POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Para DIETRANS CARGO SAS, la información y en especial la definida como de tipo personal es considerada como uno de los principales activos, la cual es necesaria para la ejecución de sus actividades del día a día y como agente primordial para la toma de decisiones en pro del crecimiento de la organización.

De acuerdo a sus necesidades DIETRANS CARGO SAS ha implementado un modelo de gestión de la seguridad de la información el cual busca mitigar los diferentes riesgos a los cuales se ve expuesta la información para así reducir los costos que se puedan generar en el momento en que un riesgo se materialice; de igual manera este modelo busca generar dentro de la organización una cultura de seguridad que irá creciendo paulatinamente a medida que el modelo definido adquiera la madurez necesaria dentro de la organización.

Dado el esfuerzo y recursos que puede demandar un sistema de gestión de seguridad de la información SGSI, DIETRANS CARGO SAS ha adoptado una serie de directrices que permitirán ir avanzando en la cultura organizacional de seguridad de la información hasta alcanzar el nivel de madurez adecuado; por lo anterior esta política y sus directrices serán revisadas periódicamente y la implementación será gradual y progresiva, así como será sometida a revisión una vez al año teniendo en cuenta adicionalmente los cambios orgánicos y estratégicos que pueda tener la organización durante el tiempo, con el fin de siempre permanecer alineados con los objetivos de la misma.

DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

DIETRANS CARGO SAS ha definido tres grandes ejes sobre los cuales están definidas las directrices de seguridad de la información y estos son INFORMACIÓN, RECURSO HUMANO y RECURSO TECNOLÓGICO, de donde, el incumplimiento de la presente política de seguridad de la información, tendrá como resultado la aplicación de sanciones conforme a lo establecido al reglamento interno de la organización.

EJE DE INFORMACIÓN

La información y los activos de información son considerados como recurso principal y de alto impacto para la toma de decisiones, por tal motivo deberán estar protegidos y resguardados de acuerdo a las directrices y posibilidades definidas dentro de la organización.

La información y en especial la de tipo personal es clasificada de acuerdo a los criterios que la organización ha adaptado y en caso particular teniendo en cuenta las consideraciones dadas por la ley de protección de datos 1581 de 2012 y demás documentos que de esta han sido generados por el estado y tengan relación con la clasificación de la información.

Información que se encuentra en medio físico o que se encuentre en cualquier tipo de almacenamiento externo (CD, Memorias portátiles, Discos duros, etc.) mientras no se encuentre en uso deberá estar almacenada en un lugar bajo llave y con acceso restringido solamente al personal quien pueda tener permiso a uso de la información que allí reside.

EJE DE RECURSO HUMANO

Todos los funcionarios y/o colaboradores tanto directos como indirectos que tiene la organización son responsables de proteger la información a la cual acceden, procesen y almacenen para así evitar la pérdida, alteración, destrucción o uso indebido.

Cada funcionario directo o indirecto solo podrá acceder a la información que sea necesaria para cumplir las funciones para las cuales ha sido contratado o tiene alguna relación con la organización.

Todo funcionario directo o indirecto tiene la obligación de advertir cualquier situación que afecte o pueda llegar a afectar la seguridad de la información o algún activo de información.

EJE RECURSO TECNOLÓGICO

El uso de equipos de escritorio, equipos portátiles o cualquier dispositivo que cumpla las funciones de herramienta de trabajo, será de uso exclusivo para las actividades y funciones del colaborador y/o funcionario, dentro de la organización.

El respaldo de la información que se encuentra dentro de los equipos de escritorio, equipos portátiles, servidores de archivos, se llevará acabo de acuerdo a lo establecido por la organización, teniendo en cuenta de manera adicional que las pruebas de recuperación de la información se hacen de manera periódica, dejando así evidencia del respaldo y recuperación de la misma.

El uso de contraseñas para acceder a los sistemas de información, recursos tecnológicos o cuando aplique tendrá como mínimo las siguientes características de seguridad:

Característica	Valor
Longitud mínima de la contraseña	8 caracteres
Longitud máxima de la contraseña	20 caracteres
Dígitos requeridos	Si
Caracteres requeridos	Si
Uso de mayúsculas	Si

Uso de minúsculas	Si
Caducidad	30 días
El Nombre de usuario no podrá ser usado como contraseña	Verdadero
Histórico de contraseñas	5 claves

El uso del correo electrónico se realizará a través de las direcciones de las cuentas oficiales de la organización, de igual manera el reenvió de mensajes a direcciones externas de la organización debe estar restringido salvo previa autorización de quien origina el mensaje, o en su defecto cuando el carácter (tipo) de la información indica que esta es pública.

El uso del Internet dentro de las instalaciones de la organización es de carácter laboral y no se podrá hacer navegaciones a sitios restringidos por la organización así como sitios que afecten la productividad de los funcionarios y/o colaboradores.

La descarga, instalación de software está restringida para los funcionarios y solo se podrá hacer por el área o departamento de Tecnología de la información o quien a su vez cumpla el rol para tal fin.

El uso de herramientas de cifrado para almacenamiento, transferencia y uso será tenido en cuenta de acuerdo a la criticidad de la información con la cual se está trabajando y para esto se dejará constancia en el momento en que se deba usar dichas herramientas.