Políticas Corporativas

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A Todos los Empleados

Todos los empleados tienen el deber de proteger la información de FENOCO. Por consiguiente, mediante la presente política se establecen las directrices que se deben seguir para garantizar la seguridad de la información de la Compañía dentro y fuera de ella.

Como miembro del equipo de FENOCO, solicito la participación de todos en la protección de nuestra información acatando las políticas de seguridad de la información, estándares y procedimientos presentados en este documento, e informando sobre cualquier conducta que no cumpla con nuestra política.

PRINCIPIOS

Los principios corporativos que enmarca esta política son los siguientes:

Respeto
Operaciones realizadas bajo el más estricto cumplimiento de las normas y procedimientos en un ambiente de cordialidad y solidaridad con nuestros grupos de interés, medio ambiente.

Integridad
Responsabilidad por resultados, actuando con coherencia y honestidad en busca de la excelencia.

Seguridad
Fortalecimiento de los análisis oportunos de riesgos, generando una cultura del autocuidado y aseguramiento nuestra operación y del bienestar de nuestra gente y comunidades.

Sentido de Pertenencia
Caracterizados por nuestro compromiso, diligencia y oportunidad en la toma de decisiones y el cumplimiento de objetivos.

1. OBJETIVO

El objetivo de esta política es establecer los lineamientos y directrices sobre la gestión de la seguridad de la información, dirigidos a mitigar los riesgos relacionados con el tratamiento de todos los documentos digitales de la compañía.

2. ALCANCE

Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por toda persona con acceso a los activos de información de FENOCO, para conseguir un adecuado nivel de protección de seguridad y protección de la calidad de la información de FENOCO.

3. CONTENIDO DE LA POLÍTICA

3.1. Declaración de la Misión de Seguridad de la Información.

"La protección de la información de FENOCO y de los activos que constituyen los sistemas de Información, de fallas que afecten su disponibilidad, confiabilidad, confidencialidad e integridad."

3.2. Funciones y responsabilidades

Toda persona con acceso a los activos de información de FENOCO (empleados, contratistas, asesores, proveedores, socios comerciales, o Contratistas de empleados temporales de FENOCO) es responsable por el manejo seguro y protección de los activos de la información de la compañía.

3.3. Principios de la política

3.3.1. Comunicación Oportuna y Exacta

Las violaciones, problemas, vulnerabilidades observadas o sospechadas, incidentes o amenazas contra la seguridad de la información, deberán ser reportados a través de los canales establecidos por la compañía en el Programa de Atención de Inquietudes para la recepción de estos reportes.

•Enviando un correo electrónico: denuncias@lineaetica-fenoco.com.

•Ingresando a la página web: www.fenoco.com.co en el enlace Programa de Atención de Inquietudes.

•Llamando a la Línea ética de Ferrocarriles del Norte de Colombia SA FENOCO: 01 800 951 0675.

• Presentando quejas, reclamos, solicitudes, denuncias y/o violaciones verbales o escritas a través del programa de atención de inquietudes.

3.3.2. Cumplimiento y conformidad

Toda persona (empleados, contratistas, asesores, proveedores, socios comerciales, o empleados temporales) con acceso a los activos e información de FENOCO de forma temporal o permanente, son responsables de

cumplir la política de seguridad de la información.

Toda persona que intente y/o vulnere los controles y mecanismos de seguridad de los sistemas o redes estarían sujetos a acciones disciplinarias de acuerdo a lo establecido en el Reglamento Interno del Trabajo y/o Código de Conducta de la compañía.

3.4. Código de Prácticas de Seguridad de la Información.

3.4.1. Políticas sobre el uso de computadoras

Los sistemas de comunicación de FENOCO, incluyendo el Internet, mensajería corporativa, y sistemas de computación, son propiedad de la Compañía y deben ser usados para fines de la misma.

3.4.2. Uso personal de Internet y Mensajería Corporativa

FENOCO reconoce que los empleados puedan utilizar los sistemas de cómputo ocasionalmente o necesitar el uso de Internet o correo electrónico para fines personales. Estas comunicaciones serán consideradas como privadas siempre y cuando el usuario las archive o catalogue como personales.

3.4.3. Actividades Prohibidas

Los recursos de FENOCO no pueden ser usados para ninguna de las siguientes actividades:

- Recibir, ver, compartir, o distribuir materiales que pudieran ser considerados ofensivos o que estuvieren prohibidos bajo la ley colombiana y las políticas de la Compañía.
- Para anuncios comerciales o personales.
- Para solicitar ventas o promover negocios externos.
- Presión política o publicidad de actividades políticas.

- Cualquier fin comercial aparte del objeto misional de FENOCO.

- Distribuir o compartir información confidencial o sensible de la compañía por medio de aplicativos de mensajería instantánea, aplicativos libres o herramientas no corporativos (Skype, Whatsapp, line, messenger, entre otros).

- Está totalmente prohibido que los empleados de FENOCO utilicen las instalaciones de la compañía y el corredor férreo para digitalizar, capturar, distribuir, compartir y/o subir fotografías, videos de accidentes, incidentes o cualquier medio digital de eventos de índole personal o corporativos que contengan información confidencial o sensible que afecte e involucre negativamente la marca, imagen u operación de FENOCO, en cualquiera de las redes sociales tales como Facebook, Instagram, Whatsapp, Messenger, o cualquier medio de esta índole o sistema similar.

Los usuarios de las redes de FENOCO tienen prohibido el uso de herramientas de prueba de seguridad, analizadores de paquete de la red, “Sniffers”, o herramientas y/o tecnologías similares. La autorización de estas herramientas solo están permitidas para La Dirección de Tecnología de la Información en los caso que se requiera para

diagnósticos de fallas y problemas que se presenten en la red, los cuales deben dejar documentado.

3.4.4. Política de Renuncia a Privacidad

Los usuarios de FENOCO renuncian a todos sus derechos de privacidad con relación a cualquier elemento o información corporativa que creen, almacenen, envíen, o reciba en las computadoras de FENOCO o por medio de las infraestructuras de Internet de FENOCO.

La información catalogada y/o archivada como personal por los usuarios se considerará como información privada y confidencial de los usuarios.

FENOCO se reserva el derecho de supervisar que los sistemas de computación y red sean utilizados dando cumplimiento con el Código de Conducta y las políticas de FENOCO, lo cual es aceptado expresamente por los empleados al firmar el consentimiento expreso del derecho de Fenoco a verificar el cumplimiento de las mismas.

FENOCO podrá supervisar el uso adecuado de los recursos de IT, incluido en esto el correo electrónico, el uso de internet, el almacenamiento de archivos y el acceso a computadoras, de acuerdo al proceso previamente avalo por el Comité de Prácticas Corporativas quien garantizará la no violación de las garantías y principios mínimos laborales y constitucionales del trabajador.

Esta supervisión permitirá a Fenoco registrar cualquier uso indebido de los sistemas, así como la creación, procesamiento y almacenamiento de información contraria a las políticas de Fenoco, o que bien infrinjan las normas y leyes.

3.4.5. Computadoras Portátiles

3.4.5.1. Seguridad Física de las Computadoras Portátiles

Las computadoras portátiles deben ser guardadas (mantenidas) físicamente seguras.

Los usuarios a quienes se asigna una computadora portátil deben asumir todas las responsabilidades de seguridad de la computadora portátil y de la información, programas y datos almacenados en la misma. Adicionalmente, deben realizar a la mayor brevedad posible la respectiva denuncia de la perdida a las entidades estatales correspondientes.

3.4.5.2. Respaldo de las computadoras Portátiles

Es responsabilidad de la Dirección de IT que todos los datos almacenados en las computadoras portátiles deberán ser respaldados como mínimo quincenalmente en un servidor centralizado o medio removible (Unidad Usb, Discos Externos, etc).

La información que será respaldada es la que se encuentre en las unidades de almacenamiento indicadas por la Dirección de IT a los usuarios.

La Dirección de IT es responsable de la seguridad de todos los medios removibles donde realice sus backup (Unidad Usb, Discos Externos, etc).

3.5. Acceso Lógico

3.5.1. Acceso a Información

Los usuarios deben contar con la aprobación de su superior Inmediato para accesar a los sistemas de información o las aplicaciones. El

acceso a la información debe ser otorgado al individuo con fundamento en las responsabilidades del cargo del usuario.

3.5.1.1. Protección de las Contraseñas

- Las contraseñas son consideradas como personales e intransferibles y deberán estar bien protegidas por cada usuario.
- Las contraseñas no deben ser escritas y dejadas en un lugar donde personas no autorizadas las pudieran acceder.
- Las contraseñas no deben ser enviadas por correo electrónico, excepto en mensajes correctamente codificados.
- La vulnerabilidad de las contraseñas será responsabilidad del propietario de la misma; sino cumple lo descrito en los puntos anteriores.

3.5.2. Política de Escritorio Limpio

Documentos confidenciales, o medios removibles que contengan información confidencial no deben dejarse donde alguien pudiera recogerlos con facilidad, tal como la copiadora, impresora, máquina fax, o una oficina o espacio de trabajo inseguro.

3.6. Prevención de Virus

3.6.1. Software Anti-Virus

La Dirección de Tecnología será responsable de instalar y activar software anti-virus en cada computadora de escritorio, portátil, y servidor de la compañía.

Cada disco, unidad usb u otro medio para transferir datos a una computadora deberá ser examinado por un software antivirus antes de hacer uso de la información contenida en el mismo.

3.6.2. Correo Electrónico

Los archivos adjuntos a e-mails entrantes deben ser examinados para detectar virus en las computadoras, si se detecta alguna anomalía deberá notificarlo a la mayor brevedad a la Dirección de IT.

Los usuarios no deben distribuir a través del sistema de mensajería de la compañía, correos en cadena con información contraria a las políticas de FENOCO o que infrinjan las normas y leyes.

3.7. Políticas de Derecho de Autor

3.7.1. Registro de Software

FENOCO tiene como política el uso de Software licenciado. Por lo tanto los equipos se encuentran restringidos para la instalación de software ilegal (No registrado). Los usuarios que intenten o vulneren estos controles e instalen software ilegal serán responsables de sanciones penales y estarían sujetos a acciones disciplinarias de acuerdo a lo establecido en el Reglamento Interno del Trabajo y/o Código de Conducta de la compañía.

3.7.2. Programas Compartidos “Shareware” y programas Libres de Derechos “Freeware”

Se prohíbe instalar software shareware o freeware en los equipos de cómputo de FENOCO.

3.8. Políticas de Conexión a Internet

3.8.1. Acceso a Internet

La Dirección de Tecnología debe garantizar que los accesos a Internet dentro de la infraestructura de FENOCO deben realizarse por medio de un equipo de seguridad (Firewall).

3.8.2. Navegación en Internet

Se prohíbe a los usuarios la descarga programas de freeware y shareware.

3.8.3. Sitios de Internet Inapropiado

Acceso a sitios inapropiados haciendo uso de equipos e infraestructura tecnológica de FENOCO está prohibido. Ejemplos de sitios de este tipo podrían incluir, aunque no se limitan a:

- Sitios sexualmente explícitos.
- Sitios para *hackers.*
- Sitios relacionados con Warez (*software ilegal* o herramientas para *hackers*).
- Sitios que pudieran entrar en conflicto con las políticas y / o intereses comerciales de FENOCO.

3.8.4. Actividades Prohibidas en Internet

- Los servicios de re-anuncio publicitario (re-mailer)
- Los usuarios no deberán usar el Internet para juegos.
- Los usuarios no deberán usar su acceso a Internet para enviar o retirar materiales pornográficos, archivos de texto inapropiados, o archivos que pongan en peligro la integridad de la red.

3.8.5. Conexiones Remotas

Todos acceso remoto o externo hacia las redes e infraestructura de FENOCO debe hacerse usando conexiones con clientes VPN a través del Firewall; cada usuario que utilice o haga uso de este tipo de conexión debe disponer de un usuario y contraseña personal e intransferible y deberán ser adecuadamente custodiadas por cada usuario.

4. GLOSARIO

- Vulnerabilidad: Son puntos débiles que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo.
- Sniffers: Programa informático que registra la información que envían los periféricos.
- Anti-virus: Programa informático que tiene el propósito de detectar y eliminar virus de los sistemas de cómputo.
- Shareware: Modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo de uso o en algunas de las formas de uso o con restricciones en las capacidades finales
- Freeware: Tipo de software que se distribuye sin costo, disponible para su uso.

- Firewall: Programa informático, hardware o combinación de ambas que controla el acceso de una computadora a la red y elementos de la red a la computadora, por motivos de seguridad.
- Hackers: Persona que descubre las debilidades de un computador, sistema o de una red informática.

5. VIGENCIA

La presente política entra en vigencia a partir del día 23 del mes de Enero de 2018 y deroga todas las disposiciones anteriores y estará vigente hasta que una nueva política modifique o derogue la presente.

ANDRES SOTO VELASCO
PRESIDENTE