1. OBJETIVO

Dar a conocer las normas en seguridad de la información y seguridad informática, aplicadas en la operación del servicio de FENALCO.

2. ALCANCE

Estas políticas aplican para todos los usuarios de FENALCO que tengan asignado un computador, conectado a la red corporativa, ejecutando labores asignadas según el cargo a desempeñar.

3. DEFINICIONES

3.1. **Usuario:** Persona contratada por FENALCO, autorizada para hacer uso de las Facilidades Tecnológicas.

3.2. **Equipo Institucional:** Equipo (computadoras de escritorio, portátiles, servidores, equipos de comunicación y otros equipos electrónicos) usado en el desempeño de sus funciones.

3.3. **Software Institucional:** Software que el área Tecnología de la Información ha definido como "Software de Uso Estándar", del cual se ha adquirido e inscrito a su nombre todas las licencias respectivas.

3.4. **Facilidades Tecnológicas:** Todos aquellos recursos de tecnología de información, disponibles para el usuario. Entre ellos se encuentran las licencias de uso de software, los sistemas automatizados, las computadoras, los servidores, las redes de transmisión de datos y sus medios de acceso, etc.

3.5. **Comunicaciones electrónicas:** Todo tipo de comunicación enviada por medios digitales en cualquier tipo de formato, incluyendo sus anexos (attachments).

3.6. **BYOD (Bring Your Own Device):** cuya traducción sería “trae tu propio dispositivo”, hace referencia a que los empleados tienen la posibilidad de utilizar sus propios dispositivos (ordenadores portátiles, smartphones y tabletas) para acceder a los recursos de su compañía.

3.7. **Incidente de seguridad:** Es la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información y que violan la Política de Seguridad de la Información de la organización.

3.8. **Teletrabajo:** De acuerdo con la Ley 1221 de 2008 es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación - TIC para el contacto

entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

3.9. **Trabajo en Casa:** De acuerdo con la Ley 2088 de 2021 se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones.

3.10. **Trabajo Remoto:** De acuerdo con la Ley 2121 de 2021 es una forma de ejecución del contrato de trabajo en la cual toda la relación laboral, desde su inicio hasta su terminación, se debe realizar de manera remota mediante la utilización de tecnologías de la información y las telecomunicaciones u otro medio o mecanismo, donde el empleador y trabajador, no interactúan físicamente a lo largo de la vinculación contractual. En todo caso, esta forma de ejecución no comparte los elementos constitutivos y regulados para el teletrabajo y/o trabajo en casa.

4. DESCRIPCION

4.1. Para todo el personal que ingrese nuevo a FENALCO se le debe dar a conocer la existencia y funcionamiento de estas políticas y se registrara en el Formato FRM-TH-03 Programa de Inducción y/o FRM-GC-09 Formato Lista de Asistencia.

4.2. FENALCO mediante la aplicación de controles y políticas de seguridad, asegura la confidencialidad, integridad y disponibilidad de la información interna y de los clientes. Protege los activos de información, a través de la gestión de riesgos y la administración de los planes de continuidad de negocio.

4.3. Los equipos de cómputo utilizados por el usuario podrán ser:

- Computador asignado por Fenalco, provisto con el licenciamiento para todo el software utilizado y a través de conexión VPN.
- Computador propio del Usuario: a través de conexión VPN

4.4. Política de Sesión Abierta

4.4.1. Objetivo

Evitar la suplantación de identidad con el fin de impedir robos, fraudes, transferencias y modificaciones en los sistemas de información utilizados en las líneas de atención de servicio al cliente.

4.4.2. Condiciones Generales

a) Cuando se habla de "Sesión Abierta" se hace referencia a no cerrar la sesión de usuario en Windows al abandonar su puesto de trabajo.

b) Con el fin de mantener la seguridad y la identidad de cada funcionario durante la ejecución de la operación, este debe cerrar su sesión cada vez que se ausente de su puesto de trabajo.

c) Con el fin de supervisar la efectividad de la política cualquier empleado será el encargado de reportar su incumplimiento al Coordinador y/o Supervisor quien debe reportar la falta al Jefe Inmediato del área quien tiene la responsabilidad de diseñar sanciones de tipo educativo con el propósito de crear cultura y facilitar la implementación de la presente política cuando un funcionario la incumpla.

d) Transcurridos 3 meses desde la publicación, socialización e implementación de la presente política se aplicarán las sanciones disciplinarias derivadas del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), de acuerdo a los procedimientos establecidos por la Organización y en estricto acato de las estipulaciones legales vigentes.

4.5. Política de Usuarios

4.5.1. Objetivo

Establecer los parámetros que deben tener en cuenta los usuarios, con el fin de garantizar que la seguridad de la información es gestionada correctamente.

4.5.2. Condiciones Generales

a) A cada usuario se le asignarán un usuario de red con el fin de poder identificarse y tener acceso a los recursos necesarios para el correcto desempeño de sus labores

b) La solicitud de una nueva cuenta o el cambio de privilegios debe ser realizada diligenciando el formato *"FRM-IT-01 "Formato Solicitud de Requerimientos"* creado para solicitar servicios de informática y debe ser debidamente aprobada por el Jefe Inmediato.

c) No debe concederse una cuenta a personas que no sean empleados de la Organización a menos que estén debidamente autorizados por el Jefe Inmediato, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

d) Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a usuarios directamente responsables de la administración o de la seguridad de los sistemas.

e) No deben otorgarse cuentas a técnicos de mantenimiento a menos que el área de IT de FENLCO determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo.

f) Se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad.

g) Toda cuenta queda automáticamente suspendida después de 30 días de inactividad.

h) El Coordinador de Infraestructura o el Supervisor de Help Desk debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.

i) Cuando un empleado es despedido o renuncia, debe desactivarse su cuenta antes que deje el cargo.
j) A menos que sea formalmente autorizado por un Cargo Superior, el usuario no deberá utilizar o divulgar códigos, claves o contraseñas de acceso de otro usuario, así como abrir, borrar, modificar o recuperar archivos que no son de su propiedad.

4.6. Políticas de Escritorios Limpios

4.6.1. Objetivo

Garantizar que los medios magnéticos y físicos que contienen información propia de la entidad se encuentran resguardados en los escritorios de los miembros de la comunidad que labora en la entidad.

4.6.2. Condiciones Generales

a) Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD, memorias USB y otros dispositivos de almacenamiento, (dichos dispositivos son usados, solo por el personal autorizado por el Departamento de Informática y Telecomunicaciones), con el fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo. Los dispositivos de almacenamiento deben ser guardados bajo llave, especialmente aquellos en los que se hayan realizado copias de respaldo de archivos magnéticos, los documentos sensibles también deben permanecer guardados bajo llave.
b) Revisar que deja su lugar de trabajo en orden, los equipos apagados y ningún documento sin guardar, antes de irse definitivamente de su oficina o puesto de trabajo.

c) En períodos prolongados conocidos fuera del puesto de trabajo, Ej: hora de almuerzo, se espera que los documentos sensibles sean colocados en cajones cerrados.
d) Asignar tiempo para eliminar el papeleo.
e) Siempre se debe limpiar el área de trabajo antes de salir por períodos más largos de tiempo.
f) Bloquear el escritorio y archivadores al final del día.
g) El incumplimiento de esta política conllevará a notificación al superior inmediato, con copia a Gestión Humana.

4.7. Políticas de Contraseña Segura

4.7.1. Objetivo

Establecer un estándar para la creación de contraseñas fuertes, la protección de dichas contraseñas, y el cambio frecuente de las mismas.

4.7.2. Condiciones Generales

a) Todos los usuarios son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos para el desempeño de sus actividades cotidianas.

b) El ámbito de esta política incluye a todos aquellos usuarios de los servicios y recursos Informáticos que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera una contraseña) en cualquiera de los servicios de esta campaña.

c) Todas las contraseñas de cuentas que den acceso a recursos y servicios de la Organización deben seguir las siguientes directrices generales:

d) Las claves de acceso son personales e intransferibles y de acuerdo con un perfil especifico por lo tanto no pueden ser utilizadas por una persona diferente a la que fue asignada.

e) Usar claves de acceso que no estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.

f) Cambiar de clave de acceso mensualmente, requerido por parámetro por el Sistema Operativo.

g) Es responsabilidad del usuario el buen uso de los privilegios que se le han otorgado para su desempeño laboral.

h) La longitud de las contraseñas no debe ser inferior a los seis caracteres.

i) Las contraseñas deben estar formadas por una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas) y números.

j) La contraseña no debe contener el identificador o el nombre del usuario.

k) Cuando se realice un cambio de contraseña, esta debe ser diferente de las 12 utilizadas anteriormente por el mismo usuario.

4.8. Del Uso de la Red Institucional y de sus Recursos

a) Las identificaciones y claves de entrada a la Red Institucional, la Intranet o a cualquier otro recurso tecnológico son propiedad de la campaña. Estas identificaciones y claves son para uso estrictamente personal del usuario al que se le asignan y por lo tanto la responsabilidad por el uso correcto de las mismas recae exclusivamente en el usuario mismo.

b) El usuario no podrá, por restricciones del perfil, hacer modificaciones a la red institucional, la intranet o a sus recursos. No se permitirá ningún intento de vulnerar o de atentar contra los sistemas de protección o de seguridad de la red. Ante cualquier acción de este tipo la Organización procederá a ejecutar cualquier acción de carácter administrativo, laboral, penal y/o civil que corresponda.

c) En la red Institucional se controla y restringe la operación de software para la descarga y distribución de archivos de música, videos y similares. Cualquier aplicación de este tipo que requiera ser utilizada, deberá ser previamente consultada con la dirección de tecnologías de información.

d) El usuario no podrá compartir archivos y carpetas en el computador asignado, excepto con la autorización del Coordinador y/o Supervisor del área y el Coordinador de Infraestructura, solo se podrán usar para compartir documentos laborales. Esta funcionalidad es administrada únicamente por el Coordinador de Infraestructura de FENALCO. Las carpetas compartidas en los servidores y asignadas a las áreas, solo podrán contener documentos laborales.

e) La seguridad de los recursos compartidos en el computador es responsabilidad del usuario.

f) Está prohibido acceder o intentar acceder a cualquier tipo de información (archivos o programas) para la cual no se está autorizado.
g) No está permitido el uso de módems en PCs que tengan conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN de la organización.
h) Deben tener control con acceso a las redes, quitarle los privilegios e implementar restricciones, donde no puedan hacer cambios en la configuración del equipo y se restringa el modo de instalar software.

4.9. De la Instalación y Uso de Software

a) De acuerdo con las normas locales e internacionales relativas a los derechos de propiedad intelectual, el único software que será instalado en el computador del usuario será aquel que previamente haya sido estandarizado y/o autorizado por la campaña y para lo cual esta dispone de las licencias respectivas a su nombre y sea necesario para el correcto desempeño de las labores del usuario.
b) Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso.
c) Solo el personal de soporte del área de Informática y Telecomunicaciones de FENALCO está autorizado de la instalación del software, por restricciones del perfil el usuario no puede instalar ningún tipo de software (Ejemplo: salva pantallas, software gratuito y/o juegos).
d) Adicionalmente, todo usuario debe garantizar el cumplimiento de los siguientes lineamientos:
e) El usuario no deberá participar en la copia, distribución, transmisión o cualesquiera otras prácticas no autorizadas en las licencias de uso de software. Cualquier duda al respecto deberá ser consultada con el área de IT de FENALCO.
f) Toda instalación, desinstalación o traslado de software (incluyendo aquellos de "dominio público" o de "distribución libre"- "shareware", "freeware", etc.) desde y hacia el Equipo Institucional requiere autorización y coordinación previas con el área de IT de FENALCO.
g) Cualquier requerimiento de licencias de software que deban ser consideradas como parte del Equipo Institucional y que podrían ser utilizadas por el usuario para el desarrollo de la actividad de la campaña, deberá ser solicitado en forma escrita a la Jefatura del área de IT de FENALCO para su respectiva valoración y autorización. Cualquier software que se haya instalado en el equipo institucional que no cumpla con lo estipulado anteriormente, será desinstalado sin que ello derive ninguna responsabilidad para la Organización.
h) Al usar una licencia de software que ha sido instalado en el equipo institucional el usuario reconoce los derechos de descritos y consiente en ellos.

4.10. Del Uso de Internet

a) El acceso a Internet sólo se asignará a aquellos cargos que lo requieran para su desempeño laboral.
b) El uso de Mensajería instantánea debe ser con fines laborales y debe ser autorizado por el Jefe Inmediato y otorgado por el área de IT de FENALCO.

c) No se permite la navegación por Internet, envío o recepción correo electrónico, mensajería instantánea, ni ningún otro servicio que permita el intercambio de información a menos que el tercero lo solicite por escrito.
d) La asignación del servicio de Internet no implica que el usuario tenga total privacidad sobre el uso realizado, la empresa tiene la potestad de hacer seguimiento y control sobre las páginas accesadas.
e) El uso del servicio de Internet debe ser prudente y sólo para aquellas actividades relacionadas con el desempeño laboral.
f) El servicio de Internet no debe ser usado para acceder a páginas con fines no laborales.
g) No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.
h) No se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes compartidas como KaZaa, Morpheus, BearShare, etc. o vía FTP.
i) Está prohibido bajar por Internet música, videos o software no autorizados por el Coordinador de Soporte o Administrador de Servicios de red.

4.11. Del Uso de los Computadores

a) Los equipos de cómputo del cliente, solo deben tener instalado los aplicativos de uso de trabajo únicamente para esta campaña y sus accesos URLs estrictamente necesarios.
b) Ningún computador puede ser retirado sin una autorización firmada por el Jefe Inmediato
c) Los equipos deben ser debidamente conectados en las tomas adecuados, o sea aquellos marcados como UPS. Cualquier anomalía o inquietud debe ser comunicada a mantenimiento.
d) No conecte otros aparatos (Radios, máquinas de escribir, calculadoras, etc.) en la misma toma del computador.
e) Los computadores se entregan configurados con el estándar de la compaña y según la necesidad de usuario, por lo tanto, no está permitido modificar estas configuraciones por personal diferente al área de Soporte de Sistemas y debidamente soportada por una solicitud de servicio.
f) El computador es una herramienta de trabajo por lo tanto la persona es responsable de este y debe garantizar su buen manejo reportando oportunamente cualquier anomalía al área de Sistemas o Seguridad, según el caso.
g) Todos los periféricos (Impresora, teclado, ratón, modem, parlantes, quemador de CD, scanner, etc.), son responsabilidad del usuario, por lo tanto es su responsabilidad informar inmediatamente al personal de Informática y Telecomunicaciones en caso de pérdida o daño
h) El consumo de alimentos cerca al equipo de cómputo no está permitido. En caso de daño del equipo por causa inherente a este consumo (bebidas derramadas, migas en teclado, etc.), el usuario al que

se asignó dicho equipo es responsable por los costos en que se incurra por la reparación o reemplazo del elemento.

i) Solo el personal de Soporte de Informática y Telecomunicaciones está autorizado de la instalación del software, el usuario no puede instalar ningún tipo de Software (Ejemplo: salva pantallas, software gratuito y/o juegos).

j) El equipo asignado al personal debe ser utilizado solamente para las actividades laborales propias de su cargo.

k) Los equipos de cómputo no pueden ser reubicados ni reasignados a otro usuario sin la autorización del área de Informática y Telecomunicaciones.

l) Los documentos almacenados en el disco duro del computador, deben reposar en una sola carpeta de acuerdo con la indicación del área de Informática y Telecomunicaciones.

m) Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Así como de definir qué información debe respaldarse y la frecuencia del respaldo.

n) Para prevenir el acceso no autorizado, el usuario debe activar el protector de pantalla manualmente, oprimir al tiempo Ctrl.+Alt+Sup, cada vez que se ausente de su oficina y que requiera una contraseña para reasumir la actividad.

o) Los usuarios no deben copiar a medio removible el software o los datos residentes en las computadoras de la Organización, sin la aprobación previa del Coordinador de la campaña.

p) No deben usarse medios de almacenamiento externos en ninguna computadora.

q) No está permitido conectar computadores portátiles de personas ajenas a la campaña y en caso de ser necesario se requiere solicitar la autorización correspondiente por el Jefe Inmediato.

r) Se debe mantener una hoja de vida de los equipos de cómputo de la campaña, con información de la configuración, aplicativos instalados, Red, usuario, inventario general actualizado, etc.

4.12. De las Comunicaciones Electrónicas

a) El correo electrónico sólo puede ser usado por el personal autorizado por la organización.

b) El tamaño de los archivos adjunto debe ser lo más pequeño posible, debido a que se afecta la velocidad que se requiere para el óptimo funcionamiento de la red.

c) En vista de que las Comunicaciones Electrónicas pueden, en algún evento fortuito, ser interceptadas por terceras personas, la Organización no puede garantizar la confidencialidad de la información enviada y/o recibida a través de este medio.

d) El usuario acepta que la Organización no está en capacidad de protegerle de ataques o mensajes ofensivos que le pudieren llegar a través de la red de comunicaciones. Por tanto, la Organización no asume ningún tipo de responsabilidad en este sentido.

e) La organización no garantiza la privacidad de la información que se maneje en el correo electrónico. La empresa tiene la potestad de revisar la información si lo considera necesario.

f) No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.

g) No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.

h) A menos que sea formalmente autorizado por un supervisor apropiado, el Usuario no deberá utilizar o divulgar códigos, claves o contraseñas de acceso de otro usuario, así como abrir, borrar, modificar o recuperar archivos que no son de su propiedad.

i) Son expresamente prohibidas las siguientes acciones:

i. Envío de correo electrónico de carácter personal que resulte masivo y/o no solicitado.
ii. Propagación de cadenas de mensajes.
iii. Publicación de anuncios personales sin autorización de la Organización (servicios, productos, objetos y otros).
iv. Transmisión de material ilegal, de acoso, difamatorio, amenazador, nocivo, vulgar, obsceno o de cualquier otra manera censurable.
v. Divulgar o promover ideales políticos, religiosos o sociales.
vi. Transmitir cualquier material que contenga virus o mensaje que puedan generar daños en el funcionamiento de los equipos de cómputo.
vii. Transmisión de material diferente al requerido para la ejecución de las funciones propias del trabajo asignado.

4.13. Incumplimiento de Políticas de Riesgo

a) La Organización hará responsable al usuario del conocimiento de la presente política y las consecuencias que se derivarían de su incumplimiento. Así mismo, el usuario deberá conocer estas políticas desde su ingreso a la campaña.

b) FENALCO y el tercero se reservan el derecho de evaluar periódicamente el cumplimiento de estas políticas. Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por la organización y en estricto acato de las estipulaciones legales vigentes.

c) En materia de irregularidades o incumplimiento en el uso del software, el usuario que no cumpla con esta política será directamente responsable de las sanciones legales (que por responsabilidad laboral, penal y/o civil se incurra) derivadas de sus propios actos. Igualmente, será responsable de los costos y gastos en que pudiera incurrir la organización derivados de la defensa por el uso no autorizado o indebido de licencias de software.

4.14. Confidencialidad de la Información

a) Es obligación prioritaria de los usuarios de los recursos de TI, durante el tiempo que labore para la Organización el guardar absoluta reserva de los hechos, documentos, informaciones y en general, sobre todos los asuntos y materias que lleguen a sus conocimientos por causa o con ocasión de las labores desempeñadas en su cargo.

El usuario de los recursos de TI se compromete a no divulgar información a ninguna persona, excepto a los empleados que necesariamente deban conocer dicha información.

La organización considerará como justa causa para dar por terminado el contrato de trabajo, el que el usuario de las TI revele los secretos técnicos o comerciales o dé a conocer cualquier información que pertenezca a un tercero y/o cliente.

4.15. Trabajo en Casa, Teletrabajo y/o Trabajo Remoto

El acceso remoto a los recursos corporativos desde los equipos de teletrabajo, trabajo en casa y/o trabajo remoto debe realizarse a través de una conexión VPN que se provee desde el área de TI y sólo se debe permitir acceso a los recursos para los cuales se haya autorizado.

Para evitar que terceros espíen su actividad o roben datos de la empresa, los usuarios deben utilizar una conexión Wi-Fi privada y segura. Esto significa que:

- La red Wi-Fi debe estar protegida con contraseña y el proveedor de Wi-Fi debe ser conocido.
- Las contraseñas deben ser únicas y no compartidas.
- Evite el uso de una contraseña predeterminada en cualquier tecnología.
- Evite las redes Wi-Fi públicas no seguras

Una VPN proporciona una conexión segura entre su dispositivo y la red de la empresa. Todos los datos transferidos de un lado a otro entre estos puntos están encriptados. El cifrado proporcionado por la VPN garantiza que los delincuentes no puedan obtener claves o los datos que se transfieren entre su dispositivo y los recursos de su empresa. Cuando se inicia sesión en la VPN puede acceder a la información y realizar sus funciones como lo harían normalmente en la oficina, pero desde cualquier ubicación.

El acceso al correo electrónico y los aplicativos Web institucionales se hará a través de los navegadores conocidos.

No instalar programas o extensiones de navegadores de fuentes desconocidas ya que estas suelen traer malware el cual puede afectar sus dispositivos y extraer la información sensible.

Para el teletrabajo, trabajo en casa y/o trabajo remoto se permitirá el uso de equipos personales, bajo el compromiso de uso de software legal y antivirus actualizado y de requerirse se creará conexión VPN para acceso a los recursos autorizados.

En estos casos el equipo debe ser revisado por el área de IT para asegurarse de que todo el software esté actualizado antes de acceder a los sistemas de la empresa. Con esto se busca evitar que dispositivos de alto riesgo se conecten a los sistemas de la organización.

En los equipos de cómputo de los usuarios, no se deberá almacenar información corporativa. Esta información deberá quedar en un repositorio en un servidor de archivos definido para tal fin, en donde se controle el acceso. Para este caso la organización tiene disponible el Drive de Google y servidores.

La información del repositorio del servidor de archivos definido para los usuarios está sujeta de una política de respaldo y retención. De requerir un backup especial lo debe solicitar al área de IT.

Si la clasificación de la información que produzca procese o transfiera el usuario teletrabajador, de trabajo en casa y/o trabajo remoto lo requiere, se deben celebrar acuerdos de confidencialidad o de no divulgación.

La contraseña de inicio de sesión en el equipo de cómputo del usuario de teletrabajo, trabajo en casa y/o trabajo remoto debe tener una vigencia definida de acuerdo con las políticas de seguridad de la información.

Impedir guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.

Los equipos siempre deben tener un software antivirus, puede ser comprado o gratuito. La base de firmas y definiciones del producto de protección antivirus debe actualizarse cuando el equipo de cómputo del usuario se conecta desde el sitio remoto.

Los equipos siempre deben tener activado un Firewall para impedir que los atacantes o las amenazas externas accedan al sistema identificando y bloqueando el tráfico no deseado.

El equipo de cómputo del usuario debe descargar y aplicar las actualizaciones de seguridad del sistema Operativo y otras actualizaciones de software que requiera para sus funciones. Posponer la actualización de sus aplicaciones puede provocarle problemas a largo plazo. Es importante que lo haga inmediatamente, como una forma de prevenir ataques informáticos en sus dispositivos.

Las actualizaciones se encargan de corregir errores en sus dispositivos, agregar nuevas características y, entre otras cosas, arreglar los huecos y debilidades en la seguridad informática que los hackers suelen aprovechar. El área de IT debe configurar en los computadores las actualizaciones automáticas para que el teletrabajador pueda descargar el parche de forma segura.

En ninguna circunstancia los empleados deben buscar en Internet el software que necesitan para cumplir con su trabajo. El software o las aplicaciones no aprobadas pueden contener virus u otros tipos de malware.

Los usuarios deben aceptar la política de uso y restricción de software. Esta señala que no pueden instalar ningún software en el equipo o usar alguno que se encuentra por fuera de la línea base definida por el área de TI de la organización.

El usuario debe conocer y cumplir las políticas de seguridad de la información y de protección de datos personales establecidas en la organización.

El usuario debe tomar las medidas necesarias en caso de robos o pérdidas, estas situaciones pueden poner en riesgo su información y la de la empresa. Debido a lo anterior, el usuario deberá colocar una denuncia ante las autoridades correspondientes e informar de manera inmediata a su jefe inmediato, área de gestión humana, área de TI y demás contactos. Siempre que pueda hacerlo, trate de rastrear el dispositivo a través de las opciones que las diferentes marcas ofrecen. Esta información de seguimiento es vital para la policía. En caso de que el ladrón burle el sistema de bloqueo del dispositivo, usted debe entrar a los sitios web de las aplicaciones que usa, para cerrar las sesiones y cambiar las contraseñas.

La protección de la información confidencial de la empresa es especialmente importante. En caso de presentarse un incidente de seguridad, deberá reportarse de manera inmediata a su jefe inmediato y área de TI con el fin de que se puedan realizar las acciones que correspondan, tendientes a mitigar el riesgo. Algunos consejos para ayudar a proteger su espacio son:

a) Evite el uso de dispositivos personales para el trabajo.

b) Evite el uso de aplicaciones o hardware externo que no estén aprobados por la empresa (por ejemplo, iCloud o unidades externas para almacenar documentos).

c) Prohibir a los miembros de la familia el uso de los dispositivos para fines personales durante la jornada de trabajo.

d) Habilite la pantalla de bloqueo protegida con contraseña en sus dispositivos cada vez que se aleje.

e) Evite dejar los dispositivos al aire libre durante períodos prolongados o en un lugar donde sean visibles a través de una ventana y, por lo tanto, vulnerables al robo.

f) Los documentos físicos de la empresa deben guardarse en un lugar seguro al terminar la jornada.

g) Ponga especial atención a lo que otras personas pueden ver detrás o alrededor de usted. Hay que asegurarse de que no se vea ninguna información confidencial relacionada con el trabajo. Esto podría incluir:

- Horarios
- Notas de reuniones o proyectos no relacionados
- Información confidencial del cliente
- Información confidencial del empleado

h) Esté atento a los dispositivos domésticos digitales activados por voz mientras trabaja. Estos dispositivos pueden grabar accidentalmente el audio de llamadas telefónicas o videoconferencias confidenciales del trabajo.

i) No enviar archivos con información de la organización y/o entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.

Siempre se debe requerir una autenticación sólida, que incluya un nombre de usuario y una contraseña para iniciar sesión en los dispositivos y acceder a las redes de la empresa.

Utilice contraseñas que no puedan verse comprometidas fácilmente, estableciendo estándares de buena etiqueta para generar las contraseñas:

- Una combinación de letras mayúsculas y minúsculas
- Que contenga números y caracteres especiales
- Una longitud mínima de 10 caracteres.
- Rotación obligatoria de contraseñas después de un período de tiempo establecido (por ejemplo: 30 días).
- Las contraseñas deben ser únicas, complejas y no deben compartirse.

Siempre que sea posible, se integrará la autenticación multifactor para una capa adicional de seguridad durante el inicio de sesión.

Limitar el uso de dispositivos externos como las USB en los equipos utilizados para el teletrabajo, trabajo en casa y/o trabajo remoto.

Optimizar el uso del internet, dado que por un mismo canal se van a establecer todas las conexiones, priorice las actividades laborales en los horarios establecidos para que no sufra caídas del servicio.

Se debe tener especial cuidado con los virus y las estafas de phishing y pharming, estos ataques se han vuelto cada vez más sofisticados. Un ataque de phishing ocurre cuando un delincuente se disfraza de fuente legítima para obtener datos confidenciales de su empresa y empleados o infectar sus dispositivos y sistemas con malware.

Verificar la credibilidad cuando reciba alguna información que le genere desconfianza, revisa en los buscadores si otras personas han hecho preguntas o búsquedas relacionadas con esa marca o servicio. Un buen ejercicio es revisar si tienen redes sociales para conocer la opinión de más personas.

A continuación, se ofrecen algunos consejos sobre cómo los usuarios pueden evitar problemas:

a. Correo electrónico

- Ser escéptico sobre cada correo electrónico que llegue a la bandeja de entrada.

- Tener cuidado con los remitentes de correo electrónico que utilizan nombres de dominio sospechosos o engañosos o líneas de asunto inusuales. Si sospecha del remitente, no abrir el correo electrónico.
- Nunca abrir archivos adjuntos ni hacer clic en enlaces incrustados en correos electrónicos de remitentes que no reconoce.
- Informar al área de TI si recibe correo electrónico sospechoso y no responderlo.
- Tener mucho cuidado al ingresar contraseñas cuando se soliciten por correo electrónico. Asegurarse de verificar la autenticidad del sitio web de destino.

b. Sitios web falsos

- No registrarse en cualquier sitio, ni instalar cualquier programa. Verificar que la página que está visitando tenga certificado de seguridad, es decir, que inicie con https, sobre todo si se va a incluir información personal.
- Estos sitios pueden proporcionar cifrado para mejorar la apariencia de legitimidad.
- Prestar especial atención a los enlaces del sitio web para confirmar que está visitando el sitio correcto. Los ciberdelincuentes escriben mal los enlaces de los sitios web de formas sutiles, por lo que son sumamente parecidos como para parecer legítimos y engañarlo si no lee cuidadosamente.
- Habilitar la autenticación de múltiples factores para cada inicio de sesión.
- No seguir los enlaces que se reciben en un correo electrónico. Abrir una pestaña en su navegador e ingresar directamente el enlace correcto del sitio que desea visitar. No confiar en que el correo electrónico lo llevará al destino correcto.

c. Software antivirus

- Siempre se debe activar un software antivirus.
- Los usuarios no pueden deshabilitar el software antivirus

La información en papel debe ser destruida correctamente evitando tirarla directamente al contenedor del reciclaje o designándolo como hojas de borrador para labores domésticas.

Los documentos impresos deben ser almacenados de acuerdo con su sensibilidad en un lugar seguro mientras no se estén utilizando.

Recuerde que, aunque se esté trabajando de forma remota, siempre debe garantizar la seguridad de los datos y cumplir con las exigencias de seguridad impuestas por la organización y/o Entidad y la ley de protección de datos personales.

El retiro del recurso humano de la organización debe ser controlado garantizando la eliminación de las credenciales de acceso a los sistemas. Revocando en primer lugar aquellos accesos a los sistemas más críticos o vulnerables, y además hacer un monitoreo del uso de las cuentas de correo electrónico para

garantizar que no se extraiga información confidencial. Todo lo relacionado con la finalización de contrato estar formalizado para incluir el retorno previo del software, documentos corporativos, dispositivos móviles e información guardada en medios electrónico, etc.

4.16. Roles y Responsabilidades para la Seguridad de la Información

Es responsabilidad del área de TI evaluar, actualizar, verificar y socializar las políticas de seguridad de la información.

El área de TI es responsable de revisar y proponer a las directivas para su aprobación, el texto de la Política de Seguridad de la Información para teletrabajo, las funciones generales en materia de seguridad de la información y la estructuración, recomendación, seguimiento y mejoras en pro de la seguridad de la información. Es responsabilidad de dicha área definir las estrategias de capacitación en materia de seguridad de la información al interior de FENALCO.

La Gerencia de TI es responsable de implementar los controles tecnológicos definidos en pro de la seguridad de la información.

El área de recursos humanos proporcionará los mecanismos para propender por notificar a todo el personal que se vincula contractualmente con FENALCO, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información para el teletrabajo, trabajo en casa y/o trabajo remoto y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan como recomendación del área de TI.

La Jefatura Jurídica propenderá porque en todos los contratos que suscriba FENALCO quede consignada la cláusula de confidencialidad y la obligatoriedad tanto de trabajadores como de proveedores de dar cumplimiento a las políticas de seguridad de la información y tratamiento de datos personales.

4.17. Sensibilización Y Concienciación En Seguridad Para Colaboradores

Esta política debe ser socializada de acuerdo con las actualizaciones que puedan llevarse a cabo, y publicarla en la intranet y pagina web de la Entidad para conocimiento de todo el personal objetivo e incluirla en el proceso de inducción de nuevos funcionarios y contratistas.

Todo el personal de la organización con acceso a los sistemas de información corporativos debe recibir formación relacionada con buenas prácticas en materia de seguridad de la información y ciberseguridad en el desempeño de sus funciones.

El Coordinador de Selección, Bienestar y Desarrollo y/o persona asignada es la encargada de dar la bienvenida al personal nuevo y realizar la presentación corporativa. De igual manera tendrán un espacio durante la inducción corporativa para abordan los temas relacionados con la seguridad de la información.

Una vez terminada la inducción se realizará evaluación a la inducción presentada, la cual será objeto de calificación.

El usuario debe asistir a las capacitaciones, inducciones, entrenamientos, cursos, seminarios, talleres y cualquier otro tipo de actividad de actualización o de formación relacionadas con seguridad de la información programada por el empleador, o a las que la empresa los delegue para que participen; y cumplir con los requerimientos mínimos de evaluación de estas en cada caso.

Estas acciones buscan educar a los empleados sobre los diferentes riesgos y amenazas que existen en ciberseguridad, así como los posibles puntos débiles en un sistema. Se espera que los empleados entiendan de las mejores prácticas y procedimientos para mantener las redes y los datos seguros, así como las consecuencias de no hacerlo.

Estas consecuencias pueden incluir la pérdida del trabajo, sanciones penales o incluso daños irreparables a la empresa.

4.18. Supervisar Que Se Cumplen Las Buenas Prácticas En Seguridad

Se implementarán mecanismos para comprobar que los usuarios siguen los procedimientos definidos y que cumplen las normativas vigentes. Para tal efecto se podrán realizar auditorías, ya sean internas o externas. Además, se podrían llegar a utilizar herramientas de auditoría informática que registren las operaciones que realizan los usuarios en las aplicaciones y bases de datos corporativas, con objeto de garantizar la trazabilidad de esas operaciones.

5. CONTROL DE CAMBIOS

VERSIÓN	FECHA DE ACTUALIZACIÓN	DESCRIPCION DEL CAMBIO
01	20/08/2019	Creación del documento.
02	12/12/2023	Se incluye política para Teletrabajo.

ELABORADO POR	REVISADO POR	APROBADO POR
Original Firmado _____ Diana Marcela Ramirez Líder de Infraestructura	Original Firmado _____ Richard Antonio Castaño Gómez Jefe de Informática y Telecomunicaciones	Original Firmado _____ Richard Antonio Castaño Gómez Jefe de Informática y Telecomunicaciones