Política de Perímetro de Defensa y Seguridad de Redes de F-BridgeDigital

1. Propósito

Esta política tiene como propósito establecer los lineamientos de **F-BridgeDigital** para la **protección, segmentación y monitoreo del perímetro de red**, asegurando que todo el tráfico, especialmente aquel relacionado con el servicio al Banco, se mantenga seguro, controlado y conforme a los estándares y normativas de ciberseguridad vigentes. Esto incluye la gestión de conexiones externas, la segmentación de red y el uso de dispositivos de seguridad como firewalls, IPS y WAF.

2. Alcance

Esta política aplica a toda la infraestructura de red, plataformas tecnológicas y servicios de conectividad gestionados por **F-BridgeDigital**, utilizados para la prestación de servicios a clientes críticos, incluyendo el Banco, abarcando redes internas, externas y conexiones de terceros.

3. Requisitos de Perímetro de Defensa

a. Diseño de Red con Zonas de Seguridad

- **F-BridgeDigital** mantendrá un diseño de red segmentado por zonas según la criticidad del servicio y la exposición al riesgo.
- Estas zonas incluirán: zonas de alto riesgo (DMZ, acceso a Internet), zonas internas protegidas, y zonas críticas (bases de datos, backend, sistemas confidenciales).
- El diseño estará orientado a limitar la superficie de ataque y aislar los activos más sensibles frente a accesos no autorizados.

b. Gestión de Conexiones de Red Externas

- Se mantiendrá un **inventario actualizado** de todas las conexiones externas, incluyendo IPs, puertos abiertos y servicios expuestos.
- Se registrará y auditará la **transferencia de datos entre F-BridgeDigital y el Banco**, con una retención mínima de 6 meses para fines de trazabilidad y auditoría.

c. Zonas Desmilitarizadas (DMZ)

- Los servicios públicos (ej. servidores web, correo, APIs expuestas) se alojarán exclusivamente en zonas DMZ, separadas de la red interna.

- Estas zonas estarán protegidas mediante **firewalls, IPS y controles específicos** para evitar accesos no autorizados a la red interna.

d. Protección del Tráfico de Red

- Se emplearán tecnologías especializadas para proteger el tráfico de red:
    - **Firewalls**, para filtrar tráfico entrante/saliente.
    - **Sistemas de Prevención de Intrusos (IPS)**, que monitorean y bloquean ataques en tiempo real.
    - **Firewalls de Aplicación Web (WAF)**, para proteger aplicaciones web de ataques como inyecciones de código o XSS.
- Todos estos dispositivos serán configurados, mantenidos y actualizados regularmente, conforme a políticas internas de seguridad.

4. Responsabilidades

- **Diseño de Red y Segmentación:** Nuestro equipo de infraestructura será responsable de mantener una red segmentada, basada en principios de seguridad por diseño.
- **Conexiones Externas:** Mantendremos documentación actualizada sobre todas las conexiones y flujos de datos hacia y desde el Banco.
- **Gestión de Seguridad Perimetral:** Se asignarán responsables para la operación y mantenimiento de dispositivos de seguridad como firewalls, IPS y WAF.
- **Cumplimiento y Evidencias:** F-BridgeDigital se comprometerá a conservar evidencia documentada sobre la implementación y efectividad de estos controles para auditorías.

5. Cumplimiento y Auditoría

- Esta política es de cumplimiento obligatorio para todas las áreas técnicas involucradas en la operación de redes y servicios al Banco.
- Su cumplimiento será evaluado mediante **auditorías internas periódicas**, y estamos preparados para **auditorías externas** que el Banco o entes reguladores soliciten.
- Cualquier desviación será tratada conforme a nuestro procedimiento interno de gestión de incidentes y no conformidades.

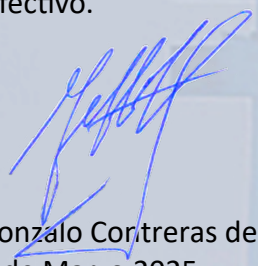
6. Gestión de Cambios y Parchado de Seguridad

- **F-BridgeDigital** mantendrá un proceso formal de **gestión de cambios** que asegure que toda modificación en la infraestructura tecnológica (software o hardware) esté planificada, aprobada y documentada.
- Este proceso incluirá la evaluación del impacto en la seguridad y la continuidad del servicio.
- Se aplicará una **estrategia de parchado y actualizaciones de seguridad**, que incluye:
    - Instalación de parches críticos en cuanto estén disponibles.
    - Evaluación del riesgo antes de la implementación.
    - Validación post-implementación para confirmar que no se introdujeron nuevas vulnerabilidades.

- Todo el proceso es controlado y auditado por el equipo de Seguridad de la Información.

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: 3 de Marzo 2025
Cargo: Gerente General