Dada la naturaleza de la información que se maneja en la Zona Franca Internacional de Pereira S.A.S. Usuario Operador de Zonas Francas, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso; la pérdida o mal uso de esta información puede resultar en vulnerabilidad de la confidencialidad.

Es responsabilidad de todo usuario evitar la fuga de información que se encuentre almacenada en los equipos tecnológicos de la Zona Franca Internacional de Pereira S.A.S. Usuario Operador de Zonas Francas, según se establece en el acuerdo de confidencialidad, firmado por cada colaborador para tal fin. Los usuarios deberán utilizar los mecanismos corporativos para proteger la información que reside en los sistemas de información, dando uso a la infraestructura tecnológica de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas; de igual forma, deberán proteger la información reservada o confidencial que por necesidades corporativas deba ser almacenada o transmitida, ya sea dentro de la red interna de Zona Franca Internacional de Pereira S.A.S. Usuario Operador de Zonas Francas o hacia redes externas como Internet.

Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida. Gestión de Tecnología en Informática será responsable de aplicar un mecanismo automático para imponer esta práctica.

Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible, lo anterior incluye claves de acceso de aplicativos externos de manejo institucional, reiterando que las contraseñas son asignadas de manera particular y deben ser de uso personal e intransferible.

Los informes impresos que contienen información sensitiva, restringida o confidencial, deben ser retirados inmediatamente de las impresoras.

Los usuarios serán los responsables de almacenar semanalmente la información sensitiva y crítica que se encuentre en sus equipos de cómputo; para ello cuentan con una carpeta instalada en el escritorio de sus equipos, en la cual se debe guardar toda la información ligada a sus actividades, ya que lo almacenado en esta carpeta quedará guardado en un equipo ubicado en el cuarto de telecomunicaciones de la empresa, así mismo, se debe dejar constancia por escrito en el formato FO-TI-06 Back-Up. El Proceso de Gestión Tecnología e Informática será el encargado de verificar el cumplimiento de este numeral.

Semanalmente, el Proceso de Gestión Tecnología e Informática será el encargado de resguardar las copias de seguridad en la nube de todos los equipos de cómputo. La Gerencia y la Directora de Gestión Jurídica y Propiedad Horizontal deberán realizar la copia de seguridad en dos discos duros previamente asignados, y semanalmente el Proceso de Gestión Tecnología e Informática solicitará dichos discos para subir la información a la nube, estos dos cargos están exentos de dejar registro en el formato FO-TI-06 Back Up, debido a sus funciones.

Toda solicitud para utilizar un medio de almacenamiento de información compartido deberá ser aprobada por el Proceso de Gestión Tecnología e Informática y se deberá aplicar las políticas de seguridad.

En caso de contingencia, el único medio autorizado por la compañía para resguardar la información de los procesos son los discos duros USB que están a cargo del Proceso de Gestión Tecnología e Informática, por tal motivo está prohibido hacer copias de la información en discos, memorias, CD-DVD personales o ajenos a la compañía.

Cualquier actividad que requiera el uso de un medio de almacenamiento externo debe ser previamente consultada con el responsable del Proceso de Gestión Tecnología e Informática.

Periódicamente el Proceso de Gestión Tecnología e Informática realizará seguimiento al formato FO-TI-06 Back-Up, con el fin de llevar el control de cumplimiento y generar informes al Proceso de Gestión Administrativa, los cuales se realizarán y serán enviados cuando sean solicitados para fines pertinentes.

Los dispositivos móviles que tengan sincronizado el correo corporativo de los directores y coordinadores deberán contar con un antivirus instalado y licenciado, no importa si el dispositivo es de la empresa o persona, esto con el fin de proteger la información que reposa en ellos.

|  |  |  |
| --- | --- | --- |
| **ELABORADO POR:** | **REVISADO POR:** | **APROBADO POR:** |
| Nombre: Dubian Sánchez | Nombre: Yuly Viviana Ríos | Nombre: Orlando Ossa |
| Fecha: 19 de Octubre de 2020 | Fecha: 19 de Octubre de 2020 | Fecha: 19 de Octubre de 2020 |
| Firma: | Firma: | Firma: |