

# Políticas de Seguridad de la Información – Transferencias y Transacciones electrónicas

## 1. Artículo. - Objetivo

El presente reglamento tiene por objetivo definir el marco de gestión seguridad lógica y física para el sistema de transacciones electrónicas de La Entidad.

## 2. Artículo. - Seguridad del sistema

Los sistemas funcionalmente deben permitir a un usuario:

- ✓ Ejecutar transacciones electrónicas de transferencias de dinero
- ✓ Ejecutar transacciones electrónicas de transferencias de información: solicitud de bloqueo, etc.
- ✓ Emitir reportes de transacciones ejecutadas con todos los datos del log permitido.

En función a la Política de Seguridad de la Información, Estrategias de Seguridad de la Información, y evaluación y análisis de riesgos de seguridad de la información deben velar por la confiabilidad, no repudio, autenticidad e integridad el sistema, al menos debe considerar las siguientes herramientas:

Para el acceso a los usuarios deben establecer:

- ✓ Control de accesos por perfil de usuario externo
- ✓ Registro de logs de auditoría que permitan identificar la fuente de los mensajes con la información suficiente de usuario, fecha, hora, transacción, identificación de la terminal remota, ubicación física regionalizada, propietario (caso cajeros).
- ✓ Mecanismos que aseguren la conclusión/rollback de las transacciones ante caída de comunicación manteniendo la integridad de los datos.
- ✓ Si bien el acceso es mediante la página WEB, debe insertarse un nivel adicional de seguridad controlado por contraseñas de seguridad.

La información debe ser conservada acorde a disposiciones legales vigentes.

## 3. Artículo. - Canal de comunicación cifrado

Toda información relacionada a transferencias y transacciones electrónicas, deberá ser encriptación garantizando su integridad y disponibilidad durante todo el flujo operativo de los Sistemas. La Entidad deberá utilizar certificados digitales para las conexiones establecidas entre sus clientes y los sistemas en función a la Política de Seguridad de la Información, Estrategia de Seguridad de la Información, y evaluación y análisis de riesgos en seguridad de la información.

## 4. Artículo. - Difusión

Tanto la descripción del servicio, condiciones, formalidad legal y elementos del producto establecidos se publican en todo medio de información disponible en especial mediante la Pagina web Institucional de la Entidad para sus clientes.

## 5. Artículo. - Certificación

Los sitios y servidores establecidos por la Entidad para la realizar transacciones y transferencias electrónicas deberán contar con una Certificado en función a la Política de Seguridad de la Información, Estrategia de Seguridad de la Información, y evaluación y análisis de riesgos en seguridad de la información, mismos que permanecerán vigentes siendo responsabilidad del departamento de TI su renovación anual.

Asimismo, el dominio de la página web Institucional, deberá ser registrado ante la ADSIB (Agencia para el Desarrollo de la Sociedad de la Información en Bolivia) y se encontrará alojado en un sitio VPS (Virtual Private Server) principalmente con las siguientes características:

- ✓ Soporte 24x7
- ✓ Obtención de Backups Automatizados
- ✓ Herramientas de Seguridad
- ✓ Certificado en función a la Política de Seguridad de la Información, Estrategia de Seguridad de la Información, y evaluación y análisis de riesgos en seguridad de la información.

## 6. Artículo. - Continuidad Operativa

El Plan de Contingencias de Tecnologías de la Información deberá considerar especial acciones y recursos para reducir el impacto frente a eventos fortuitos o deliberados que afecten principalmente los servicios de Transferencias y Transacciones electrónicas.

## 7. Artículo. - Pistas de Auditoria

Los sistemas utilizados por la , además de permitir el registro y seguimiento íntegro de las transferencias y/o transacciones electrónicas realizadas, generan archivos que permitan respaldar los antecedentes de cada operación electrónica, necesarios para efectuar cualquier seguimiento, examen o certificación posterior, tales como, fechas y horas en que se realizaron las mismas, el contenido de los mensajes, identificación de los operaciones, emisores y receptores, cuentas y montos involucrados, así como la identificación de terminales desde las cuales se realizaron.

La conservación de esta información se mantiene por un período no menor a diez (10) años;

## 8. Artículo. - Verificación y control

Los sistemas que realicen Transferencias y Transacciones electrónicas permitirán:

- ✓ Definir el límite diario de tanto en monto como en cantidad de veces de las transferencias y transacciones electrónicas según términos establecidas por LA ENTIDAD y en caso de que así lo requieran los clientes.
- ✓ Determinar el origen de las operaciones Electrónicas a nivel nacional e Internacional.
- ✓ Emisión de reportes de transacciones ejecutadas por región.

## 9. Artículo. - Contratos Legales

Las relaciones con los participantes en el servicio de transacciones y transferencias electrónicas deben establecer contratos especificando al menos el nivel de servicio, condiciones, aspectos operativos, políticas de seguridad, confidencialidad, y otros en función a la Política de Seguridad de la Información, Estrategia de Seguridad de la Información, y evaluación y análisis de riesgos en seguridad de la información.