Política de Uso de Instrumentos Electrónicos

I. Objetivo:

El objetivo de esta política es establecer las normas y directrices para el uso adecuado de los instrumentos electrónicos proporcionados por FONDO COMPLEMENTARIO PREVISIONAL CERRADO FCPC DE JUBILACION Y CESANTIA BANECUADOR FCPC BANECUADOR a sus empleados, con el fin de asegurar la protección de la información, la eficiencia operativa y el cumplimiento de las regulaciones legales y corporativas.

II. Alcance:

Esta política se aplica a todos los empleados, contratistas, consultores, pasantes y cualquier otra persona que utilice instrumentos electrónicos proporcionados por FONDO COMPLEMENTARIO PREVISIONAL CERRADO FCPC DE JUBILACION Y CESANTIA BANECUADOR FCPC BANECUADOR, incluyendo, pero no limitado a, computadoras, teléfonos móviles, tablets, servidores, redes y cualquier otro dispositivo electrónico o sistema de información.

III. Uso Aceptable

1. Propósito Comercial y/o Laboral: Los instrumentos electrónicos deben ser utilizados principalmente para fines relacionados con las actividades comerciales de el fondo y el ejercicio de sus deberes laborales dentro de la FONDO COMPLEMENTARIO PREVISIONAL CERRADO FCPC DE JUBILACION Y CESANTIA BANECUADOR FCPC BANECUADOR.
2. Acceso Autorizado: Solo el personal autorizado puede acceder y utilizar los sistemas y dispositivos electrónicos de el fondo.
3. Protección de la Información: Los usuarios deben proteger la confidencialidad, integridad y disponibilidad de la información de el fondo, siguiendo las políticas y procedimientos de seguridad de la información establecidos.
4. Software Autorizado: Solo se debe instalar y utilizar software autorizado y licenciado. La instalación de software no autorizado está prohibida.

IV. Uso Inaceptable

1. Uso Personal Extensivo: El uso personal de los instrumentos electrónicos debe ser limitado y no interferir con las responsabilidades laborales.
2. Actividades Ilegales: Está prohibido utilizar los dispositivos electrónicos para actividades ilegales, incluyendo la descarga, distribución o visualización de contenido ilegal.
3. Contenido Ofensivo: Está prohibido el uso de los dispositivos electrónicos para crear, almacenar o distribuir contenido ofensivo, discriminatorio o que viole las políticas de el fondo.
4. Seguridad: No se deben deshabilitar o eludir los controles de seguridad implementados en los dispositivos o instrumentos electrónicos.

V. Correo Electrónico y Comunicaciones

1. Uso Adecuado: El correo electrónico corporativo debe ser utilizado para comunicaciones laborales. Los correos electrónicos personales deben ser utilizados con moderación y no deben interferir con las responsabilidades laborales
2. Privacidad: Aunque el fondo respeta la privacidad de sus empleados, se reserva el derecho de monitorear el uso del correo electrónico y otras comunicaciones para asegurar el cumplimiento de esta política
3. Phishing y Spam: Los usuarios deben ser cautelosos con los correos electrónicos sospechosos y no deben abrir enlaces o archivos adjuntos de fuentes no confiables.

VI. Uso de Internet

1. Acceso a Internet: El acceso a Internet debe ser utilizado principalmente para fines laborales. El acceso a sitios web no relacionados con el trabajo debe ser limitado y no debe interferir con las responsabilidades laborales.
2. Descargas: Las descargas de archivos de Internet deben ser limitadas a contenido relacionado con el trabajo y deben seguir las políticas de seguridad de el fondo.
3. Redes Sociales: El uso de redes sociales debe ser adecuado y no debe comprometer la imagen de el fondo o la confidencialidad de la información.

VII. Seguridad y Protección de Datos

1. Contraseñas: Los usuarios deben mantener la confidencialidad de sus contraseñas y no compartirlas con otros. Las contraseñas deben cumplir con los requisitos de complejidad establecidos por el fondo.
2. Encriptación: La información confidencial debe ser encriptada cuando se almacene o se transmita a través de redes no seguras.
3. Respaldo de Información: Los usuarios deben seguir las políticas de respaldo de información para asegurar que los datos críticos estén protegidos contra pérdida o daño.
4. Reportes de Incidentes: Cualquier incidente de seguridad o sospecha de violación de esta política debe ser reportado inmediatamente al departamento de TI o al Delegado de Protección de Datos.

VIII. Consecuencias del Incumplimiento

El incumplimiento de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del empleo, a través de su aplicación en el Reglamento Interno de Trabajo, así como en acciones legales en caso de violaciones graves debidamente tipificadas en el Código Orgánico Integral Penal.

IX. Revisión y Actualización

Esta política será revisada periódicamente y actualizada según sea necesario para asegurar su relevancia y efectividad. Cualquier cambio será comunicado a todos los empleados y usuarios de instrumentos electrónicos de FONDO COMPLEMENTARIO PREVISIONAL CERRADO FCPC DE JUBILACION Y CESANTIA BANECUADOR FCPC BANECUADOR.

X. Contacto

Para cualquier pregunta o aclaración sobre esta política, los empleados pueden contactar al departamento de TI o al Delegado de Protección de Datos a través del correo: info@fcpcbanecuador.com.ec

Fecha de emisión y publicación: 18 de marzo de 2025

FONDO COMPLEMENTARIO PREVISIONAL CERRADO FCPC DE JUBILACION Y CESANTIA BANECUADOR FCPC BANECUADOR

En pleno cumplimiento con la Ley Orgánica de Protección de Datos del Ecuador.