Plan Anual de Pruebas de Contingencia y Comunicación ante Incidentes Críticos

de F-BridgeDigital

1. Objetivo

Establecer un marco de pruebas anuales que verifique la capacidad operativa de F-BridgeDigital para responder a incidentes críticos que puedan afectar la continuidad de los servicios prestados, incluyendo eventos de ciberseguridad, ausencia masiva de personal e interrupciones en la infraestructura crítica. El documento también define los protocolos de comunicación a seguir durante y después de tales eventos.

---

2. Alcance

Este plan aplica a:

- Todos los procesos críticos de la organización.
- Personal clave de operaciones, seguridad, soporte técnico y gestión de servicios.
- Infraestructura tecnológica y operativa que sustenta los servicios prestados al Banco y otros clientes.

---

3. Categorías de Incidentes Críticos

3.1. Incidentes de Ciberseguridad

Ataques de ransomware, filtración de datos, denegación de servicio, intrusiones, etc.

3.2. Ausencia Masiva de Personal

Situaciones como pandemias, paros, huelgas o eventos naturales que afecten la disponibilidad general del recurso humano.

3.3. Fallas en Infraestructura Crítica

Cortes prolongados de energía, fallas de red, fallos físicos en data centers, incendios, terremotos, etc.

4. Plan Anual de Pruebas de Contingencia

Tipo de Prueba	Frecuencia	Responsable	Metodología	Objetivo Principal
Simulacro de Incidente de Ciberseguridad	Anual (mínimo)	CISO / TI	Ataque simulado (phishing, ransomware)	Validar respuesta técnica y comunicacional
Ejercicio de Ausencia Masiva de Personal	Anual	RRHH / Continuidad	Simulación de 40% de personal no disponible	Validar continuidad con personal de respaldo
Prueba de Recuperación Infraestructura Crítica	Anual	TI / Infraestructura	Fallo simulado de data center primario	Evaluar recuperación ante desastres (DRP)

Se documentarán todos los resultados de las pruebas, tiempos de recuperación (RTO), puntos de recuperación (RPO), y se generarán informes de mejora.

5. Protocolos de Comunicación ante Incidentes Críticos

5.1. Objetivo del Protocolo

Garantizar que las comunicaciones durante un incidente sean oportunas, claras, controladas y alineadas con las necesidades del Banco y otras partes interesadas.

5.2. Roles y Responsables

Rol	Función
Gerente General	Vocero oficial ante el Banco y otras autoridades si se requiere
CISO / Seguridad TI	Comunicación técnica de incidentes de ciberseguridad
Encargado de Comunicaciones	Redacción y aprobación de mensajes internos y externos
Jefe de Operaciones	Coordinación interna del flujo de información

5.3. Canales de Comunicación

- **Internos:** correo corporativo, Teams, SMS, canal de emergencia.
- **Con el Banco:** correo seguro, canal dedicado, teléfono directo 24/7.
- **Externos (si aplica):** sitio web, correo a clientes, declaraciones públicas.

5.4. Mensajes Predefinidos

Ejemplo – Comunicación inicial al Banco en caso de incidente de ciberseguridad:

"Estimado equipo del Banco, se ha detectado un incidente de ciberseguridad que podría afectar el entorno de servicios contratados. Actualmente se encuentra contenido. Adjuntamos informe inicial y mantendremos comunicación cada 2 horas hasta su resolución."

---

6. Reportes y Lecciones Aprendidas

- Todos los ejercicios serán documentados en un **Informe de Prueba de Contingencia**.
- Los incidentes reales o simulados deberán incluir:
    - Tiempo de detección, contención y recuperación.
    - Impacto operativo.
    - Brechas encontradas.
    - Plan de acción correctiva.
- Las lecciones aprendidas serán incorporadas al proceso de mejora continua del BCP y DRP.

---

7. Revisión y Actualización del Plan

- Este plan será revisado al menos **una vez por año**.
- También se actualizará tras:
    - Un incidente crítico real.
    - Cambios en los servicios contratados por el Banco.
    - Reorganización operativa o técnica interna.

Aprobación del Plan

El presente plan será aprobado 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: 12 de Enero 2026
Cargo: Gerente General