

|   |  |                                 |                                |
|---|--|---------------------------------|--------------------------------|
|  | POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN |                                 | CÓDIGO: M.SI.P21<br>VERSIÓN:02 |
|   | FECHA DE EMISIÓN: 20/05/20222                        | FECHA ÚLTIMO CAMBIO: 10/07/2023 | Página 1 de 5                  |

## POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Alta dirección establece las condiciones necesarias para el acceso a los recursos de red y activos de información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** a través de los dispositivos de tecnología móviles (computadores, portátiles, celulares, tabletas, o cualquier tipo de dispositivos electrónicos con capacidad de acceso a las redes).

La autorización de conexión de dispositivos móviles a las redes de datos de la Entidad se realiza una vez se identifican, gestionan y mitigan los riesgos de seguridad de la información asociados al uso de dispositivos.

### 1. ALCANCE

La presente política aplica a todos los trabajadores, colaboradores, contratistas y terceros que accedan a través de dispositivos y equipos móviles que estén autorizados para conectarse a las redes de datos y comunicaciones de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, a la información organizacional o a cualquier servicio de tecnologías de la información y comunicación de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**. Igualmente, para todos trabajadores colaboradores, contratistas y terceros que tengan acceso a información de cualquier tipo de información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**

### 2. OBJETIVO GENERAL

Establecer las condiciones para el manejo de los dispositivos móviles organizaciones o personales que accedan a información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** y velar por el uso responsable de los mismos de acuerdo con los lineamientos de las políticas de seguridad de la información en la organización.

### 3. LINEAMIENTOS

El Coordinador de Mejoramiento Continuo debe definir y dar seguimiento al cumplimiento de la Política de dispositivos móviles de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**.

Los dispositivos móviles de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** son una herramienta de trabajo y deben ser utilizados exclusivamente para las comunicaciones de los colaboradores y/o contratistas, en desarrollo de las funciones laborales o de las obligaciones contractuales correspondientes

La Gerencia de Tecnología y Operaciones y la Dirección de Tecnología están autorizadas para realizar la desactivación, eliminación y/o retiro de los permisos de acceso de las aplicaciones y/o cuentas de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** cuando el dispositivo móvil haya sido extraviado, hurtado o se presente algún evento que comprometa la seguridad de la información organizacional.

|  |   |                                 |                                |
|--|---|---------------------------------|--------------------------------|
|  | <b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 | CÓDIGO: M.SI.P21<br>VERSIÓN:02 |
|  | FECHA DE EMISIÓN: 20/05/20222                               | FECHA ÚLTIMO CAMBIO: 10/07/2023 | Página 2 de 5                  |

El acceso a todos los dispositivos móviles con acceso a información organizacional debe estar configurado con contraseña segura y bloqueo automático.

La Gerencia de Tecnología y operaciones y la Dirección de Tecnología adoptan e implementan los mecanismos de seguridad necesarios para salvaguardar la información contenida y transmitida mediante el uso de dispositivos móviles de los colaboradores, contratistas y terceros de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, a través de los cuales se les autoriza el acceso a los recursos tecnológicos de la organización.

En cualquier momento el coordinador de mejoramiento continuo podrá hacer revisión del cumplimiento de la presente política directamente en los dispositivos móviles.

El equipo de trabajo encargado de realizar las auditorías internas o externas que se realicen al Sistema de Gestión de Seguridad de la Información -SGI de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, podrá realizar la verificación de las configuraciones de seguridad de los equipos móviles y su cumplimiento con los lineamientos de esta política.

#### **4. SEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES QUE ACCEDAN A INFORMACIÓN DE PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**

El acceso a la información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** a través de dispositivos móviles de propiedad de los colaboradores contratistas y/o terceros se autorizará previa solicitud de los líderes de los procesos a través de correo electrónico y posterior autorización por parte del Gerente y visto bueno de la Gerencia de Tecnología y Operaciones y la Dirección de Tecnología.

No está permitido transferir ni almacenar la información clasificada, reservada o sensible de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** en los dispositivos móviles privados, ni en sitios o redes públicas como cafés internet, servicios de nube gratuitos, correos electrónicos personales, WhatsApp, OneDrive, Google Drive, Dropbox, ni cualquier otro medio NO autorizado por la Gerencia de Tecnología y Operaciones y la Dirección de Tecnología de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**.

Se debe hacer uso de las herramientas y medios suministrados por la Gerencia de Tecnología y Operaciones y la Dirección de Tecnología de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** para almacenar, transmitir, procesar y en general para tratar la información a que tenga acceso mediante el uso de dispositivos móviles personales.

En el momento de cesar la vinculación laboral o relación contractual que dio lugar a la autorización para el uso de dispositivos móviles privados para acceder a la información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, se deben eliminar los accesos a aplicaciones de la Entidad en los que se almacene o transmita la información organizacional, como por ejemplo el correo electrónico institucional.

|   |   |                                 |                                |
|---|---|---------------------------------|--------------------------------|
|  | <b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 | CÓDIGO: M.SI.P21<br>VERSIÓN:02 |
|   | FECHA DE EMISIÓN: 20/05/20222                               | FECHA ÚLTIMO CAMBIO: 10/07/2023 | Página 3 de 5                  |

En caso de cambio, pérdida, hurto de un dispositivo móvil personal con acceso a la información de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** el colaborador, contratista o tercero a quien se le haya autorizado el uso del dispositivo, será responsable de informar con carácter urgente a su jefe inmediato de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, Gerencia de Tecnología y Operaciones y la Dirección de Tecnología a través de correo electrónico.

#### 5. SEGURIDAD DE DISPOSITIVOS MÓVILES DE PROPIEDAD DE PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN

Está prohibido almacenar información personal en los dispositivos móviles asignados por **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**. **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** no se hará responsable por la pérdida o eliminación de esa información.

Está prohibido cambiar en los equipos de propiedad de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** la configuración de seguridad o realizar instalación de aplicaciones o software no autorizadas por la Gerencia de Tecnología y Operaciones y la Dirección de Tecnología. Únicamente está autorizada la instalación de actualizaciones del software instalado. De igual manera, se prohíbe rootear o alterar el *software* instalado dentro del dispositivo. Cuando producto de cualquier modificación o alteración de los dispositivos se produzcan daños a **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** o a terceros, se podrá repetir patrimonialmente en contra de quien favoreció dicha vulneración o modificó dichos dispositivos.

Los colaboradores o contratistas que tengan asignados dispositivos móviles de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** no deben conectarse a través de redes inalámbricas públicas.

El sistema de mensajería instantánea autorizado para el uso en los dispositivos móviles de propiedad de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** es SoapBox, la cual debe ser instalada y configurada de acuerdo con las instrucciones emitidas por la Gerencia de Tecnologías y Operaciones y la Dirección de Tecnología.

Los colaboradores deben proteger física y lógicamente los dispositivos móviles asignados y que son de propiedad de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** para prevenir el hurto y/o acceso o divulgación no autorizada de la información organizacional.

En caso de pérdida o hurto de un dispositivo móvil de propiedad de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** el colaborador, contratista o tercero a quien haya sido asignado el dispositivo, será el(la) responsable de informar con carácter urgente a su jefe, a la Gerencia de Tecnología y Operaciones y la Dirección de Tecnología a través de los canales de comunicación autorizados.

#### 6. INCUMPLIMIENTO

El incumplimiento de la presente política traerá consigo las consecuencias legales que apliquen a **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, incluyendo lo establecido en las normas que

|  |   |                                 |                                |
|--|---|---------------------------------|--------------------------------|
|  | <b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 | CÓDIGO: M.SI.P21<br>VERSIÓN:02 |
|  | FECHA DE EMISIÓN: 20/05/20222                               | FECHA ÚLTIMO CAMBIO: 10/07/2023 | Página 4 de 5                  |

competen al Gobierno Nacional y Territorial en cuando a seguridad y privacidad de la información se refiere.

## 7. RESPONSABLES

### 7.1. Gerencia de Tecnologías y Operaciones y la Dirección de Tecnología:

- 7.1.1. Establecer las condiciones necesarias para garantizar el acceso de los colaboradores y contratistas de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** a los recursos de red y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, celulares, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes).
- 7.1.2. Designar el personal idóneo para que establezca los parámetros de seguridad y configure los accesos de los dispositivos móviles requeridos, adoptando los lineamientos de seguridad necesarios para garantizar la seguridad de la información organizacional.
- 7.1.3. Programar capacitaciones con el fin de sensibilizar y comunicar acerca de la presente política y sus actualizaciones, concientizando acerca de las consecuencias que puede traer dentro de la organización.
- 7.1.4. Programar auditorías con el fin de evaluar la seguridad de las redes, dispositivos y programas de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**.
- 7.1.5. Hacer uso, en caso de ser posible, de herramientas tales como el *legal hacking*, o *hacking ético* con el fin de robustecer la seguridad de los sistemas informáticos dentro de la organización.
- 7.1.6. Generar herramientas de bloqueo o desinstalación remota con el fin de evitar vulneraciones a la seguridad informática de la organización.
- 7.1.7. Designar mecanismos de protección ante código malicioso.

### 7.2. Coordinador de Mejoramiento Continuo:

- 7.2.1. Velar por el cumplimiento de la presente política, contribuyendo a la implementación de los niveles de seguridad adecuados para el uso de dispositivos móviles organizacionales.
- 7.2.2. Estudiar y evaluar las vulneraciones, en caso de que las haya, con el fin de tomar acciones correctivas.

### 7.3. Colaboradores y Contratistas:

- 7.3.1. Hacer uso responsable de los dispositivos móviles acogiendo los lineamientos establecidos por **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN** en la presente política.
- 7.3.2. Tomar todas las medidas necesarias con el fin de garantizar una adecuada seguridad de la información a la cual tenga acceso.

|   |   |                                 |                                |
|---|---|---------------------------------|--------------------------------|
|  | <b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 | CÓDIGO: M.SI.P21<br>VERSIÓN:02 |
|   | FECHA DE EMISIÓN: 20/05/2022                                | FECHA ÚLTIMO CAMBIO: 10/07/2023 | Página 5 de 5                  |

- 7.3.3. Comunicar de manera oportuna cualquier vulneración a la seguridad de los sistemas informáticos de la compañía.
- 7.3.4. Informar oportunamente la pérdida o hurto de los dispositivos tanto propios del colaborador o trabajador en los cuales hay información que le pertenece a **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**, como de aquellos equipos que son de propiedad de **PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN**.
- 7.3.5. Darle cumplimiento a la presente política.

Esta política será revisada como mínimo una vez al año y de requerirse será actualizada con los cambios en materia de Seguridad de la Información.

#### 8. FECHA DE ENTRADA EN VIGENCIA

Esta política entrará en vigencia desde el 10/07/2023

Cualquier cambio que se presente respecto de la presente política, se informará a través de la página web [www.peoplecontact.com.co](http://www.peoplecontact.com.co) o el correo electrónico [contacto@peoplecontact.com.co](mailto:contacto@peoplecontact.com.co); [habeasdata@peoplecontact.com.co](mailto:habeasdata@peoplecontact.com.co) o para quienes soliciten la información directamente en las sedes ubicadas en Manizales, calle 19 Av. Bernardo Arango 16 – 04 y Bogotá, calle 72 13 -23 Edificio NuevaGranada.

Atentamente,



**DIEGO HERNANDO CEBALLOS LÓPEZ**  
**GERENTE**  
**PEOPLE CONTACT S.A.S. EN REESTRUCTURACIÓN S.A.S.**

Visto bueno asesor  
 jurídico  
 29/05/2023

Jorge Eliecer Ruiz Sierra

  
**DOXA** S.A.S  
 Soluciones Jurídicas

