Política de Protección de Datos y Seguridad de la Información de F-Bridge Digital

1. Objetivo de la Política

El objetivo de esta política es establecer un conjunto de directrices y prácticas para proteger los datos personales, la información sensible y garantizar la seguridad de la información en todas las operaciones realizadas por la empresa. Esto incluye proteger los sistemas, redes y aplicaciones informáticas de posibles accesos no autorizados, divulgación, alteración o destrucción de datos.

2. Alcance

Esta política se aplica a todos los empleados, contratistas, proveedores y cualquier persona que tenga acceso a los sistemas de información de la empresa. Incluye también la protección de datos de clientes, proveedores, empleados y otros actores relevantes, conforme a la legislación vigente en Chile.

3. Marco Legal y Normativo

La empresa se compromete a cumplir con la legislación nacional e internacional en materia de protección de datos personales y seguridad de la información, incluyendo:

- **Ley N° 19.496** sobre Protección de los Derechos de los Consumidores.
- **Ley N° 20.584** sobre los Derechos y Deberes de los Pacientes (cuando aplique).
- **Ley N° 19.223** sobre delitos informáticos.
- **Ley N° 21.096** sobre Protección de Datos Personales y su reglamentación (cuando entre en vigor).
- **Reglamento General de Protección de Datos (GDPR)** de la Unión Europea, cuando los datos sean procesados de manera transnacional.

4. Principios de Protección de Datos y Seguridad de la Información

La empresa adoptará los siguientes principios fundamentales en el tratamiento de datos personales y la gestión de la seguridad de la información:

- **Confidencialidad:** Garantizar que los datos solo sean accesibles a quienes estén autorizados.
- **Integridad:** Asegurar que los datos sean exactos, completos y actualizados.
- **Disponibilidad:** Asegurar que los datos sean accesibles y utilizables cuando sean necesarios.

- **Responsabilidad:** Los responsables del tratamiento de los datos deben ser claros y estar definidos en todo momento.
- **Minimización de Datos:** Recoger únicamente los datos necesarios para cumplir con la finalidad de su tratamiento.

5. Responsabilidades de los Empleados

Todos los empleados y contratistas deberán cumplir con las siguientes responsabilidades en materia de protección de datos y seguridad de la información:

- **Acceso Restringido:** Acceder únicamente a los datos que sean necesarios para el cumplimiento de sus funciones laborales.
- **Protección de Contraseñas:** Utilizar contraseñas seguras y cambiarlas regularmente.
- **Cifrado de Información Sensible:** Asegurar que los datos sensibles estén cifrados tanto en reposo como en tránsito.
- **Uso Responsable de Dispositivos:** Asegurar la correcta utilización de los dispositivos corporativos y protegerlos contra pérdida o robo.
- **Notificación de Incidentes de Seguridad:** Informar inmediatamente a los responsables de seguridad de la empresa sobre cualquier incidente de seguridad o sospecha de violación de datos.

6. Medidas Técnicas y Organizativas de Seguridad

La empresa implementará las siguientes medidas de seguridad para proteger los sistemas y datos:

- **Control de Acceso:** Implementar sistemas de autenticación robustos, como autenticación multifactor (MFA), y garantizar que los usuarios solo tengan acceso a la información necesaria para su trabajo.
- **Cifrado de Datos:** Cifrar la información sensible tanto en reposo como en tránsito para evitar accesos no autorizados.
- **Auditorías y Monitoreo:** Realizar auditorías periódicas y monitoreo continuo de los sistemas para identificar posibles vulnerabilidades o brechas de seguridad.
- **Backup y Recuperación de Datos:** Realizar copias de seguridad periódicas de la información y contar con procedimientos claros de recuperación ante desastres.
- **Protección contra Malware:** Utilizar soluciones antivirus, cortafuegos (firewalls) y sistemas de detección y prevención de intrusiones (IDS/IPS).
- **Actualizaciones de Seguridad:** Mantener todos los sistemas operativos, aplicaciones y dispositivos actualizados con los últimos parches de seguridad.

7. Protección de Datos Personales

La empresa garantiza que los datos personales de clientes, empleados y terceros serán tratados de acuerdo con las siguientes directrices:

- **Consentimiento:** Solicitar el consentimiento explícito y previo de los titulares de los datos personales para su tratamiento, cuando corresponda.
- **Finalidad Limitada:** Recoger y tratar los datos personales solo con fines legítimos y específicos, informando adecuadamente a los titulares sobre la finalidad de la recolección de datos.
- **Derechos de los Titulares:** Garantizar que los titulares de los datos puedan ejercer sus derechos de acceso, rectificación, cancelación y oposición (ARCO), según corresponda.
- **Transferencias Internacionales:** Si se realizáran transferencias internacionales de datos personales, se tomarán las medidas necesarias para garantizar que los datos reciban un nivel adecuado de protección, conforme a las leyes aplicables.

8. Gestión de Incidentes de Seguridad

La empresa tiene un protocolo establecido para la gestión de incidentes de seguridad, que incluye:

- **Detección:** Implementar mecanismos de monitoreo para la detección temprana de incidentes de seguridad.
- **Notificación:** Notificar inmediatamente a los responsables de seguridad de la empresa sobre cualquier incidente relevante.
- **Respuesta y Mitigación:** Tomar medidas inmediatas para mitigar los efectos de un incidente de seguridad y evitar su propagación.
- **Investigación:** Realizar una investigación exhaustiva para identificar las causas y efectos del incidente, y adoptar medidas correctivas.
- **Notificación a Autoridades:** Si se determina que ha habido una violación de datos personales, se notificará a la autoridad competente y a los titulares de los datos según lo exijan las normativas aplicables.

Respuesta a Incidentes que Afectan al Banco o cliente

F-BridgeDigital cuenta con un proceso formal y documentado para responder de manera **rápida y eficaz** ante incidentes de ciberseguridad que pudiesen afectar los **activos de información o los servicios utilizados por el Banco**.

Este proceso incluye:

- **Notificación inmediata al Banco** ante cualquier incidente relevante.
- **Clasificación prioritaria** para incidentes que involucren datos o sistemas del Banco.
- **Comunicación inicial dentro de las primeras 2 horas** tras la detección del incidente.
- **Coordinación de acciones** con los equipos de seguridad del Banco.
- **Reporte post incidente** con análisis de causa raíz, impacto y medidas correctivas, dentro de los 5 días hábiles.

El personal involucrado será capacitado para la correcta atención de este tipo de eventos críticos, y se mantendrá un canal de contacto activo 24/7 para la atención inmediata de emergencias.

9. Simulación de Amenazas y *Pruebas de Penetración* (Pentesting)

F-BridgeDigital realizará simulaciones periódicas de amenazas y pruebas de penetración (pentesting) sobre sus aplicaciones y la infraestructura tecnológica involucradas en la prestación de servicios al Banco y a otros clientes estratégicos. Estas actividades serán ejecutadas por proveedores de seguridad calificados y con experiencia en el sector financiero.

- Las pruebas tendrán como objetivo identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.
- Se documentarán los hallazgos y se establecerán planes de acción para su remediación.
- Los informes resultantes serán revisados por el área de ciberseguridad y, cuando corresponda, compartidos con clientes bajo acuerdos contractuales de confidencialidad.

Estas prácticas formarán parte del ciclo de mejora continua en la protección de la confidencialidad, integridad y disponibilidad de las plataformas tecnológicas de F-BridgeDigital.

---

10. Gestión de Cambios y Parchado de Seguridad

F-BridgeDigital cuenta con un proceso formalizado de gestión de cambios que aplica a toda su infraestructura tecnológica, tanto de software como de hardware. Este proceso asegura que los cambios:

- Sean planificados, evaluados, aprobados y documentados antes de su implementación.
- Incluyan la aplicación oportuna de parches de seguridad y actualizaciones críticas.
- No introduzcan riesgos inaceptables para la continuidad de los servicios ni para la seguridad de los activos tecnológicos.

Se mantiene un control estricto sobre la instalación de parches, asegurando que los sistemas estén protegidos contra vulnerabilidades conocidas. Además, se aplica una estrategia de evaluación de riesgos que permite:

- Identificar impactos potenciales antes del cambio.
- Mitigar riesgos derivados de actualizaciones mal ejecutadas.
- Validar la efectividad de los parches una vez aplicados.

Este proceso está alineado con las mejores prácticas del sector y con los estándares de seguridad exigidos por la industria financiera.

11. Formación y Concientización

La empresa proporcionará formación periódica a todos sus empleados sobre la importancia de la protección de datos personales y la seguridad de la información. Esta formación incluirá:

- Políticas de seguridad de la información.

- Buenas prácticas en el manejo de datos personales.
- Procedimientos de respuesta ante incidentes de seguridad.
- Uso adecuado de contraseñas y medidas de autenticación.

12. Computación en la nube

En caso de que la empresa utilice la nube para ofrecer servicios críticos o estratégicos al Banco, se asegura que los proveedores de servicios en la nube con los cuales se externalicen dichos servicios cumplan con los siguientes requisitos de seguridad, conforme a la normativa RAN 20-7 sobre la externalización de servicios:

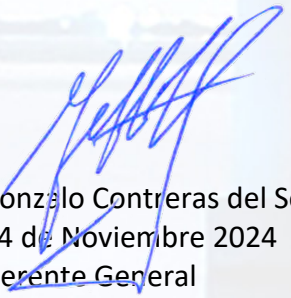
- **Certificaciones Internacionales:** El proveedor de servicios en la nube debe contar con **certificaciones de seguridad** reconocidas internacionalmente, tales como ISO 27001, SOC 2, o cualquier otra certificación aplicable que demuestre un compromiso con la seguridad de la información y continuidad de negocio.
- **Reputación y Experiencia:** El proveedor de servicios en la nube debe contar con **experiencia comprobada** y un **reconocido prestigio** en la provisión de servicios en la nube, específicamente en el ámbito de la ciberseguridad y la protección de datos.
- **Contratos de Externalización:** Los contratos de externalización de servicios serán celebrados directamente entre la empresa y el proveedor de servicios en la nube, asegurando que los términos de seguridad y confidencialidad sean claramente especificados y cumplidos.
- **Controles de Seguridad en la Nube:** El proveedor de la nube debe implementar **controles físicos y lógicos**adecuados que aseguren el aislamiento de los componentes de la infraestructura de nube compartida, de manera que se prevengan fugas de información o cualquier evento que pueda comprometer la confidencialidad, integridad o disponibilidad de los datos del Banco.
- **Protección de la Información en la Nube:** Los sistemas de nube utilizados para prestar servicios al Banco deberán cumplir con controles proporcionales al perfil de riesgo y la criticidad de la información. Esto incluye, pero no se limita a, el uso de **cifrado** de los datos en tránsito y en reposo, autenticación robusta y medidas de protección ante vulnerabilidades.
- **Auditoría y Cumplimiento:** La empresa realizará **auditorías periódicas** a los proveedores de servicios en la nube, asegurando que se mantengan los estándares de seguridad adecuados y que se tomen las acciones necesarias para abordar cualquier vulnerabilidad o brecha de seguridad detectada.

13. Revisión y Actualización de la Política

Esta política será revisada y actualizada anualmente o cuando haya cambios relevantes en la legislación aplicable o en las prácticas de seguridad de la información. Los cambios serán comunicados a todos los empleados y contratistas de la empresa.

Aprobación de la Política

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