Política de Uso Aceptable de Recursos Tecnológicos de F-BridgeDigital

1. Propósito

Establecer los lineamientos de uso aceptable de los recursos tecnológicos de la organización, garantizando su uso seguro, eficiente y conforme a los requerimientos contractuales con terceros, como contratista.

2. Alcance

Esta política aplica a:

- Todo el personal interno (empleados, contratistas, pasantes).
- Terceros que brinden servicios relacionados con el contrato con el Banco.
- Todo uso de recursos tecnológicos, redes, dispositivos y plataformas provistos por **F-BridgeDigital.**

3. Requisitos de Uso Aceptable

a. Uso de Internet

- Está permitido solo para fines laborales.
- Se prohíbe el acceso a sitios con contenido ilegal, ofensivo, o no relacionado con las funciones del trabajo.
- Todo el tráfico web puede ser monitoreado y registrado.

b. Uso de Redes Sociales

- No se permite el uso de redes sociales para actividades personales durante horas laborales en equipos corporativos.
- El uso institucional debe estar aprobado por el área de comunicaciones o seguridad.
- Está prohibido divulgar información confidencial o relacionada con el Banco en redes sociales.

c. Uso del Correo Electrónico Corporativo

- Debe utilizarse exclusivamente para fines laborales.
- Está prohibido reenviar información confidencial a cuentas personales.

- El correo puede ser monitoreado por el área de seguridad de la información.

d. Uso de Mensajería Instantánea

- Solo se permite el uso de plataformas corporativas autorizadas (ej. Teams, Slack).
- No se permite el uso de WhatsApp u otras aplicaciones personales para compartir datos sensibles.
- Toda comunicación sensible debe realizarse por canales seguros.

e. Uso de Equipos Informáticos Facilitados por **F-BeridgeDigital**.

- El usuario es responsable del uso seguro del equipo asignado.
- No se debe instalar software sin autorización previa.
- Deben aplicarse parches, antivirus y configuraciones de seguridad provistas por TI.

f. Uso de Equipos Informáticos Personales (BYOD)

- Su uso requiere autorización previa del área de TI o Seguridad.
- Deben cumplir con los requisitos mínimos de seguridad: antivirus, cifrado y autenticación segura.
- Se podrá requerir instalación de herramientas MDM (gestión de dispositivos móviles).

g. Uso de Dispositivos de Almacenamiento Portátil o Extraíbles

- Solo se permite el uso de dispositivos cifrados y autorizados.
- Se debe realizar escaneo antivirus antes de cada uso.
- Está prohibido almacenar información confidencial del Banco sin protección adecuada.

h. Responsabilidades Relativas al Tratamiento de Activos de Información del Banco

- El personal debe proteger los activos de información del Banco conforme a los acuerdos de confidencialidad.
- Está prohibida la copia, transferencia o uso no autorizado de dicha información.
- Toda pérdida o incidente de seguridad debe reportarse inmediatamente al área correspondiente.

---

4. Formación y Comunicación

- Esta política será comunicada a todos los empleados y terceros antes del inicio de su relación contractual.
- Será parte del proceso de inducción y estará disponible en la intranet o medio oficial.

---

5. Supervisión y Cumplimiento

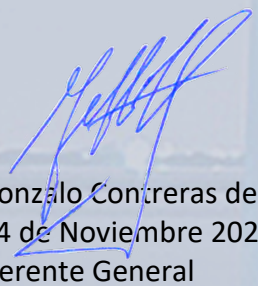
- La organización realizará auditorías y controles para verificar el cumplimiento.
- El incumplimiento podrá dar lugar a sanciones disciplinarias, despido o acciones legales según la gravedad.

---

6. Revisión

- Esta política será revisada anualmente o en caso de cambios tecnológicos, legales o contractuales.

La presente política será aprobada por la alta dirección de la empresa y se difundirá de manera clara a todos los empleados y colaboradores para asegurar su cumplimiento efectivo.



Firma: Gonzalo Contreras del Solar
Fecha: 14 de Noviembre 2024
Cargo: Gerente General