

2024

Banco País

6-6-2024

Política de Uso Aceptable

**Política de Uso Aceptable - Banco País**

**1. Descripción General**

La Política de Uso Aceptable del Banco País establece las normas y directrices para el uso adecuado de los recursos tecnológicos y la información de la empresa. Esta política está diseñada para proteger tanto a los empleados como a la organización frente a riesgos de seguridad, violaciones de la privacidad y otros problemas derivados del uso inadecuado de los sistemas informáticos.

**2. Propósito**

Los propósitos principales de esta política son:

* Asegurar el uso adecuado y responsable de los recursos tecnológicos del Banco País.
* Proteger la información confidencial y los activos tecnológicos de la empresa.
* Definir las actividades permitidas y prohibidas para los usuarios de los sistemas del Banco País.
* Promover la seguridad y la integridad de la red y los datos de la organización.

**3. Alcance**

Esta política se aplica a todos los empleados, contratistas, consultores, trabajadores temporales y otros trabajadores del Banco País, incluyendo todo el personal afiliado a terceros. Abarca todos los equipos, sistemas y datos propiedad del Banco País o que estén bajo su control.

**4. Política**

4.1 Uso General y Propiedad

4.4.1 Todos los datos creados o almacenados en los sistemas del Banco País son propiedad de la empresa.

4.4.2 Los usuarios deben entender que los datos y comunicaciones generados en el curso de sus labores pueden ser monitoreados y auditados.

4.4.3 Cada empleado es responsable de reportar a tiempo cualquier pérdida o robo de la información de Banco País.

4.4.4 El acceso a los recursos tecnológicos debe ser utilizado principalmente para propósitos relacionados con el trabajo.

4.4.5 Puede acceder, utilizar o compartir información patentada de la institución solo en la medida en que esté autorizado y sea necesario para cumplir con las tareas laborales asignadas.

4.4.6 Los dispositivos y sistemas proporcionados por el Banco País deben ser utilizados de manera ética y legal.

4.2 Seguridad e Información Propietaria

4.2.1 Los empleados deben proteger la información confidencial y propietaria del Banco País.

4.2.2 Las contraseñas deben ser complejas y mantenerse confidenciales. Queda prohibido el compartir credenciales con otros empleados o personas externas a la institución.

4.2.3 No se debe compartir información confidencial con personas no autorizadas, interna o externamente.

4.2.4 Se deben seguir todas las directrices y protocolos de seguridad establecidos por el Banco País.

4.2.5 Los empleados deben extremar las precauciones al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, que pueden contener malware.

**4.3 Uso Inaceptable**

Las siguientes actividades están, con carácter general, prohibidas. Los empleados pueden estar exentos de estas restricciones durante sus responsabilidades laborales legítimas (por ejemplo, el personal de administración de sistemas puede tener la necesidad de desactivar el acceso a la red de un host si ese host está interrumpiendo los servicios de producción).

En ninguna circunstancia un empleado de Banco País está autorizado a participar en ninguna actividad que sea ilegal según las leyes locales, estatales, federales o internacionales mientras utiliza recursos propiedad de Banco País.

Las listas siguientes no son en modo alguno exhaustivas, pero intentan proporcionar un marco para las actividades que entran en la categoría de uso inaceptable.

4.3.1 Actividades del Sistema y de la Red

No se debe interferir con el funcionamiento de la red del Banco País.

Está prohibido el acceso no autorizado a sistemas, redes o datos.

No se deben instalar ni utilizar software no autorizado o pirata. La instalación y manejo de Software licenciado se realizará por medio del Departamento de Sistemas y Tecnologia.

No se deben realizar actividades de hacking o pruebas de penetración sin autorización expresa.

4.3.2 Actividades de Correo Electrónico y Comunicación

No se debe utilizar el correo electrónico de la empresa para enviar spam o mensajes no solicitados.

No se deben enviar correos electrónicos con contenido ofensivo, difamatorio o ilegal.

El correo electrónico corporativo debe ser utilizado únicamente para fines laborales.

Uso no autorizado o falsificación de la información del encabezado del correo electrónico.

Crear o reenviar "cartas en cadena", "Ponzi" u otros esquemas "piramidales" de cualquier tipo.

4.3.3 Blogging y Redes Sociales

Los empleados deben ser conscientes de que sus actividades en redes sociales pueden reflejarse en la reputación del Banco País.

No se debe divulgar información confidencial o propietaria del Banco País en blogs o redes sociales.

Las opiniones expresadas en blogs o redes sociales deben ser personales y no representar la posición del Banco País.

**5. Cumplimiento de la Política**

El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del empleo y posibles acciones legales. Todos los empleados deben informar cualquier violación de esta política a su supervisor o al departamento de TI.

5.1 Medición de cumplimiento

El equipo de Departamento de Seguridad de la Información verificará el cumplimiento de esta política a través de varios métodos, incluidos, entre otros, informes de herramientas comerciales, auditorías internas y externas y comentarios al propietario de la política.

5.2 Excepciones

Cualquier excepción a la política debe ser aprobada previamente por el equipo de Departamento de Seguridad de la Información.

5.3 Incumplimiento

Un empleado que haya violado esta política puede estar sujeto a medidas disciplinarias, que pueden incluir el despido.

**6. Estándares, Políticas y Procesos Relacionados**

Esta política está relacionada con los siguientes documentos:

* Política de Seguridad de la Información del Banco País.
* Procedimientos de Gestión de Incidentes de Seguridad.
* Manual del Empleado del Banco País.

**7. Definiciones y Términos (Definitions and Terms)**

PII (Personally Identifiable Information): Información que puede ser utilizada para identificar a una persona, como nombres, direcciones, números de teléfono, etc.

Información propietaria: Información que pertenece exclusivamente al Banco País y no debe ser divulgada sin autorización.

Redes Sociales: Plataformas de comunicación en línea como Facebook, Twitter, LinkedIn, etc.

Pentest: Abreviatura de "penetration test" o prueba de penetración, es una evaluación de seguridad que simula un ataque real a un sistema informático, red o aplicación para identificar y explotar vulnerabilidades. El objetivo de un pentest es descubrir las debilidades de seguridad antes de que puedan ser aprovechadas por atacantes malintencionados.

**8. Historial de Revisión**

|  |  |  |  |
| --- | --- | --- | --- |
| **Fecha de cambio** | **Responsable** | **Resumen de cambios** | **Versión** |
| **8 de Julio de 2023** | Dirección de planificación y desarrollo | Mejoras en el alcance | 1.0 |
| **6 Junio 2024** | Dirección de planificación y desarrollo | Agregado estándares, políticas y procesos relacionados | 1.1 |

Esta Política de Uso Aceptable será revisada periódicamente y actualizada conforme a los cambios tecnológicos y organizativos.