Política Corporativa

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

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.

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.

1. CONTENIDO DE LA POLÍTICA

1.1. Declaración de la Misión de Seguridad de la Información.

"La protección de la información de FEN0CO y de los activos que constituyen los sistemas de Información, de fallas que afecten su disponibilidad, confiabilidad, confidencialidad e integridad."

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 dela información de compañía.

1.2. Principios de la Política

1.2.1. Comunicación Oportuna y Exacta

Las violaciones, problemas, vulnerabilidades observadas o sospechadas, incidentes amenazas contra la seguridad de la información de la empresa, 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:

Las violaciones, problemas, vulnerabilidades observadas o sospechadas, incidentes amenazas contra la seguridad de la información de la empresa, 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 página web: www.fenoco.com.co en el enlace Programa de Atención de Inquietudes, donde se encuentran las instrucciones para realizar un reporte.
- Llamando a la Línea ética de Ferrocarriles del Norte de Colombia SA FENOCO: 01 800 9510675.

1.2.2. 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 /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. Igualmente, y en el evento en que resulte procedente, serán sujetos de las acciones legales pertinentes de conformidad Con nuestro ordenamiento jurídico.

2. CODIGO DE PRACTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1. Políticas sobre el Uso de computadoras servicios de Tecnología.

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

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

2.2. Seguridad Física de las Computadoras Portátiles.

Las computadoras portátiles deben ser guardadas (mantenidas) físicamente en lugares seguros. Los usuarios a quienes se asigna una computadora portátil deben asumir todas las responsabilidades de seguridad de ésta y de la información, programas y datos almacenados en la misma. Adicionalmente, en el evento de pérdida, hurto, o cualquier situación que afecte la seguridad de la información o del dispositivo; el responsable debe realizar a la mayor brevedad posible la respectiva denuncia de la perdida ante las entidades estatales correspondientes.

2.3. Respaldo de la Información

La información que se genere en los equipos de cómputo de la compañía quedará

almacenada en los servidores virtuales contratados con sus respectivos backups.

La Dirección de tecnología debe validar periódicamente el cumplimiento de las políticas de seguridad y respaldo de los proveedores de servicios en nube contratados por la Compañía.

La Dirección de IT es responsable de la seguridad de todos los medios removibles donde realice su backup (Unidad USB, Discos Externos, etc.), en los casos excepcionales que aplique.

2.4. 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 que estuvieren prohibidos bajo la ley colombiana y las políticas de Compañía.
- Para solicitar ventas promover negocios externos, o para rifas.
- Presión política publicidad de actividades políticas.
- Cualquier fin comercial aparte del objeto misional de FENOCO.
- Distribuir compartir información confidencial o sensible de la compañía por medio de aplicativos de mensajería instantánea, aplicativos libres herramientas no corporativas (WhatsApp, Messenger, hangouts, 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 accidentes, de incidentes o cualquier medio digital de eventos de índole personal corporativos que contengan información confidencial o sensible que afecte e involucre negativamente la marca, imagen u operación de FENOCO,O para afectar en la intimidad de terceros, 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 casos que se requiera para diagnósticos de fallas y problemas que se puedan presentar en la red, en todo caso debe quedar documentado.

2.5. Uso adecuado de herramientas tecnológicas

Todos los archivos, planos y demás documentos que creen y desarrollen los trabajadores en el ejercicio de sus funciones o con el uso de los dispositivos tecnológicos suministrados por la compañía, son de propiedad exclusiva de la compañía. En consecuencia, los trabajadores en vigencia del Contrato laboral o con posterioridad no podrán alegar propiedad o cualquier otro tipo derecho sobre los mencionados documentos dispositivos.

La información catalogada y/o archivada como personal por los usuarios en los dispositivos suministrados por la compañía se considerará como información privada y confidencial de los usuarios. En consecuencia de ello la compañía no será responsable por el uso inadecuado, fraudulento o ilegal de la información que allí se almacene.

En el evento que la compañía advierta el uso irregular de dichos elementos, adelantará las investigaciones y procesos disciplinarios a los que haya lugar.

FENOC0 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 sus recursos de IT, incluido en esto el correo electrónico, uso de internet, el almacenamiento de archivos y el acceso a computadoras demás dispositivos proporcionados para ejecutar las actividades enmarcadas en los contratos laborales con los colaboradores, de acuerdo al proceso previamente avalado 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 almacenamiento de información contraria a las políticas de Fenoco, o que bien infrinjan las normas y leyes.

2.5.1. Correo Electrónico

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.

El Usuario debe garantizar que el correo o herramienta tecnológica sea utilizado de manera adecuada y racional para las funciones propias de su cargo, respetando los principios de confidencialidad, integridad, privacidad y autenticidad de quienes realizan las comunicaciones.

La cuenta de correo asignada es de carácter individual; por lo tanto, ningún funcionario bajo ninguna circunstancia debe usar la cuenta de correo de otro funcionario.

2.5.2. Uso de Internet

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

Está completamente prohibido el uso del internet para:

- Acceso a sitios inapropiados haciendo uso de equipos e infraestructura tecnológica de FENOCO. Ejemplos de sitios de este tipo podrían incluir, aunque no se limitan a: sitios sexualmente explícitos, Sitios para hackers, Sitios relacionados Con software ilegal o herramientas para hackers, sitios que

pudieran entrar en conflicto con las políticas y/o intereses comerciales de FENOCO.

- Reenvío masivo de anuncios publicitarios o cadenas de mensajes de tipo comercial, político o religioso entre otros y, cualquier contenido ofensivo para los funcionarios de la compañía.
- Juegos en línea.
- Envío descarga de material pornográfico, archivos de texto inapropiados, o archivos que pongan en peligro la integridad de la red.

2.5.3. Conexiones Remotas

Todo 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 contraseña personal intransferible.

3. ACCESOS

3.1. Accesos Lógicos

3.1.1. Acceso a Información

Los usuarios deben contar con la aprobación de su superior Inmediato para acceder a los sistemas de información o las aplicaciones. El acceso a la información debe ser otorgado de acuerdo con las funciones y responsabilidades del cargo.

3.1.2. Protección de Contraseñas

- Las contraseñas son consideradas como personales e intransferibles y deberán estar bien protegidas personales 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 dela misma; sino cumple lo descrito en los puntos anteriores.

3.1.3. Política de Escritorio Limpio

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

3.1.4. Detección y Prevención de Virus

La Dirección de Tecnología será responsable desinstalar y activar un software antivirus licenciado, en cada computador de escritorio, computador 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.

Igualmente, los archivos adjuntos a e-mails entrantes deben ser examinados para detectar virus, si se detecta alguna anomalía deberá ser notificado inmediatamente a la Dirección de IT.

3.2. Acceso Físico

El acceso a las oficinas o instalaciones donde se encuentran ubicados los recursos informáticos solo será permitido para el personal del área de Tecnología, en caso que se requiera el ingreso de personal ajeno al área, deberá realizarse con previa autorización y/o acompañamiento.

4. POLÍTICAS DE DERECHO DE AUTOR

4.1. 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 con lo establecido en el Reglamento Interno del Trabajo y/o Código de Conducta de la compañía.

4.2. Programas Compartidos "Shareware" y programas Libres de Derechos "Freeware".

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

5. GLOSARIO

- **Vulnerabilidad**: Debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.
- **Sniffers**: Software o hardware que se utiliza para monitorizar, capturar y analizar en tiempo real los paquetes de datos que pasan por una red.
- **Anti-virus**: Software que brinda protección a los dispositivos contra diferentes tipos de amenazas virtuales o locales.
- **Shareware**: Modalidad de distribución de software, en la que el usuario puede evaluar de forma gratuita el producto, pero con limitaciones en el tiempo o forma de uso.
- **Freeware**: Tipo de software que se distribuye sin costo, de manera ilimitada.
- **Firewall**: Dispositivo de seguridad (hardware y software) que monitorea el tráfico de red entrante y saliente y decide si permite o bloquea tráfico especifico en función de un conjunto definido de reglas de seguridad.
- **Hackers**: Persona que descubre las debilidades de un computador, sistema de comunicación e información.

La presente política entra en vigencia a partir del día 24 de Abril 2025 y deroga todas las disposiciones anteriores y estará vigente hasta que una nueva política modifique o derogue la presente.

ANDRES SOTO VELASCO
Presidente