POLÍTICA DE USO ACEPTABLE Y DISPOSITIVOS MÓVILES

CONTROL DOCUMENTAL		
Realizado por:	**Cargo**	**Fecha**
Andrés Gutiérrez	Ingeniero en Analítica de datos	20-09-2024
Aprobado por:	**Cargo**	**Fecha**
David Correa	Gerente General	

CONTROL DE CAMBIOS			
VERSIÓN	**FECHA**	**CAMBIO**	**REALIZADO POR**
1.0	20-09-2024	Creación de documento	Andrés Gutiérrez

CONTENIDO

1. Objetivo

El objetivo de esta política es garantizar un uso adecuado, seguro y eficiente de los activos de información y sistemas tecnológicos de COMFICA, protegiendo la confidencialidad, integridad y disponibilidad de la información.

2. Alcance

Esta política aplica a todos los colaboradores, contratistas y terceros que tengan acceso a la información de COMFICA, independientemente de su formato (digital o físico) o ubicación (local o remota).

3. Definiciones

- Activos de Información: Todos los sistemas, bases de datos, documentos, aplicaciones, equipos de cómputo, servidores y redes de comunicación propiedad o bajo la custodia de COMFICA.
- Dispositivo Móvil: Teléfonos inteligentes, tablets, computadoras portátiles y otros dispositivos que permiten acceso a la información de COMFICA desde fuera de las instalaciones.
- Teletrabajo (VPN): El acceso remoto a los sistemas de información mediante una conexión segura (VPN), permitiendo a los colaboradores realizar sus funciones fuera de la oficina.
- Antivirus: Software de seguridad que protege los equipos y redes de COMFICA contra malware, virus y otras amenazas cibernéticas.
- Escritorio Limpio: Política que asegura que toda la información confidencial se almacene de manera segura y no se deje en áreas visibles cuando no se está utilizando.
- Pantalla Limpia: Política que garantiza que las pantallas de los dispositivos estén bloqueadas o apagadas cuando no se utilicen para evitar accesos no autorizados.
- Acceso Remoto: El uso de dispositivos para conectarse a los sistemas de COMFICA desde fuera de sus instalaciones.
- Incidente de Seguridad: Cualquier evento que ponga en peligro la confidencialidad, integridad o disponibilidad de la información de COMFICA.

4. Uso aceptable

El uso de los activos de información debe estar alineado con los objetivos laborales y operativos de COMFICA. Se espera que los usuarios hagan un uso responsable y adecuado de los recursos tecnológicos, evitando comprometer la seguridad de la información o los sistemas.

5. Responsabilidad sobre los activos

Queda prohibido el uso de los activos de COMFICA para actividades no relacionadas con el trabajo, incluyendo, pero no limitado a:

- Uso indebido de los sistemas de información: Acceso no autorizado, modificación o destrucción de información sin permiso.

- Instalación de software no autorizado: No se permite la instalación de software, aplicaciones o plugins sin la autorización del área de TI.
- Acceso a sitios inapropiados: Está prohibido acceder a sitios web que puedan comprometer la seguridad, como páginas con contenido malicioso o inapropiado.
- Uso de dispositivos personales: Está prohibido usar dispositivos personales para acceder a los sistemas de COMFICA sin autorización previa.
- Reproducción o descarga no autorizada de software o contenido multimedia.
- Compartir credenciales: Está estrictamente prohibido compartir nombres de usuario y contraseñas con cualquier persona.
- Manipulación de equipos: Modificar, reparar o intentar alterar los dispositivos móviles, redes o sistemas de información sin la autorización adecuada.
- Uso de correos electrónicos corporativos para actividades personales o fraudulentas.
- Uso de redes públicas no seguras: No se debe conectar a redes Wi-Fi públicas sin el uso de herramientas de seguridad como VPN. Utilizar los activos para actividades comerciales personales o ilegales.

6. Actividades prohibidas

Queda prohibido el uso de los activos de COMFICA para actividades no relacionadas con el trabajo, incluyendo, pero no limitado a:

- Uso indebido de los sistemas de información: Acceso no autorizado, modificación o destrucción de información sin permiso.
- Instalación de software no autorizado: No se permite la instalación de software, aplicaciones o plugins sin la autorización del área de TI.
- Acceso a sitios inapropiados: Está prohibido acceder a sitios web que puedan comprometer la seguridad, como páginas con contenido malicioso o inapropiado.
- Uso de dispositivos personales: Está prohibido usar dispositivos personales para acceder a los sistemas de COMFICA sin autorización previa.
- Reproducción o descarga no autorizada de software o contenido multimedia.
- Compartir credenciales: Está estrictamente prohibido compartir nombres de usuario y contraseñas con cualquier persona.
- Manipulación de equipos: Modificar, reparar o intentar alterar los dispositivos móviles, redes o sistemas de información sin la autorización adecuada.
- Uso de correos electrónicos corporativos para actividades personales o fraudulentas.
- Uso de redes públicas no seguras: No se debe conectar a redes Wi-Fi públicas sin el uso de herramientas de seguridad como VPN. Utilizar los activos para actividades comerciales personales o ilegales.

7. Uso de activos fuera de las instalaciones

El uso de dispositivos móviles y portátiles fuera de las instalaciones debe cumplir con los mismos estándares de seguridad que en las oficinas de COMFICA. Esto incluye el uso de contraseñas seguras, cifrado de la información y acceso a redes seguras (VPN).

8. Devolución de activos a la finalización de un contrato

Al finalizar la relación laboral o contractual, todos los activos, dispositivos y accesos asignados deben ser devueltos a COMFICA.

9. Protección antivirus

Todos los dispositivos que accedan a la red de COMFICA deben contar con software antivirus actualizado. Se realizarán revisiones periódicas para garantizar que los dispositivos estén protegidos.

10. Facultados para el uso de sistemas de información

Solo los colaboradores y contratistas autorizados tienen acceso a los sistemas de información de COMFICA. Los permisos se otorgan en función de los roles y responsabilidades asignadas, y se auditan periódicamente para garantizar su correcta asignación.

11. Responsabilidades sobre las cuentas de usuario

Cada usuario es responsable de proteger su cuenta y credenciales de acceso. Esto incluye el uso de contraseñas seguras y la no divulgación de estas a terceros.

12. Responsabilidades sobre las claves o contraseñas

Las contraseñas deben cumplir con los criterios de robustez establecidos por COMFICA en el **procedimiento de uso, creación, y gestión de accesos físicos y lógicos (SGSI-PR-10)**. Los usuarios son responsables de cambiar sus contraseñas de manera periódica y de mantenerlas seguras.

13. Política de pantalla y escritorios limpios

- Política de escritorio limpio:

Todos los usuarios deben asegurarse de que no haya documentos sensibles en sus escritorios al final de la jornada laboral. Los documentos impresos deben guardarse en lugares seguros.

- Política de pantalla limpia:

Las pantallas de los dispositivos deben bloquearse cuando los usuarios se ausenten de su puesto de trabajo. No debe dejarse información visible en pantalla que pueda ser vista por personas no autorizadas.

14. Protección de instalaciones y equipos compartidos

Los equipos y dispositivos compartidos deben ser utilizados de manera responsable y ser protegidos de accesos no autorizados. Se deben aplicar medidas de control de acceso para áreas restringidas dentro de las instalaciones de COMFICA.

15. Uso de Internet

El acceso a internet en los dispositivos de COMFICA debe ser usado exclusivamente para actividades laborales. Está prohibido visitar sitios web inseguros, inapropiados o que puedan comprometer la seguridad de los sistemas.

16. Correo electrónico y otros medios de comunicación

El correo electrónico corporativo debe ser utilizado de manera responsable. Los mensajes que contengan información confidencial deben ser cifrados. Está prohibido el uso de correos personales para asuntos laborales.
Se permite el uso de mensajería instantánea como Whatsapp para fines laborales y siempre desde líneas corporativas asignadas por el área de TI.

17. Derechos de autor

Todos los usuarios deben respetar las leyes de derechos de autor y propiedad intelectual. Está prohibido utilizar, copiar o distribuir software, música, videos o cualquier otro contenido protegido por derechos de autor sin la debida autorización.

18. Dispositivos móviles

Los dispositivos móviles permiten flexibilidad en el trabajo, pero también presentan riesgos de seguridad. La política de uso de dispositivos móviles establece las directrices para su uso seguro.

- Los dispositivos móviles deben estar protegidos con contraseñas robustas y medidas de seguridad como la autenticación multifactor.
- El acceso a información sensible desde dispositivos móviles debe realizarse a través de redes VPN o conexiones seguras.
- Los usuarios deben reportar inmediatamente la pérdida o robo de dispositivos a TI.

19. Teletrabajo (VPN)

Para acceder a la red corporativa desde ubicaciones remotas, los usuarios deben utilizar una conexión VPN aprobada por el área de TI. Todas las actividades realizadas bajo teletrabajo están sujetas a las políticas de uso aceptable.

20. Supervisión del uso de sistemas de información y comunicación

El uso de los sistemas de información de COMFICA será monitoreado de manera continua para detectar y prevenir actividades no autorizadas o peligrosas. Los registros de uso serán auditados periódicamente por el equipo de seguridad de la información.

21. Incidentes

Cualquier incidente de seguridad o violación de esta política debe ser reportado inmediatamente al área de TI y al equipo de seguridad de la información para su investigación y resolución. Las acciones correctivas serán tomadas para mitigar riesgos futuros.

22. Responsabilidades

- Colaboradores y contratistas: Responsables de cumplir con las políticas establecidas, mantener la seguridad de la información y reportar cualquier incidente o sospecha de violación de la política.
- Área de TI: Responsable de la implementación, supervisión y monitoreo de las políticas de uso aceptable, gestión de incidentes y protección de la infraestructura tecnológica.
- Gerencia: Responsable de aprobar y revisar las políticas, asegurando que se alineen con los objetivos y las normativas de COMFICA.

23. Revisión y aprobación

Este documento será revisado anualmente o cuando se considere necesario debido a cambios en los procesos, tecnologías o regulaciones. Las revisiones estarán a cargo del Departamento de TI y deberán ser aprobadas por la Gerencia General.