c) Cuando viole las políticas antivirus.

#### 5.18 Uso de Escritorio y Pantallas

- Es una responsabilidad de cada uno de los funcionarios y personal contratista
- Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información que se considere privada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.
- En la medida de lo posible los documentos con información que se considere privada debe quedar bajo llave o custodia en horas no laborables.
- Se deben controlar la recepción, flujo envío de documentos físicos en People Marketing S.A.S por medio de registro de sus destinatarios desde el punto de correspondencia.
- Al imprimir o fotocopiar documentos con información privada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.
- No se debe enviar ni recibir documentos clasificados o reservados por medio de Fax.
- No se debe reutilizar papel que contenga información privada de People Marketing S.A.S.

#### 5.19 Centro de Datos y Centro de Cableado

- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte
- En las instalaciones del centro de datos o de los centros de cableado, no se permite, fumar, consumir alimentos, mover o desconectar equipos, alterar software instalado en los equipos sin autorización, alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas
- Extraer información de los equipos en dispositivos externos
- Abuso y/o mal uso de los sistemas de información
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice
- Cada gabinete o armario contiene llave de ingreso y/o tarjeta de proximidad, así como cada centro de cableado, las cuales deben permanecer almacenadas en la debida caja de seguridad de doble factor dispuesta para ello dentro del centro de cómputo
- Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

## 5.20 Seguridad del Personal

El área de recursos humanos de People Marketing S.A.S se asegura que los funcionarios, contratistas y demás colaboradores de People Marketing S.A.S, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información, el conocimiento de las políticas de seguridad de la información a través del GH-FO-15 **acuerdo de confidencialidad** que asegura que los funcionarios, contratistas y demás colaboradores, entiendan sus responsabilidades, como usuarios con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Los funcionarios, contratistas y demás que estén vinculados deben dar aprobación a People Marketing S.A.S en el formato **GH-FO-11 Autorización de manejo y tratamiento de datos personales** para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

## 5.21 Seguridad en Acceso a Terceros

- El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo o asociación para el servicio, el cual deberá estar firmado por las involucradas en el mismo.
- Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.
- Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de People Marketing S.A.S., además de los requisitos expuestos en su contrato/convenio.

## 5.22 Seguridad Física de Instalaciones

People Marketing S.A.S cuenta con cámaras de seguridad para ayudar a grabar cualquier actividad que se desarrolle alrededor de las áreas donde están ubicadas e instaladas en la oficina principal y en las bodegas, las cuales pueden ser monitoreadas durante las veinticuatro (24) horas por parte del Director de Tecnología e Infraestructura, el analista de Help Desk y demás usuarios de la compañía autorizados. Es recomendable realizar el acceso a la IP por Internet Explorer y configurar los plugins correspondientes, posteriormente ingresar al DVR (HIK VISION), con el usuario y contraseña asignado.

Las cámaras utilizadas en People Marketing S.A.S son conocidas como cámaras IP que envían las señales captadas al enrutador inalámbrico de la empresa. La información de las cámaras se respalda automáticamente en el disco DVR durante 5 días.



	<b>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>CODIGO:</b>	TI-ES-01
		<b>VERSIÓN:</b>	6
		<b>FECHA DE VIGENCIA:</b>	01/03/2022

### 5.23 Disposiciones Finales:


El incumplimiento a los parámetros establecidos en la presente política, será considerado como falta disciplinaria y se evaluarán de acuerdo al reglamento interno de trabajo de People Marketing S.A. S. Artículo 47, literal d) *“La falta disciplinaria diferente a las antes mencionadas, que implique, a juicio del empleador, la violación por parte del trabajador de cualquiera de las obligaciones legales, contractuales, o reglamentarias, o si éste incurriere en una conducta prohibida, y que el empleador considere aún como leve, implica por primera vez, suspensión en el trabajo hasta por ocho (8) días y por segunda vez suspensión en el trabajo hasta por dos (2) meses”*

## 6. DOCUMENTOS ASOCIADOS

CODIGO	NOMBRE DEL DOCUMENTO
GE-ES-03	Reglamento Interno de Trabajo
TI-FO-05	Inventario de Software People Marketing S.A.S.
GH-FO-11	Autorización de Manejo y Tratamiento de Datos Personales
SST-FO-18	Control de Visitantes
GH-FO-15	Acuerdo de Confidencialidad

## 7. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
1	Creación de documento	30/11/2015
2	<ul style="list-style-type: none"> <li>Actualización de información y estandarización de documento.</li> <li>Unificación de documentos back up, y contraseñas aplicadas.</li> <li>Optimización de actividades e información</li> </ul>	18/09/2018
3	<ul style="list-style-type: none"> <li>Modificación del objetivo</li> <li>Actualización de responsabilidades</li> <li>Actualización de definiciones</li> <li>Se incluyen lineamientos para el uso de dispositivos móviles (celulares) personales.</li> <li>Se anexa descripción de las sanciones que se derivan por el incumplimiento de la Política (Disposiciones finales)</li> </ul>	28/01/2019
4	<ul style="list-style-type: none"> <li>Modificación de responsabilidades</li> </ul>	15/02/2021
5	<ul style="list-style-type: none"> <li>Modificación de Uso de Dispositivos Móviles Personales</li> <li>Modificación de Centro de Datos y Centro de Cableado</li> </ul>	28/01/2022

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN		CODIGO:	TI-ES-01	
			VERSIÓN:	6	
			FECHA DE VIGENCIA:	01/03/2022	
Elaborado Por: Original Firmado		Revisado Por: Original Firmado		Aprobado Por: Original Firmado	
Carlos Mesia Gonzales Director de Tecnología				Juan Manuel Casas Gerente General	