Política de Gestión de Activos Tecnológicos de F-BridgeDigital

1. Propósito

El propósito de esta política es establecer los lineamientos para la **gestión, protección, administración y destrucción segura** de los activos tecnológicos e informáticos de **F-BridgeDigital**, incluyendo información sensible y elementos criptográficos, en cumplimiento con los estándares de seguridad, normativas regulatorias vigentes y los compromisos contractuales asumidos con clientes como el Banco.

2. Alcance

Esta política aplica a:

- Todos los **activos tecnológicos e informáticos**, tanto físicos como lógicos, gestionados por F-BridgeDigital.
- Todo el **software, llaves criptográficas, módulos criptográficos y datos asociados** a la prestación de servicios tecnológicos al Banco u otras entidades reguladas.

3. Requisitos de Gestión de Activos

a. Gestión de Software

- Mantenemos una política de **gestión de software** actualizada anualmente.
- Gestionaremos todo el ciclo de vida del software: adquisición, instalación, configuración, actualización y control de versiones, con foco en su seguridad y legalidad.
- Todo el software utilizado deberá ser **homologado, licenciado y validado por el área de TI y Seguridad de la Información**.

b. Intercambio de Llaves Criptográficas

- Contamos con **procedimientos documentados y controlados** para el intercambio seguro de llaves criptográficas con clientes, incluyendo el Banco.
- Se definen roles y responsabilidades, y se registra toda transacción de intercambio de llaves.
- Este proceso se realiza exclusivamente en **entornos seguros y bajo estrictos controles de acceso**.

c. Inventario de Activos Informáticos

- Mantendremos un **inventario detallado y actualizado** de todos los activos informáticos asignados a la prestación de servicios por cliente.
- Este inventario será**auditado periódicamente** y contempla:
    - Activos en operación
    - Activos en baja o reemplazo
    - Componentes críticos de respaldo
- Se aplicarán procedimientos formales para la **desincorporación y destrucción segura** de activos, incluyendo el borrado seguro de información.

d. Administración de Módulos Criptográficos

- Existirán procedimientos definidos para la administración segura de **módulos criptográficos** utilizados en nuestra infraestructura.
- Se asegurará la configuración segura, actualización de firmware, y control de acceso a estos dispositivos conforme a mejores prácticas del sector.

e. Destrucción y Eliminación Segura de Activos

- La destrucción de activos, tanto físicos como electrónicos, se realizará conforme a **protocolos internos documentados**, considerando la clasificación de la información contenida.
- Toda eliminación de información confidencial se efectuará al término de la relación contractual, con supervisión de personal autorizado.
- Se asegurará que los medios destruidos sean **ilegibles e irrecuperables**, y se genera evidencia de su eliminación cuando sea requerido.

4. Responsabilidades

- **Gestión de Activos:** El área de Tecnología y Seguridad de la Información será responsable de mantener el inventario, aplicar controles de seguridad y asegurar el cumplimiento de esta política.
- **Criptografía:** El equipo responsable de Seguridad gestionará los procesos de intercambio y administración de llaves y módulos criptográficos.
- **Evidencia de Cumplimiento:** Toda la documentación y evidencia de cumplimiento estará disponible para auditorías internas o externas y será compartida con el Banco o entidades regulatorias cuando sea requerido.

5. Cumplimiento y Auditoría

- Esta política es de cumplimiento obligatorio para todas las unidades y colaboradores de F-BridgeDigital que administren activos informáticos.
- Se realizarán **auditorías periódicas**, internas y externas, para verificar el cumplimiento.
- El incumplimiento puede derivar en sanciones administrativas o contractuales, según la criticidad del hallazgo y la normativa vigente.

6. Gestión de Incidentes Relacionados con Activos Tecnológicos

6.1 Propósito

Establecer los lineamientos para la identificación, tratamiento y mitigación de incidentes de seguridad que afecten los activos tecnológicos de F-BridgeDigital, garantizando la continuidad de los servicios al Banco y la protección de la información.

6.2 Identificación y Mitigación de Vulnerabilidades

F-BridgeDigital contará con procedimientos establecidos para la identificación oportuna de vulnerabilidades explotadas durante un incidente de seguridad, así como su mitigación, sin comprometer las actividades de investigación ni las acciones de respuesta ante incidentes.

- Se realizará un análisis técnico para determinar el alcance y la naturaleza del incidente.
- Se evaluarán los activos afectados y se aplican medidas de contención y corrección de acuerdo con el impacto identificado.
- Las evidencias relevantes del incidente se protegerán y documentarán para su análisis forense, manteniendo la trazabilidad.

6.3 Planes de Acción y Gestión de Riesgos

F-BridgeDigital implementará planes de acción específicos para cada incidente de seguridad, incluyendo las siguientes actividades:

- Identificación de causas raíz.
- Asignación de responsables y plazos para la ejecución de medidas correctivas.
- Seguimiento del cumplimiento de las acciones definidas.
- Revisión de controles existentes y actualización de procedimientos si es necesario.

Estos planes formarán parte del proceso continuo de gestión de riesgos de seguridad de la información y se documentarán para auditoría y mejora continua.

6.4 Plan de Reparación

En caso de incidentes de ciberseguridad, se activará un plan de reparación que incluye:

- Acciones correctivas técnicas, operativas o administrativas.
- Designación de responsables para cada actividad de reparación.
- Revisión de la efectividad de las acciones tomadas.
- Documentación del incidente, incluyendo la causa, impacto, acciones realizadas y lecciones aprendidas.

6.5 Coordinación con el Banco

Cuando el incidente afecta servicios o activos relacionados con el Banco, se activará el protocolo de notificación y coordinación, asegurando:

- La comunicación oportuna al punto de contacto designado por el Banco.
- La entrega de informes preliminares y finales sobre el incidente.
- La cooperación en auditorías o revisiones solicitadas por el Banco.

6.6 Capacitación y Concientización

F-BridgeDigital impartirá capacitación periódica a su personal técnico y administrativo sobre:

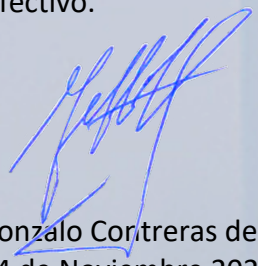
- Detección de incidentes.
- Procedimientos de reporte interno.
- Acciones preventivas y correctivas.

6.7 Auditoría y Mejora Continua

Los incidentes gestionados serán revisados periódicamente como parte de auditorías internas o externas. Esta revisión alimentará el proceso de mejora continua de la seguridad de los activos tecnológicos.

7. Revisión de la Política

- Esta política será revisada anualmente y actualizada conforme a cambios regulatorios, tecnológicos o contractuales, para asegurar que se mantenga alineada con las mejores prácticas y las exigencias del Banco.
- 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