Manual de Políticas de Gobierno de Riesgos de Ciberseguridad
de F-BridgeDigital

1. Propósito

Este documento establece las políticas y directrices para la gestión de los riesgos de ciberseguridad de la organización, garantizando la confidencialidad, integridad y disponibilidad de la información, alineándose con las mejores prácticas y estándares internacionales como **ISO/IEC 27001**, **NIST Cybersecurity Framework (CSF)** y **ISO 27005**.

---

2. Alcance

Estas políticas aplican a:

- Todos los empleados y contratistas.
- Proveedores y terceros con acceso a sistemas de información.
- Todos los sistemas, redes, activos digitales y datos gestionados por la organización.

---

3. Marco Normativo y Referencial

Este manual se fundamenta en:

- **ISO/IEC 27001:2022**
- **ISO/IEC 27002:2022**
- **ISO/IEC 27005:2022** – Gestión de Riesgos
- **NIST Cybersecurity Framework (CSF) v2.0**
- **NIST SP 800-30** – Guía para análisis de riesgos
- **NIST SP 800-61** – Gestión de incidentes
- **COBIT 2019** (complementario para gobierno TI)
- **COSO ERM** (integración de riesgos corporativos)

---

4. Principios Rectores

1. Compromiso de la alta dirección con la ciberseguridad.
2. Gestión de riesgos como proceso continuo y sistemático.
3. Adopción de un enfoque basado en riesgo para priorizar controles.
4. Cumplimiento legal, normativo y contractual.
5. Mejora continua del sistema de gestión de seguridad.

5. Políticas de Ciberseguridad

5.1. Política de Gobierno de Seguridad de la Información

- Se establecerá un **Comité de Seguridad de la Información**.
- El comité supervisará las decisiones estratégicas de seguridad y el tratamiento de riesgos.
- Se designará un **Responsable de Seguridad de la Información (CISO)**.

5.2. Política de Gestión de Riesgos de Ciberseguridad

- Se aplicará una metodología documentada para identificar, analizar, evaluar y tratar riesgos.
- Se mantendrá un **Registro de Riesgos** con responsables y planes de tratamiento.
- La evaluación de riesgos será revisada **anualmente** o tras cambios relevantes.
- Se aplicará el ciclo de vida del riesgo: **Identificación → Evaluación → Tratamiento → Monitoreo**.

5.3. Política de Evaluación de Riesgos de Proveedores (TPRM)

- Los proveedores serán clasificados por nivel de riesgo.
- Se exigirán controles mínimos de seguridad en contratos.
- Se realizarán auditorías o evaluaciones periódicas a terceros críticos.

5.4. Política de Gestión de Incidentes de Ciberseguridad

- Se deberá reportar todo incidente sospechoso de forma inmediata.
- Se seguirá un proceso estructurado: **detección, análisis, contención, erradicación, recuperación y lecciones aprendidas**.
- Se mantendrá un **registro centralizado de incidentes**.

5.5. Política de Continuidad del Negocio y Recuperación ante Desastres

- Se desarrollarán y mantendrán actualizados planes de continuidad (BCP) y recuperación (DRP).
- Se realizarán pruebas **al menos una vez al año**.
- Los planes incluirán escenarios de ciberataques (ransomware, denegación de servicio, etc.).

5.6. Política de Gestión de Activos de Información

- Se mantendrá un inventario actualizado de activos.
- Todos los activos serán clasificados por nivel de criticidad (Alta, Media, Baja).
- Cada activo tendrá un responsable asignado.

- Se contará con mecanismos tecnológicos de descubrimiento automático y validación de activos de hardware y software, que permitan detectar en la red dispositivos o aplicaciones no autorizados, falsificados o considerados de alto riesgo.
- Este control busca prevenir la conexión y operación de elementos que no estén homologados o que representen amenazas activas, y forma parte del monitoreo continuo de la postura de seguridad.
- Cualquier hallazgo será gestionado como incidente de seguridad, conforme al protocolo de respuesta correspondiente.

5.7. Política de Seguridad en el Ciclo de Vida del Software

- Se aplicarán principios de **desarrollo seguro** (DevSecOps).
- Se realizarán pruebas de seguridad (SAST, DAST) antes de liberar código.
- Se exigirá que el código sea revisado por al menos otro desarrollador.

5.8. Política de Control de Accesos

- Acceso basado en el principio de **mínimo privilegio**.
- Se aplicará **autenticación multifactor (MFA)** para accesos críticos.
- Los accesos serán revisados al menos **trimestralmente**.
- Inventario de accesos con historial de altas, bajas, cambios.
- Cuentas inactivas suspendidas tras 60 días.
- Eliminación de accesos en 24h tras baja del usuario.
- Accesos definidos por roles/perfiles mínimos necesarios.
- Gestión y monitoreo de acceso remoto seguro.
- Registro de eventos de acceso.
- Contraseñas con cambios obligatorios cada 90 días y 12 contraseñas históricas.
- Bloqueo tras 5 intentos fallidos.

5.9. Protección de la Red

- Diseño de red segmentado por zonas de riesgo.
- Servicios en DMZ restringidos a los necesarios.
- Firewalls, IPS, WAF, IDS y sistemas de detección de DoS/DDoS activos.
- Inventario de conexiones externas.
- Monitoreo de transferencia de datos con el Banco.

5.10. Seguridad en Endpoints

- Parches y antivirus actualizados.
- Uso de software homologado.
- Protección contra malware y configuración segura.
- Reglas sobre finalización de sesiones, privilegios, bloqueo y apagado de estaciones.
- Políticas contra desactivación de controles.

5.11. Monitoreo y Registro

- Monitoreo 24/7 con correlación de eventos.
- Herramientas SIEM para análisis y detección de incidentes.
- Sincronización horaria (NTP/PTP).
- Conservación de logs: mínimo 12 meses.
- Alertas de comportamiento anómalo y recolección de logs multisistema.

5.12. Gestión de Incidentes

- Proceso estructurado: detección, contención, erradicación, recuperación, lecciones aprendidas.
- Registro centralizado de incidentes.
- Reportes obligatorios y trazabilidad.

5.13. Copias de Seguridad

- Política de respaldos con frecuencia y métodos validados con el Banco.
- Plan de recuperación alineado con BCP y DRP.
- Backups cifrados, validados y con pruebas periódicas.

5.14. Protección Contra Pérdida de Datos (DLP)

- Herramientas de cifrado en tránsito y en reposo.
- Evaluación de privacidad de información por sistemas.
- Procedimientos de prevención de fugas.
- Clasificación de datos según criticidad.

5.15. Desarrollo Seguro (DevSecOps)

- Seguridad desde el diseño (Secure by Design).
- Pruebas SAST, DAST, RASP.
- Mecanismos de protección de código fuente y binario.
- Recuperación segura de contraseñas.
- Aplicación de controles OWASP, OSSTMM, CVSS y CIS Controls.
- Autoprotección de aplicaciones y control de tiempos de ejecución.
- Registros de auditoría en aplicaciones, SO y BD: ID, IP, fecha/hora, descripción del evento.

5.16. Política de Concientización y Capacitación

- Todos los empleados deberán recibir formación básica en ciberseguridad.
- Se realizarán campañas internas contra **phishing**, manejo seguro de contraseñas, y protección de datos.
- La formación se renovará **anualmente** y será parte del proceso de onboarding.
- **Política de Uso Aceptable de Recursos Tecnológicos (ver Anexo A)**

En este documento se detallan las pautas y directrices sobre el uso adecuado de los recursos tecnológicos proporcionados por **F-BridgeDigital** o el proveedor, incluyendo el uso de internet, redes sociales, correo electrónico corporativo, mensajería instantánea, y dispositivos informáticos. El personal debe cumplir con estas políticas para asegurar la seguridad y privacidad de la información de la organización y del

---

6. Roles y Responsabilidades

Rol	Responsabilidad
Alta Dirección	Aprobar políticas, asignar recursos, supervisar el marco de riesgo
CISO	Diseñar, implementar y mantener políticas y controles de ciberseguridad
Comité de Seguridad	Revisar informes, validar decisiones clave de tratamiento de riesgos
Equipos Técnicos	Implementar controles, reportar incidentes, mantener configuraciones seguras
Recursos Humanos	Incluir cláusulas de confidencialidad y seguridad en contratos laborales
Proveedores y Terceros	Cumplir con los requerimientos de seguridad establecidos en los contratos

---

7. Cumplimiento y Auditoría

- El cumplimiento será revisado mediante auditorías internas y externas.
- Se evaluará la efectividad del sistema de gestión de seguridad y tratamiento de riesgos.
- Incumplimientos podrán dar lugar a sanciones disciplinarias o contractuales.

---

8. Prevención de Filtración de Datos (DLP) y Protección de Información Sensible

8.1 Evaluación de Privacidad y Seguridad de los Sistemas

- Se contará con procedimientos documentados para evaluar el nivel de seguridad y privacidad de la información que manejan los sistemas utilizados en el entorno tecnológico de F-BridgeDigital.
- Estas evaluaciones consideran:
    - Tipo de información procesada.
    - Clasificación de los datos (confidencial, sensible, etc.).
    - Riesgos de exposición.
    - Controles técnicos y organizativos existentes.

8.2 Cifrado de la Información

- **En tránsito:**
  Toda comunicación de datos entre los sistemas de F-BridgeDigital y el Banco se realizará utilizando **protocolos seguros de cifrado (TLS 1.2 o superior)**, evitando exposiciones a riesgos de interceptación, escucha o manipulación.
- **En reposo:**
  Los activos de información del Banco almacenados eventualmente en infraestructuras de **F-BridgeDigital** serán cifrados utilizando algoritmos criptográficos robustos (AES-256 o equivalente), garantizando confidencialidad ante pérdida, robo o acceso no autorizado.

8.3 Herramientas de Prevención de Fugas de Información (DLP)

- Se utilizarán herramientas de DLP (Data Loss Prevention) que permitan:
  - Identificar y clasificar información sensible.
  - Detectar movimientos inusuales de datos.
  - Bloquear o alertar sobre transferencias no autorizadas de datos sensibles por canales de correo, web o almacenamiento externo.
- Se realiza monitoreo de estas herramientas y se generarán alertas ante posibles violaciones de políticas de protección de datos.

---

9. Copias de Seguridad y Recuperación de Información

9.1 Política de Respaldo

- F-BridgeDigital contará con una política de respaldo formalmente documentada que define:
  - Tipos de datos y sistemas a respaldar.
  - Frecuencia de ejecución (diaria, semanal, mensual).
  - Métodos de respaldo (incrementales, completos, diferenciales).
  - Responsable(s) de su ejecución y verificación.
  - Procedimientos de restauración probada.

9.2 Requisitos Contractuales con el Banco

- Los respaldos de información vinculada al Banco cumplen con los **requisitos de frecuencia y método** acordados explícitamente con el responsable de los activos del Banco.
- Se garantizará la protección criptográfica de los respaldos, así como su almacenamiento en entornos seguros y segregados.
- Se realizarán **pruebas periódicas de restauración** para asegurar la integridad y disponibilidad de los datos respaldados.

9.3 Eliminación Segura

- Los respaldos expirados o no requeridos se eliminarán utilizando métodos de destrucción segura conforme a la política de borrado seguro, garantizando su **irrecuperabilidad e ilegibilidad**.

---

10. Gestión de Accesos Lógicos (Logical Access Management - LAM)

10.1 Política de Control de Accesos

- Se contará con una política formal de gestión de accesos lógicos que:
  - Restringe el acceso únicamente a usuarios autorizados.
  - Establece una cadena de aprobación documentada para cada alta, modificación o baja de acceso.
  - Aplica principios de **"necesidad de conocer"** y **mínimo privilegio**.
  - Establece **segregación de funciones** en la administración de permisos, asegurando que al menos dos personas participen en el control y validación.
  - Define roles, perfiles, accesos y responsabilidades basados en clasificación de la información y criticidad del activo.

10.2 Registro de Accesos

- Se mantendrá un **inventario actualizado de accesos** a activos tecnológicos, incluyendo altas, modificaciones y bajas, con una retención de mínimo 1 año.
- Se garantizará la baja de accesos lógicos de personal interno o externo en un plazo máximo de:
  - 24 horas para accesos relacionados al Banco.
  - 7 días para accesos secundarios.
- Las cuentas inactivas por más de 60 días consecutivos serán deshabilitadas automáticamente.

10.3 Métodos y Seguridad de Acceso

F-BridgeDigital establece las siguientes directrices para garantizar la seguridad en el acceso lógico a sus sistemas, especialmente aquellos vinculados a servicios críticos y activos del Banco:

- **Autenticación robusta:** Todos los accesos a sistemas críticos deberán utilizar mecanismos de autenticación robusta, incluyendo obligatoriamente la autenticación multifactor (2FA), en especial para servicios que involucren transacciones financieras o instrucciones de pago.
- **Accesos remotos seguros:** El acceso remoto a los sistemas deberá realizarse exclusivamente a través de canales cifrados y seguros. Se deberán aplicar políticas de autorización explícita, autenticación contextual (que considere el usuario, el dispositivo,

la ubicación y la postura de seguridad) y mecanismos de segmentación o segregación de red para proteger el entorno tecnológico.

- **Monitoreo y registro de accesos:** Todos los accesos lógicos a sistemas, aplicaciones y activos del Banco deberán ser registrados y monitoreados de forma continua. Los registros deberán conservarse conforme a las políticas de auditoría y trazabilidad establecidas por la organización.

10.4 Políticas de Contraseñas

- Contraseñas para usuarios deben cambiarse cada 90 días.
- Cuentas administrativas: cambio obligatorio cada 30 días.
- Cuentas de altos privilegios deben forzar cambio al primer acceso tras reseteo.
- La contraseña nueva debe ser diferente a las últimas 12 utilizadas.
- Desactivación automática tras 5 intentos fallidos consecutivos.

10.5 Responsabilidades del Usuario

- Cada usuario deberá proteger sus credenciales.
- Estará obligado a notificar inmediatamente al Banco cualquier incidente relacionado con pérdida, robo o uso indebido de credenciales.

---

11. Protección Integral de Aplicaciones

11.1 Gestión de Información Confidencial

- Se aplicará una política que contempla la triada **Confidencialidad, Integridad y Disponibilidad (CID)** para el tratamiento de datos sensibles de clientes, empleados y terceros.
- Los procesos ABM (Altas, Bajas y Modificaciones) consideran definición de accesos por roles/perfiles, autenticación y bloqueo automático por inactividad o error.

11.2 Seguridad en el Desarrollo de Software

- Se contará con políticas para:
    - Aplicar desarrollo seguro (por ejemplo, secure coding y DevSecOps).
    - Documentar propiedades funcionales y controles implementados.
    - Mantener el diseño técnico actualizado.
    - Proteger código binario y/o firmware contra alteraciones no autorizadas.
    - Respaldar y proteger el código fuente mediante herramientas como Bitbucket o GitLab, asegurando su envío seguro al Banco.

11.3 Autoprotección y Ejecución Controlada

- Se emplearán tecnologías de **Runtime Application Self-Protection (RASP)**.
- Se configurarán **temporizadores de ejecución** para limitar el tiempo de procesos.

- Se protegerán procesos de recuperación de contraseñas mediante cifrado end-to-end.

11.4 Gestión de Vulnerabilidades

- Se contarán con herramientas automatizadas para **identificar y clasificar vulnerabilidades** con base en estándares como:
  - **OWASP**
  - **CVSS**
  - **Mitre ATT&CK**
  - **OSSTMM**
- Los resultados serán documentados y tratados en ciclos de mejora continua.

11.5 Controles de Seguridad Basados en CIS

Se implementarán controles alineados con el **Center for Internet Security (CIS)** o mediante controles compensatorios equivalentes:

- Inventario de dispositivos y software autorizado/no autorizado.
- Gestión continua de vulnerabilidades.
- Configuración segura de hardware y software.
- Control de puertos, servicios y protocolos.
- Análisis y monitoreo continuo de logs.
- Capacidad de recuperación ante incidentes.

11.6 Registro de Eventos y Auditoría

- Se incorporarán registros de auditoría en sistemas operativos, bases de datos y aplicaciones que incluyen:
  - ID de usuario y programa.
  - IP del origen del evento.
  - Fecha y hora.
  - Descripción del evento (acceso, error, caída, etc.).

11.7 Política de Privacidad en Canales Públicos

F-BridgeDigital mantendrá publicada en su sitio web oficial una **Política de Privacidad** accesible y actualizada, a través de la cual informará de manera clara y transparente sobre los siguientes aspectos:

- La recolección, uso, tratamiento y protección de los datos personales de sus usuarios.
- Los fines y bases legales del tratamiento de la información.
- Los derechos de los titulares de datos y los mecanismos para ejercerlos.

La Política de Privacidad estará alineada con los principios de **privacidad por diseño**, **confidencialidad**, **integridad** y **disponibilidad** de la información, en cumplimiento con la

normativa legal vigente y las mejores prácticas internacionales en materia de protección de datos personales.

F-BridgeDigital revisará periódicamente esta política para asegurar su adecuación frente a cambios normativos, tecnológicos o de servicios ofrecidos, promoviendo así la confianza y la transparencia hacia sus usuarios y clientes.

11.8. Simulación de Amenazas y Pentesting:

F-BridgeDigital realizará simulaciones periódicas de amenazas y pruebas de penetración (pentesting) sobre sus aplicaciones y la infraestructura tecnológica involucradas en la prestación de servicios al Banco y a otros clientes estratégicos. Estas actividades serían ejecutadas por proveedores de seguridad calificados y con experiencia en el sector financiero.

Las pruebas tendrán como objetivo identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.

Se documentarán los hallazgos y se establecerán planes de acción para su remediación.

Los informes resultantes serán revisados por el área de ciberseguridad y, cuando corresponda, compartidos con clientes bajo acuerdos contractuales de confidencialidad.

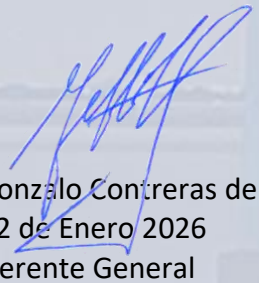
Estas prácticas formarán parte del ciclo de mejora continua en la protección de la confidencialidad, integridad y disponibilidad de las plataformas tecnológicas de F-BridgeDigital.

12. Revisión y Actualización del Manual

- Este manual debe revisarse **anualmente**.
- También se actualizará ante:
    - Cambios regulatorios.
    - Incidentes significativos.
    - Cambios en procesos, tecnologías o estructura.

Aprobación de la Política

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: 12 de Enero 2026
Cargo: Gerente General

Anexo A

Política de Uso Aceptable de Recursos Tecnológicos

Objetivo:
Esta política tiene como objetivo establecer las directrices claras sobre el uso adecuado de los recursos tecnológicos proporcionados por **F-BridgeDigital** o por los proveedores asociados en el contexto de servicios al Banco. El cumplimiento de esta política es obligatorio para todos los empleados, contratistas, proveedores y terceros con acceso a los recursos tecnológicos de la organización.

Ámbito de Aplicación:

Esta política aplica a todos los empleados, contratistas, proveedores, y terceros que utilicen los recursos tecnológicos proporcionados por **F-BridgeDigital**, incluyendo dispositivos informáticos, redes, sistemas, aplicaciones, correo electrónico corporativo y cualquier otro equipo relacionado con la operación de la organización.

1. Uso de Internet

- El acceso a internet debe ser utilizado para actividades laborales relacionadas con el servicio proporcionado a **F-BridgeDigital** o al Banco.
- Queda prohibido el acceso a contenidos inapropiados, ilegales o que representen una amenaza para la seguridad de la organización, incluyendo pero no limitado a material de contenido explícito, violento o cualquier actividad no autorizada que pueda comprometer la red.
- Los recursos de internet no deben ser utilizados para la descarga de software o material que no esté relacionado con las tareas laborales.

2. Uso de Redes Sociales

- El uso de redes sociales debe ser realizado de manera profesional y respetuosa, y únicamente en el contexto de actividades relacionadas con la organización.
- Está prohibido el uso de las redes sociales para divulgar información confidencial o sensible relacionada con **F-BridgeDigital** o el Banco sin la debida autorización.

3. Uso del Correo Electrónico Corporativo

- El correo electrónico corporativo debe utilizarse exclusivamente para fines laborales y actividades relacionadas con el servicio proporcionado.
- Queda prohibido el uso del correo electrónico corporativo para actividades personales, promoción de productos o servicios no relacionados con el trabajo o la organización.

- El correo electrónico no debe utilizarse para transmitir información confidencial sin las medidas de seguridad adecuadas, como el cifrado de la información.

4. Uso de la Mensajería Instantánea

- La mensajería instantánea debe usarse exclusivamente para comunicación interna relacionada con actividades laborales.
- No está permitido el intercambio de información sensible o confidencial por mensajería instantánea sin las debidas protecciones de seguridad.

5. Uso de Equipos Informáticos Facilitados por el Proveedor

- Los dispositivos informáticos proporcionados por **F-BridgeDigital** o el proveedor deben ser utilizados exclusivamente para actividades laborales y en conformidad con las políticas de seguridad y privacidad de la organización.
- Los dispositivos no deben ser modificados, alterados o utilizados para instalar software no autorizado que pueda representar una amenaza para la seguridad.
- El personal no debe conectar dispositivos personales o externos sin autorización previa de **F-BridgeDigital**.

6. Uso de Equipos Informáticos Personales

- El uso de equipos informáticos personales (portátiles, teléfonos, tablets) en el trabajo debe estar limitado a actividades autorizadas y siempre que se adhieran a las políticas de seguridad de **F-BridgeDigital**.
- Los dispositivos personales deben estar protegidos mediante contraseñas, cifrado y otras medidas de seguridad apropiadas antes de acceder a los recursos de la organización.

7. Uso de Dispositivos de Almacenamiento Portátil o Extraíbles

- Los dispositivos de almacenamiento extraíbles (como USB, discos duros portátiles, etc.) no deben contener información sensible o confidencial sin cifrado previo.
- Queda prohibido el uso de dispositivos no autorizados o la transferencia no segura de datos confidenciales fuera del entorno corporativo.

8. Responsabilidades Relativas al Tratamiento de Activos de Información del Banco

- Los empleados, contratistas y proveedores deben asegurarse de que cualquier activo de información del Banco, incluyendo datos, aplicaciones, sistemas o dispositivos, sea tratado con la debida confidencialidad, integridad y disponibilidad.
- Se deben seguir todas las directrices de seguridad, cifrado, control de accesos y manejo de datos sensibles según lo estipulado en las políticas de seguridad de **F-BridgeDigital**.

Cumplimiento de la Política

- Todo el personal relacionado con el servicio está obligado a cumplir con esta política. El incumplimiento de estas directrices puede dar lugar a sanciones disciplinarias, que incluyen la terminación de contratos, suspensión de acceso a sistemas o acciones legales, según corresponda.
- **F-BridgeDigital** deberá asegurarse de que esta política sea debidamente comunicada y entendida por todos los empleados y contratistas que trabajen en el servicio.