A los efectos de la presente política se consideran dispositivos móviles los teléfonos celulares inteligentes, tabletas, lectores tipo PDA, handheld y computadores portátiles (laptops, netbooks, etc.).

Condiciones de uso

Los dispositivos móviles provistos por Cartolito deben utilizarse para actividades de carácter laboral. La Gerencia de Desarrollo de Proveedores, Compras y MP es responsable de entregar dispositivos móviles (celulares), así también como de realizar cancelaciones, modificaciones y solicitud de equipos de reposición mediante el formato **F-AL-63 Red Cartolito.**
Cuando el dispositivo móvil de Cartolito sea requerido y/o solicitado por parte del departamento de Sistemas, ya sea ser por razones de auditoría, administración o configuración, los usuarios deberán de entregarlos al solicitante.

El usuario debe tener el debido cuidado de la integridad física del dispositivo.
Los usuarios no tienen permitido realizar ni autorizar ningún arreglo y/o servicio de reparación para el dispositivo que tenga asignado.

Pérdida o robo de dispositivos de Cartolito.

Es responsabilidad del usuario tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.
Si el dispositivo está perdido, robado o se sospecha que está comprometido en cualquier sentido, el usuario debe notificar inmediatamente a la Gerencia de Desarrollo de Proveedores, Compras y MP de la situación y realizar la denuncia correspondiente. Esta notificación y la denuncia deben tener lugar para poder cancelar cualquier servicio móvil asociado al dispositivo, así como también el departamento de sistemas debe de borrar remotamente la información contenida en la memoria del mismo en la medida de lo posible.

Aplicaciones y descargas en dispositivos de Cartolito.

Todo el software para el dispositivo debe ser provisto e instalado o aprobado por el departamento de Sistemas

Respaldo, administración de archivos, sincronización y antivirus

El software necesario para realizar respaldos, sincronización de datos y de contactos será proporcionado y/o autorizado por el departamento de Sistemas. Es responsabilidad del usuario: Colocar todos los archivos de trabajo en la carpeta configurada en el dispositivo para que se generen los respaldos de la información contenida.
Notificar al departamento de Sistemas cuando detecte un incorrecto funcionamiento del antivirus o ante sospecha de desactivación u otra anomalía.

Funcionalidades y características de manejo

El Hardware, sistema operativo y utilitarios que vienen instalado de fábrica y forman parte del dispositivo no deben sufrir cambios a menos que hayan sido requeridos y autorizados por el departamento de Sistemas y/o según corresponda. No está permitido que el usuario realice el desbloqueo de las limitaciones del fabricante y/o proveedor que realice cualquier otro método de cambio de las protecciones.

Seguridad del Usuario

Se prohíbe a los conductores de cualquier tipo o categoría de vehículos, cuando circulen, el uso de dispositivos de telefonía móvil o cualquier otro medio o sistema de comunicación, excepto cuando el desarrollo de la comunicación tenga lugar sin emplear cualquiera de las manos.

Obligaciones de Seguridad y Privacidad para los datos de la empresa

Los usuarios deben tomar las apropiadas precauciones para prevenir que otras personas externas a la organización (familia, amigos, etc.) tengan acceso a los dispositivos móviles de Cartolito y los recursos asociados a los mismos. Los usuarios no deben:

- Compartir el dispositivo.
- Compartir usuario, contraseña, PIN u otro tipo de credencial.
- Tomar fotografías sin autorización dentro de la empresa.
- Si se va a retirar del dispositivo, asegurarse que éste quede bloqueado.

Nota 1. La toma de fotografías solo está permitida para tomar realizar instrucciones de trabajo, ayudas visuales, evidencia que solicita el cliente propio de la marca, maquinaria para solicitar refacciones a proveedores, esto previo aviso al departamento de seguridad y comité de seguridad de la información.

Nota 2. Es obligación del receptor de una visita de un cliente y/o proveedor el que no se ingrese con un dispositivo móvil dentro de las áreas operativas.

Buenas prácticas para la protección de los datos

Los usuarios de dispositivos móviles deben cumplir con las políticas de seguridad tanto cuando los usen en el puesto de trabajo como cuando estén fuera de la empresa.
Las instalaciones no gestionadas o no aprobadas comprometen el ambiente operativo y también constituyen un riesgo de seguridad, incluyendo el esparcimiento de virus o software malicioso tanto con o sin intención.

Los usuarios deben respetar las siguientes medidas preventivas de seguridad para proteger la información y las aplicaciones instaladas en el dispositivo:

- Los dispositivos no deben quedar a la vista en un vehículo desatendido, aunque sea por un período corto de tiempo.

- Los dispositivos no deben ser dejados en un vehículo durante toda la noche.
- Los dispositivos deben estar posicionados de manera que no queden visibles desde una ventana de la planta baja.
- Si en la pantalla de un dispositivo móvil se está mostrando información sensible en un lugar público se debe posicionar de tal manera que la información no pueda ser vista por otros.
- En situaciones vulnerables (aeropuertos, hoteles, centro de conferencias, etc.) el dispositivo no debe quedar desatendido bajo ninguna circunstancia.
- Los dispositivos deberán ser cargados como equipaje de mano cuando se viaja
- No se debe mover información desde un dispositivo a otro usando bluetooth.

  Solo está permitido copiar información sensible o confidencial al dispositivo móvil o de almacenamiento extraíble cuando sea requerida para trabajar en modo desconectado. En caso de realizarlo la información debe estar encriptada con los mecanismos que provea Sistemas.
- Para asegurar un almacenamiento adecuado, solo se debe almacenar los datos necesarios para propósitos laborales
- En lugares públicos no se debe de conectar a redes wifi abiertas. (Entiéndase por abiertas, son aquellas que no solicitan contraseña).

Responsabilidades

El responsable de autorizar el uso de dispositivos móviles de Cartolito a sus colaboradores, debe ser un superior de nivel gerencial.

Comité de seguridad de la información es responsable de:

- La identificación e inventario de los dispositivos móviles como propiedad de Cartolito en forma visible. Dicha identificación deberá ser resistente a su remoción.
- Establecer las condiciones de uso de los dispositivos móviles y comunicar las mismas a los responsables identificados en el inventario.
- Proveer el software necesario para realizar respaldos, sincronización de datos y de contactos, así como también el antivirus necesario para la protección de los dispositivos.
- Garantizar que las tecnologías, aplicaciones y medios de comunicación utilizados sean seguros y confiables.
- Asegurar que las aplicaciones para dispositivos móviles estén disponibles y optimizadas.
- Bloquear el acceso a correo externo sin una autorización previa.
- Determinar las medidas de seguridad mínimas que deben tener los equipos a adquirir.

La unidad que realice el proceso de adquisición y recepción dispositivos móviles de uso operativo específico deberá coordinar con el Comité de seguridad de la información

para inventariarlo. En caso de ser posible los equipos contarán con al menos las siguientes medidas de seguridad:

- Bloqueo de operación mediante contraseña.
- Encriptación de archivos con información confidencial o reservada.
- Antivirus habilitado y actualizado.

No es responsabilidad del Comité de seguridad de la información recuperar ningún tipo de información en caso de que el dispositivo se haya perdido, haya sido robado o dañado.

Es responsabilidad de los usuarios de dispositivos móviles de Cartolito:

- El cumplimiento de las condiciones de uso establecidas por el Comité de seguridad de la información en lo relativo al hardware y al software instalado, tanto cuando estos sean utilizados dentro como fuera de la Empresa.
- Llevar el dispositivo al departamento de sistemas cuando sea solicitado por Comité de seguridad de la información ya sea por razones de auditoría, administración o configuración.
- Tener el debido cuidado de la integridad física del dispositivo.
- Tomar las precauciones apropiadas para prevenir cualquier daño, pérdida o robo del dispositivo.
- En caso de pérdida, robo, el usuario deberá notificar inmediatamente a la Gerencia de Desarrollo de Proveedores, Compras y MP de la situación y realizar la denuncia correspondiente.
- Realizar los respaldos y verificar que el antivirus se encuentre activo y actualizado.
- Evitar el bloqueo de las limitaciones del fabricante y/o proveedor, o realizar cualquier otro método de cambio de las protecciones con las que se entregó el dispositivo.
- El cumplimiento de la Ley que prohíbe a los conductores de cualquier tipo o categoría de vehículos, cuando circulen, el uso de dispositivos de telefonía móvil o cualquier otro medio o sistema de comunicación, salvo cuando el desarrollo de la comunicación tenga lugar sin emplear cualquiera de las manos.

Historial de Cambios

Revisión	Fecha	Cambio	Elaboró (Puesto/ Firma)	Aprobó (Puesto/ Firma)
01	05/12/2021	Revisión del Documento	Jefe de SGC	Dirección General
01	05/12/2022	Revisión de documento	Jefe de SGC	Dirección General
01	19/12/2023	Revisión de documento	Jefe de SGC	Dirección General