Política de Gestión de Cambios y Parchado de Seguridad

de F-BridgeDigital

Objetivo:
Establecer las directrices para gestionar de forma segura los cambios tecnológicos y garantizar la aplicación oportuna de actualizaciones y parches de seguridad, con el fin de preservar la integridad, disponibilidad y confidencialidad de los sistemas utilizados en la prestación de servicios al Banco.

Alcance:
Esta política aplica a todos los sistemas, plataformas, aplicaciones, infraestructuras tecnológicas y servicios gestionados por F-BridgeDigital que formen parte del entorno de servicios prestados al Banco.

Lineamientos Generales:

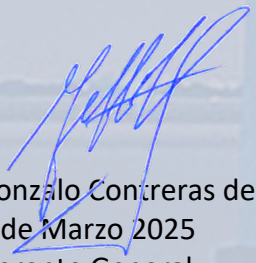
1. F-BRidgeDigital contará con un **proceso formal de gestión de cambios**, mediante el cual todos los cambios en software, hardware o configuraciones de sistemas son:
    - Planificados y documentados.
    - Evaluados desde la perspectiva de riesgos de ciberseguridad.
    - Aprobados previamente por los responsables designados.
    - Probados en ambientes controlados antes de su implementación en producción.
2. El proceso de gestión de cambios **incluirá la aplicación regular de parches de seguridad y actualizaciones críticas**, de acuerdo con:
    - Las mejores prácticas de la industria.
    - Las recomendaciones de los fabricantes o proveedores tecnológicos.
    - La criticidad del sistema y su exposición a amenazas.
3. Se mantendrá un **registro detallado de todos los cambios aplicados**, incluyendo fechas, responsables, sistemas afectados y resultados de las validaciones posteriores a la implementación.
4. Se establecerá un **control estricto sobre la instalación y aplicación de parches**, asegurando que:
    - No existan vulnerabilidades conocidas sin atender en los sistemas en producción.
    - Los parches de seguridad sean evaluados previamente respecto a su impacto funcional y operacional.
    - Se ejecuten procedimientos de reversión en caso de fallo.
5. Los cambios que puedan impactar servicios relacionados con el Banco deberán ser gestionados con especial atención, aplicando criterios de:
    - Evaluación de impacto en la disponibilidad y seguridad.

- Coordinación con las áreas responsables del servicio.
- Notificación oportuna cuando corresponda.

Revisión y Cumplimiento

- Esta política se revisa anualmente o cuando ocurren cambios en la infraestructura, amenazas emergentes o requisitos contractuales.
- El incumplimiento de estas disposiciones puede derivar en sanciones internas o contractuales según corresponda.
- Se ejecutan auditorías internas y externas que validan la efectividad de estas medidas y su alineación con los acuerdos con el 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: 3 de Marzo 2025
Cargo: Gerente General