Política de Monitoreo, Detección de Amenazas y Seguridad en Infraestructura

de F-BridgeDigital

1. Propósito

Establecer los lineamientos y controles para la detección oportuna de ciberataques (incluidos DoS/DDoS), la protección contra software malicioso, la recolección y conservación de evidencias de seguridad, así como la implementación de medidas preventivas y reactivas sobre los dispositivos de la infraestructura tecnológica.

---

2. Alcance

Esta política aplica a:

- Todos los activos tecnológicos, redes, servidores, endpoints y plataformas gestionadas por F-BridgeDigital.
- Toda la infraestructura crítica usada para prestar servicios al Banco.
- Todo el personal que utilice, administre o tenga acceso a recursos tecnológicos gestionados por **F-BridgeDigital**.

---

3. Protección Contra Ataques de Denegación de Servicio (DoS/DDoS)

- Se implementarán soluciones dedicadas (Firewall perimetral, IPS/IDS, WAF, o servicios anti-DDoS) para detectar y mitigar ataques de denegación de servicios.
- Se realizarán pruebas periódicas para validar la capacidad de respuesta ante ataques volumétricos o de agotamiento de recursos.
- Las configuraciones estarán orientadas a preservar la **disponibilidad de los servicios acordados** contractualmente con el Banco.

---

4. Monitoreo de Seguridad y Registro de Eventos

a. Monitoreo 24/7

- La infraestructura tecnológica será monitoreada 24/7 por personal o servicios especializados en ciberseguridad.
- Se detectarán en tiempo real incidentes como caídas de servicio, accesos no autorizados, movimientos laterales o escaneos sospechosos.

b. Correlación de Eventos

- Se recabarán logs y eventos desde múltiples fuentes (firewalls, EDR, servidores, aplicaciones, redes) y se correlacionarán mediante SIEM (Security Information and Event Management).
- Las alertas se generarán automáticamente ante patrones de comportamiento anómalos o signos de ataque.

c. Sincronización Horaria

- Todos los sistemas de procesamiento de información y seguridad estarán sincronizados utilizando protocolos estándar como **NTP/SNTP/PTP**.
- Esta sincronización permitirá una adecuada trazabilidad y análisis forense en caso de incidentes.

d. Conservación y Protección de Registros

- Los registros de eventos se **centralizarán y protegerán contra alteraciones o accesos no autorizados**.
- Se retendrá por un mínimo de **6 meses operativamente** y se **almacenan durante 12 meses para fines legales y contractuales**.
- Se aplicarán mecanismos de cifrado y control de acceso sobre los repositorios de logs.

---

5. Protección Contra Código Malicioso

- Todos los equipos, servidores y endpoints contarán con soluciones **antimalware y antivirus actualizadas**.
- Se incluirán capacidades de detección frente a:
    - Virus, troyanos, spyware, ransomware, keyloggers y amenazas basadas en scripts.
- Las soluciones antimalware estarán integradas con el SIEM para alertar incidentes en tiempo real.
- Se actualizarán las firmas diariamente o bajo política automática del fabricante.

---

6. Seguridad en Dispositivos de Usuario Final (Endpoints)

a. Políticas Técnicas en los Dispositivos

- Se deshabilitarán servicios, puertos y aplicaciones innecesarias para **reducir la superficie de ataque**.
- Todos los dispositivos:
    - Tendrán **firewall local activo y configurado**.
    - Contarán con parches de sistema y aplicaciones actualizados regularmente.
    - Poseerán herramientas antimalware activas y administradas.
    - Dispondrán de control de ejecución de aplicaciones autorizadas.

b. Reglas de Uso para el Personal

- Estará prohibido deshabilitar mecanismos de protección instalados (antivirus, firewall, restricciones administrativas).
- El personal deberá:
    - Cerrar sesiones cuando no las use activamente.
    - Usar solo software homologado, con licencia válida y controlado por TI.
    - Apagar los equipos de forma controlada al finalizar la jornada (salvo excepciones autorizadas).
    - No intentar escalar privilegios ni alterar componentes críticos del sistema.
- Se aplicarán controles para forzar la instalación automática de actualizaciones de seguridad y firmas de antivirus.

Asimismo, F-BridgeDigital asegurará que todos los endpoints utilicen únicamente versiones de software y sistemas operativos con soporte oficial vigente. El área de TI gestionará la instalación automática de parches y actualizaciones de firmas de antivirus conforme a las políticas internas y a los requerimientos específicos del Banco cuando corresponda. Estas medidas están diseñadas para minimizar los vectores de ataque y garantizar la continuidad y seguridad de los servicios prestados.

---

7. Gestión de Configuraciones y Actualizaciones Tecnológicas

a. Respaldo de Configuraciones Críticas

F-BridgeDigital mantendrá mecanismos de respaldo periódico de la configuración de su infraestructura tecnológica, incluyendo dispositivos de red, servidores, herramientas de ciberseguridad y otros activos críticos. Estos respaldos aseguran la recuperación operativa ante incidentes y son almacenados en entornos protegidos.

b. Planificación de Capacidad

Se contará con un proceso documentado de revisión periódica de la capacidad de la infraestructura tecnológica y de seguridad, con el fin de anticipar necesidades de crecimiento, evitar saturaciones y garantizar la disponibilidad de los servicios prestados al Banco.

c. Revisión y Actualización de Software Base y Firmware

F-BridgeDigital aplicará una política de actualización periódica y gestión de versiones de:

- Sistemas operativos.
- Bases de datos y middleware.
- Firmware de dispositivos de red, almacenamiento y seguridad (por ejemplo, switches, firewalls, appliances SAN).

Las actualizaciones serán validadas previamente y ejecutadas siguiendo los lineamientos del proceso de gestión de cambios.

d. Seguridad Aplicada a Endpoints

Como parte de la política de seguridad en dispositivos finales, F-BridgeDigital aplicará las siguientes medidas para reducir brechas de seguridad:

- Desactivación de servicios, software y puertos no necesarios en los endpoints.
- Mantenimiento activo de soporte técnico oficial para versiones de sistemas operativos y software instalado.
- Aplicación regular de parches de seguridad para sistemas operativos y aplicaciones.
- Implementación de soluciones antimalware administradas y firewall personal configurado.
- Controles de ejecución restringida de software no autorizado.

e. Reglas de Uso Obligatorias para el Personal

El personal interno y externo de F-BridgeDigital que accede a activos tecnológicos deberá cumplir con las siguientes reglas:

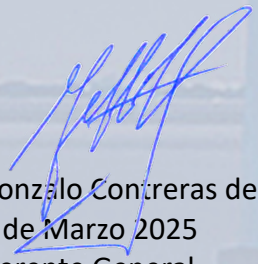
- Finalizar sus sesiones cuando no estén en uso.
- No modificar ni desactivar las soluciones de protección instaladas (antivirus, cortafuegos, etc.).
- Utilizar únicamente software homologado, licenciado y provisto por el área de TI.
- Apagar el equipo al finalizar la jornada laboral, salvo excepciones justificadas.

- No intentar escalar privilegios, alterar componentes del sistema, ni eliminar mecanismos de seguridad.
- Facilitar la instalación de parches y actualizaciones de firmas antivirus según los lineamientos internos y del Banco.

8. 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