POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

En **PRO-SER COLOMBIA S.A.S.** se establece la Política de Tratamiento de Datos Personales y controles requeridos con el fin de garantizar su recolección, almacenaje, uso y circulación de la información a sus titulares.

En la prestación de nuestros servicios de transporte terrestre de mercancías peligrosas, recolectamos información como:

1. Razón Social
2. Nombres y Apellidos
3. Contactos
4. Identificación Tributaria y Fiscal NIT -RUT
5. Información bancaria para transferencias y referencias
6. Dirección, Correo Electrónico, Teléfono Fijo, Celular y/o Fax

Recolectada por medio físico y/o electrónico en la ejecución de la gestión comercial con los clientes, proveedores o en nuestros procesos de selección y contratación de personal, dicha información será almacenada de manera electrónica y física cumpliendo nuestras tablas de retención documental, la cual estará administrada bajo el procedimiento de información documentada de nuestro sistema integrado de gestión, cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la misma.

La información será tratada conforme a lo indicado en la normatividad vigente y administrada por los trabajadores que estén autorizados para acceder a esta, empleándola exclusivamente en las actividades propias de nuestro objeto social. Solo se divulgará a terceros cuando exista obligación legal u orden de la autoridad de proporcionar información clasificada con destino a autoridades administrativas, judiciales, fiscales y regulatorias.

La administración de los datos se desarrollará mediante los principios de:

1. Veracidad y calidad de los registros
2. Finalidad
3. Acceso y circulación restringida
4. Temporalidad de la información
5. Interpretación integral de derechos constitucionales
6. Seguridad
7. Confidencialidad

Los titulares tendrán a su disposición los siguientes medios de comunicación:

1. Email: info@pro-ser.co
2. Teléfono: 601 200 3088
3. Celular: 313 880 6597
4. Escrito: Calle 5 No 71ª – 28 Nueva Marsella

Los titulares tendrán derecho a:

1. Conocer, actualizar y rectificar la información
2. Aprobar la autorización
3. Solicitar información sobre el uso de la misma
4. Revocar la autorización y solicitar supresión

5. Presentar una petición, queja o reclamo

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

En **PRO-SER COLOMBIA S.A.S.** se ha establecido las siguientes directrices como Políticas para mitigar los riesgos que se ve expuesto la información de la empresa y de la gestión de nuestras actividades:

Contraseñas

- Todo computador estará protegido con contraseña individual para cada usuario que lo utilice. La contraseña del usuario administrador, será de conocimiento de la Gerencia Administrativa y Financiera.
- Las contraseñas de acceso a los sistemas de información deberán ser cambiadas al momento del primer ingreso. El área de Administrativa y Financiera solicitará el cambio obligatorio.
- La contraseña es personal e intransferible. Está prohibido compartir contraseñas con otros usuarios del sistema.
- Está prohibido acceder a recursos de red a los cuales no tiene autorización.
- En el momento que se ausente el usuario del computador debe bloquear el sistema mientras no se encuentre en el computador para evitar que alguien lo utilice.
- Los requisitos de la contraseña son: mínimo 8 caracteres, alfanuméricos, debe tener mínimo una letra en mayúscula y un carácter especial.
- La contraseña no puede contener el nombre del usuario y no puede ser igual a las ultimas 3 usadas.

Uso de Correo Electrónico

- Las cuentas de correo electrónico suministradas por la empresa son personales e intransferibles.
- No se permite utilizar la cuenta de otro, para enviar mensajes, esto se llama suplantación y está totalmente prohibido.
- La cuenta de correo electrónica empresarial solo es para el uso estrictamente laboral y para gestión de temas relacionados con el negocio, está prohibido el uso del correo para temas personales.
- Está totalmente prohibido enviar o recibir correo electrónico desde la cuenta empresarial a la(s) cuenta(s) privada(s) o personal(s) del trabajador.
- Es necesario que todos los mails enviados desde los correos empresariales tengan la información obligatoria del remitente, la cual está manifestada en su plantilla de firma, que es establecida por la empresa.
- El envío masivo de correo electrónico está limitado, solo las cuentas generales deben ser usadas para tal fin con el objetivo de un comunicado general a clientes.
- Se prohíbe el uso del mail para hacer envíos masivos de publicidad haciendo Spam, email no deseado desde las cuentas empresariales.
- Se prohíbe el uso del correo para la exhibición, la transferencia directa o la comunicación deliberada por el email del contenido ilícito, racista, sexista, de violencia-glorificación, pornográfico u ofensivo.

¨La impresión de este documento no garantiza que corresponda a la última versión, por lo cual no es una copia controlada¨

- Los usuarios son responsables de la apertura de correos de remitentes desconocidos o anónimos con un tema no específico, se debe verificar la autenticidad de estos antes de abrirlos de lo contrario se deben suprimir inmediatamente.
- Se prohíbe el envío de información ajena al objeto social de la empresa y/o personal del usuario hacia cuentas personales del usuario o cuentas de la misma empresa u otros terceros ajenos a la empresa. Asimismo, se prohíbe suministrar la cuenta de email de la empresa para recibir información personal.
- Para los usuarios el único sistema permitido para el uso de correo empresarial es el Outlook.
- El usuario es responsable del manejo y archivo de sus mensajes de correo electrónico, la eliminación o autoarchivado de los mismos para liberar espacio de las bandejas principales de entrada y salida.
- Se debe informar de cualquier evento sospechoso o email de estafa o (Spam) que se reciba para realizar procesos de verificación de intensidad y bloqueo de dominios o remitentes de ser necesario.

Uso y Restricciones del Internet

- Toda navegación en Internet tiene su respectivo registro de visita y será auditable por la empresa con su correspondiente informe al Gerente General.
- El uso del Internet es únicamente para las labores que se desempeñan en la empresa.
- La participación en juegos en línea, chat, redes sociales, streaming, uso de plataformas de compartir archivos, la participación en el comercio en línea y el acceso a los Web sites o a las herramientas que apoyan delito informático, están restringidas y no se permite su utilización.
- Se prohíbe la descarga de programas o software desde internet, de requerirse un programa en particular se debe solicitar la aprobación del Gerente General y estas serán analizadas por el área de sistema para determinar la seguridad y licenciamiento requerido.
- Se restringe el uso de navegadores de internet personalizados y no autorizados e instalados por el área de sistema de la empresa.
- Está prohibido el uso del Internet para ingresar a páginas de contenidos para adultos, políticos u otros no relacionados con el trabajo.
-
- El uso de los registros de navegación, está disposición es para búsquedas de actividades en contra de las políticas y procedimientos de auditoría.
- La conexión a la red wifi de la red local de la empresa y de las conexiones de los clientes, tiene las mismas restricciones de uso y solo podrán ser configuradas en equipos de la empresa, se prohíbe la conexión de dispositivos móviles, la conexión a la red wifi de la empresa solo la podrá realizar el gerente general, quien custodiará la contraseña de acceso.
- Para los usuarios invitados de la empresa (Clientes / Proveedores) Se tiene a disposición una red que será asignada por la Gerencia Administrativa y Financiera.

Mantenimiento de Equipos

- El mantenimiento exterior de los equipos está a cargo del trabajador, el cual debe garantizar la limpieza constante de los equipos, realizada con un trapito.
- El trabajador deberá informar de manera oportuna a la Gerencia Administrativa y Financiera la necesidad de mantenimiento del equipo, mediante correo electrónico para su coordinación.

- El área de sistemas es el único autorizado para la revisión de HARDWARE, SOFTWARE y realización de mantenimientos preventivos o correctivos de los equipos de cómputo.

Copia de Seguridad de la Información

- El trabajador debe guardar la información de su gestión en las carpetas de los clientes asignados que se encuentran en el software del DROPBOX, no deberá dejar información en las carpetas del equipo de cómputo.
- El trabajador es el responsable de compartir su información con otros trabajadore mediante las herramientas brindadas por la empresa (Correo electrónico y Dropbox.
- Se realizará copia de seguridad a la información del Dropbox por parte del área de sistemas y Gerencia General.
- El área de Sistemas y Gerencia realizará copias a los servidores virtuales que se tienen configurados y son los responsables de la custodia de esta información.

Administración de Información

- El trabajador debe mantener el escritorio de la oficina limpio y organizado, sin documentación visibles en el puesto de trabajo.
- Documentación sensible de la empresa debe estar bajo llave en custodia del trabajador responsable, claves no deben encontrarse a la vista, documentos con información sensible y que ya no se requieran deben ser destruidos.
- No está permitido el traer o llevar información en sistemas de almacenamiento tales como USB /CDS, DVD´s, discos extraíbles, entre otros; dentro de nuestra red sin previa autorización de la Gerencia General.
- Está prohibido el tener documentos de carácter personal y de dudosa procedencia almacenados en sus equipos.
- No está permitido el uso de scanner, fotocopiadoras, faxes, entre otros; para temas no relacionados con sus labores o la empresa.
- Está prohibido la conexión a la red de la Empresa de dispositivos personales o ajenos a la Empresa por parte de los trabajadores.
- Solo está autorizado la conexión a la red de invitados para personal externo de la empresa realizando labores para la misma y en horarios de oficina.
- El trabajador debe dejar apagado y desconectado el equipo al finalizar la jornada laboral.

Uso de dispositivos tecnológicos

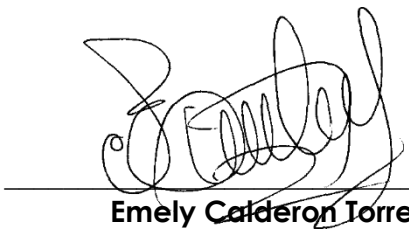
- Solo está autorizada la configuración de los correos electrónicos en los dispositivos móviles empresariales acorde al cargo a desempeñar.
- Los teléfonos móviles empresariales son de uso exclusivo para temas laborales.
- El trabajador se hará responsable de daños en los equipos de cómputo ocasionados por manipulación de bebidas y alimentos.
- El trabajador deberá velar por el buen estado y buen funcionamiento de los equipos entregados para el buen desempeño de sus funciones.

Los trabajadores que no acaten lo dispuesto en el presente manual de políticas, podrán ser sujetos a procesos disciplinarios y de sanciones según lo establecido en el Reglamento Interno

¨La impresión de este documento no garantiza que corresponda a la última versión, por lo cual no es una copia controlada¨

de Trabajo de la empresa y la metodología implementada en el procedimiento ddisciplinarios. En el caso de infracción a los controles en el presente manual por parte de los asociados de negocio, se iniciará la debida diligencia acorde a los establecido en los contratos suscritos entre la empresa y su Cliente, Proveedor o Contratista.

El presente documento se firma a los veintiocho (28) días del mes de mayo de 2023.



Emely Calderon Torres
Gerente