POLÍTICA DE USO Y MANEJO DE INFORMACIÓN CONFIDENCIAL

PROPÓSITO

El propósito de esta política es definir los estándares para salvaguardar la información contra uso no autorizado, divulgación o revelación, modificación, daño o pérdida en ALIMENTOS CAROLINA LTDA.

ALCANCE

Esta política aplica a todo el personal incluyendo pero no limitado a empleados, contratistas, consultores, personal temporero y otro personal.

DEFICIONES

Información sensitiva – Esta información debe estar disponible a los empleados de la Compañía, pero no disponible a terceros
Información restringida – Acceso a esta información debe estar limitada a una audiencia restringida, determinada por la Administración.
Información confidencial – Esta información debe estar solamente disponible a personas designadas.

POLÍTICA

Dado a la naturaleza de la información que se maneja en ALIMENTOS CAROLINA LTDA, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso, junto con la información personal de los trabajadores que se almacena en sus carpetas individuales. Pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como filtración de datos claves del negocio y acceso a información de nuestros colaboradores.

ASPECTOS GENERALES

Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensitiva, restringida o confidencial debe ser ubicada en áreas protegidas. Estos medios de almacenamiento de información nunca deben ser ubicados en un lugar donde visitantes pueda tener acceso a ellos.

- Los medios de almacenamiento de información que contienen información sensitiva, restringida o confidencial debe ser guardada en un área segura a final de cada día laborable.
- Las computadoras portátiles (“laptops”) y otros dispositivos portátiles (tales como memoria USB / pendrive, etc.) que contiene información de la Compañía, deben estar siempre protegidos con claves de acceso que impidan la entrada libre de cualquiera a su información. Si el equipo no está siendo utilizado o no está en la posesión directa del usuario asignado, debe estar asegurada físicamente.
- Toda información de respaldo de datos (“backup”) enviado o almacenado en medios de datos debe ser protegido y debe ser manejado según los procedimientos aplicable de librerías de medios políticas y seguridad vigentes en la institución. Los datos sensibles actualmente se manejan en servidores de datos

fuera de las instalaciones con procesos de respaldo que aseguran la integridad y seguridad permanente de la información.
- Las infracciones de esta política pueden tener como resultado acciones disciplinarias conforme a políticas y procedimientos disciplinarios vigentes en la institución.

PRÁCTICAS EN LAS ÁREAS DE OFICINAS

- Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida.
- Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensitiva, restringida o confidencial debe ser retirada del escritorio y asegurada en archivos de gaveta al final de la jornada de trabajo.
- Cada usuario es responsable de asegurar todo documento y medio electrónico de almacenamiento que contenga información sensitiva o confidencial que esta esté ubicada en gavetas o archivos con llave.
- Las contraseñas no pueden ser dejadas en notas en el escritorio ni en una ubicación accesible.
- Los informes impresos que contienen información sensitiva, restringida o confidencial deben ser retirados inmediatamente de las impresoras.
- Al momento de desechar, los documentos sensitivos o confidenciales deben ser destruidos previamente.
- Controles de acceso y monitoreo deben ser aplicados en áreas de oficina e instalaciones de almacenaje donde resida información restringida o confidencial.
- Las impresoras y los equipos para facsímil (“Fax”) deben ser localizados en áreas donde el público no pueda ver información sensitiva, restringida o confidencial.

PROCESO DE NOTIFICACIÓN

- En eventos los cuales información sensitiva, restringida o confidencial es extraviada o es divulgada a entidades no autorizadas o si este acontecimiento incluye pérdida de cualquier equipo, medio electrónico de almacenamiento o componente tecnológico, se debe notificar inmediatamente a la Administración.

MEDIDAS DISCIPLINARIAS

- Las sanciones aplicables al personal, de acuerdo a la ocurrencia o severidad de la violación o infracción a esta política se regirá por lo establecido en el reglamento interno de la empresa.

- La Compañía se reserva la facultad de aplicar la sanción más severa, en este caso el despido, en aquella ocasión en que la gravedad o seriedad de la infracción no amerite permitir que se repita en una futura ocasión.

VIGENCIA

Esta Política deja sin efecto cualquier circular, carta o política anteriormente emitido sobre los aspectos aquí cubiertos. La Gerencia General puede enmendar esta política en cualquier momento.

La Administración, mediante la implantación de esta política, debe asegurar que la debida diligencia sea ejercitada por todos los individuos involucrados en la operación de los sistemas de información presentes en la Compañía.