TITULO VII

REQUISITOS MÍNIMOS DE SEGURIDAD

TABLA DE CONTENIDO

Capítulo III: Reglamento para la Gestión de Seguridad Física

CAPÍTULO I: REGLAMENTO PARA DEPÓSITOS Y RETIROS DE MATERIAL MONETARIO EN Y DEL BANCO CENTRAL DE BOLIVIA

SECCIÓN 1: *ASPECTOS GENERALES*

Artículo 1° - (Objeto) El presente reglamento tiene por objeto establecer lineamientos para las medidas de seguridad que deben aplicar las Entidades de Intermediación Financiera (EIF) en cuanto a los depósitos y retiros de material monetario que éstas realicen, en las cuentas que mantienen en el Banco Central de Bolivia (BCB), en el marco de lo dispuesto en el Reglamento para la Administración de Material Monetario del Ente Emisor.

Artículo 2° - (Ámbito de Aplicación) Se encuentran sujetas al ámbito de aplicación del presente reglamento, las EIF que cuenten con Licencia de Funcionamiento otorgada por la Autoridad de Supervisión del Sistema Financiero (ASFI) y son titulares de Cuentas Corrientes y de Encaje o Cuentas de Encaje en el BCB, denominadas en adelante como entidades supervisadas.

Artículo 3° - (Definiciones) Para efectos del presente Reglamento se utilizarán las siguientes definiciones:

a. **Billete inhábil:** Es aquel billete emitido por el BCB que conserva claramente sus dos firmas y al menos un número de serie y que de acuerdo a los criterios de 1) Suciedad, manchas, grafitos y decoloración y 2) Rasgaduras, mutilaciones, agujeros y reparaciones, establecidos en el Manual para la Selección de Billetes de Boliviano, debe ser retirado de circulación;

b. **Cintillo:** Pieza de papel con el logo de la entidad supervisada, que cubre cada fajo de billetes, permitiendo su separación en otros fajos;

c. **Fajo de billetes:** Conjunto de cien piezas de billetes del mismo corte, cubierto por un cintillo;

d. **Gestión de seguridad física:** Conjunto de objetivos, políticas, procedimientos, planes y acciones que implementa la entidad supervisada con el objeto de proteger la integridad física de las personas, así como los activos que se encuentren bajo su custodia, en el interior o fuera de sus instalaciones, además de la seguridad de su personal, cuando éste realice operaciones y servicios fuera de las dependencias de la entidad;

e. **Marbete:** Etiqueta que contiene datos que permiten identificar a la entidad supervisada que conformó el paquete de billetes o monedas y que se encuentra adherido a éste, con la siguiente información:

    1. Nombre y logotipo de la entidad supervisada depositante;
    2. Nombre o sello de la empresa que conformó el paquete, si corresponde;
    3. Nombre completo, firma y sello de la que persona que conformó el paquete;
    4. Corte del material monetario e importe del paquete;
    5. Lugar y fecha de la conformación del paquete.

f. **Paquete de billetes:** Conjunto de mil piezas de billetes del mismo corte, ordenados en diez fajos de billetes cada uno, con marbetes impresos;

g. **Paquete de monedas:** Conjunto de mil piezas de monedas del mismo corte, ordenados en diez cilindros de cien monedas cada uno, con marbetes impresos.

SECCIÓN 2: *MEDIDAS DE SEGURIDAD*

Artículo 1° - (Políticas y procedimientos) Las entidades supervisadas deben contar con políticas y procedimientos específicos para la gestión de depósitos y retiros de material monetario que realicen en las cuentas que mantienen en el Banco Central de Bolivia (BCB), aprobados por el Directorio u Órgano equivalente, los cuales deben ser revisados por los niveles que correspondan al menos una (1) vez al año, los cuales como mínimo deben contener lo siguiente:

a. Controles para la mitigación del riesgo operativo;

b. Medidas operativas de seguridad;

c. Delegación de autoridad y responsabilidades, así como segregación de funciones;

d. Medidas de seguridad física bajo el marco de la gestión de seguridad de la entidad;

e. Lineamientos para el registro de los movimientos de sus cuentas y la custodia de comprobantes;

f. Aspectos referidos a la verificación, conteo, validación, clasificación y autenticación del material monetario, así como la selección de billetes por su estado y calidad;

g. Demás lineamientos contemplados en el presente Reglamento.

Artículo 2° - (Preparación y transporte) Con el propósito de precautelar la seguridad en los procesos de preparación y transporte de material monetario que realicen las entidades supervisadas, para su depósito y retiro, en sus cuentas en el BCB, además de lo previsto en el Reglamento para la Administración de Material Monetario del Ente Emisor, dichas entidades deben cumplir con los siguientes aspectos:

a. Todos los depósitos y retiros de material monetario, deben ser aprobados por los niveles de autorización correspondientes, en cumplimiento de sus políticas internas de liquidez;

b. Los paquetes de billetes y los paquetes de monedas deben estar termosellados con plástico retráctil que lleve el logotipo de la entidad supervisada y contar con marbetes impresos, además de estar clasificados y revisados según los criterios establecidos en el Manual para la Selección de Billetes de Boliviano emitido por el BCB.

Los paquetes de billetes inhábiles deberán contener fajos con billetes careados; es decir, todos los billetes del fajo en la misma orientación y posición. A su vez, los paquetes de billetes en dólares estadounidenses, deben tener las características que establezca la Reserva Federal de Estados Unidos, las cuales son comunicadas por el BCB.

Todos los paquetes deben encontrarse contenidos en bolsas plásticas de seguridad;

c. La programación y logística del transporte de material monetario debe ser de conocimiento restringido del personal autorizado de la entidad supervisada;

Toda operación de depósito y retiro de material monetario, debe ser coordinada previamente con el BCB, considerando los horarios de atención establecidos;

d. El transporte de material monetario para el depósito y retiro de material monetario, debe realizarse mediante una Empresa de Transporte de Material Monetario y Valores (ETM), que cuente con Licencia de Funcionamiento otorgada por la Autoridad de

Supervisión del Sistema Financiero (ASFI) o mediante su Servicio Propio de Transporte de Material Monetario y Valores (ESPT), autorizado por ASFI, de acuerdo a lo dispuesto en la Sección 4 del Reglamento para Transporte de Material Monetario contenido en el Capítulo IV, Título II, Libro 1° de la Recopilación de Normas para Servicios Financieros (RNSF);

e. El personal de la entidad supervisada es responsable de la entrega y recepción de material monetario a la ETM.

Artículo 3° - (Registro de operaciones) El personal autorizado al momento de realizar los depósitos y retiros de material monetario, debe revisar los comprobantes de las transacciones emitidos por el BCB, para su posterior resguardo, como respaldo de movimientos en las cuentas de la entidad supervisada. Los comprobantes deben entregarse a las instancias correspondientes, para que se realice el registro de manera oportuna.

La entidad supervisada debe conciliar diariamente los saldos de las cuentas de Disponibilidades en el Banco Central de Bolivia, con los estados de cuenta emitidos por el mismo.

Artículo 4° - (Control de depósitos en el BCB) El BCB, de acuerdo a sus procedimientos establecidos para el efecto podrá, en cualquier momento, hacer recuentos en detalle de los depósitos realizados por las entidades supervisadas.

El BCB, reportará a ASFI de acuerdo a su programación, los faltantes y sobrantes o cualquier otra anormalidad que existiera en los depósitos con los siguientes datos:

1. Entidad supervisada depositante;

2. Nombre y apellido del cajero cuyo sello figura en el marbete;

3. Nombre y apellido de la persona que efectuó el depósito en el BCB;

4. Nombre y apellido del representante del BCB;

5. Nombres de los veedores y controladores de la entidad supervisada depositante;

6. Detalle de la anormalidad;

7. Moneda, corte y monto.

Cualquier diferencia detectada deberá ser conciliada con los comprobantes de la operación, para determinar los cargos y abonos correspondientes.

SECCIÓN 3: *OTRAS DISPOSICIONES*

Artículo 1° - (Responsabilidad) El Gerente General de la entidad supervisada, es responsable del cumplimiento y difusión interna del presente Reglamento.

Artículo 2° - (Régimen de Sanciones) El incumplimiento o inobservancia al presente Reglamento dará lugar al inicio del procedimiento administrativo sancionatorio.

CONTROL DE VERSIONES

L03T07C01		**Secciones**		
Circular	**Fecha**	**1**	**2**	**3**
ASFI/531/2018	12/03/2018	*	*	
ASFI/477/2017	18/08/2017	*	*	*
SB/288/1999	01/04/1999			

CAPÍTULO II: REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SECCIÓN 1: DISPOSICIONES GENERALES

Artículo 1° - (Objeto) El presente Reglamento tiene por objeto establecer las directrices y requisitos mínimos que las Entidades de Intermediación Financiera (EIF), Empresas de Servicios Financieros Complementarios (ESFC) y Sociedades Controladoras de Grupos Financieros (SCGF), deben cumplir para la gestión de seguridad de la información, de acuerdo a su naturaleza, tamaño y estructura, así como con la complejidad de los procesos y operaciones que realizan.

Artículo 2° - (Ámbito de aplicación) Están comprendidas en el ámbito de aplicación del presente Reglamento las EIF, ESFC (excepto Casas de Cambio) y SCGF, que cuenten con Licencia de Funcionamiento otorgada por la Autoridad de Supervisión del Sistema Financiero (ASFI), denominadas en adelante como Entidad Supervisada.

Artículo 3° - (Definiciones) Para efectos del presente Reglamento, se utilizarán las siguientes definiciones:

a. **Activo de información:** Aquellos datos, información, sistemas y elementos relacionados con la tecnología de la información, que tienen valor para la Entidad Supervisada;

b. **Acuerdo de nivel de servicio (*SLA: Service Level Agreement*):** Documento en el cual se estipulan las condiciones de un servicio en función a parámetros objetivos, establecidos de mutuo acuerdo entre un proveedor de servicio y la Entidad Supervisada;

c. **Ambientes de desarrollo, prueba y producción**: Recursos de Tecnologías de Información, destinados al desarrollo, pruebas y uso oficial de sistemas informáticos;

d. **Análisis y evaluación de riesgos en seguridad de la información:** Proceso por el cual se identifican los activos de información, así como las amenazas y vulnerabilidades a las que éstos se encuentran expuestos y que representan un riesgo para la seguridad de la información, se evalúa la probabilidad de ocurrencia y se calcula el impacto potencial de su materialización, con el fin de establecer controles que minimicen los efectos de los posibles incidentes de seguridad de la información;

e. **Área de exclusión:** Área de acceso restringido identificada en las instalaciones de la Entidad Supervisada;

f. **Banca electrónica:** Servicio financiero ofertado por las entidades de intermediación financiera autorizadas, a través de Internet u otros medios electrónicos para procesar de manera automática el registro de datos, desarrollo de transacciones y pagos, así como el intercambio de información, dinero y otros;

g. **Cajero automático (CA):** Punto de atención financiera que permite a los clientes y/o usuarios de servicios financieros, mediante la operación de una máquina dedicada al efecto, de forma enunciativa y no limitativa, realizar retiros y/o depósitos de efectivo, consultas de movimientos y saldos, rescate de cuotas, transferencias entre cuentas propias y a cuentas de terceros, carga y efectivización de billetera móvil y/o pagos de servicios, mediante el uso

de tarjetas de débito, tarjetas de crédito, tarjetas prepagadas o un dispositivo móvil, que debe cumplir con lo establecido en el Reglamento para el Funcionamiento de Cajeros Automáticos, contenido en la Recopilación de Normas para Servicios Financieros (RNSF). Los cajeros automáticos son también conocidos por su sigla en inglés: ATM (*Automated Teller Machine*);

h. **Centro de procesamiento de datos (CPD):** Infraestructura tecnológica e instalación(es); clasificada(s) como área de exclusión, donde están ubicados los recursos utilizados para el procesamiento de información;

i. **Centro de procesamiento de datos alterno (CPDA):** Infraestructura tecnológica e instalación(es), que cuenta con los recursos utilizados para el procesamiento de información en forma alterna al CPD;

El ambiente físico donde se encuentra instalado el CPDA, debe ser clasificado como área de exclusión y encontrarse en una ubicación geográfica distinta al CPD;

j. **Cifrar:** Proceso mediante el cual la información o archivos es alterada, en forma lógica, incluyendo claves en el origen y en el destino, con el objetivo de evitar que personas no autorizadas puedan interpretarla al verla, copiarla o utilizarla para actividades no permitidas;

k. **Contraseña o clave de acceso (*Password*):** Conjunto de caracteres que una persona debe registrar para ser reconocida como usuario autorizado, para acceder a los recursos de un servicio, sistema, programa, equipo computacional o red;

l. **Computación en la nube (*Cloud Computing*):** Modelo de Acceso bajo demanda a través de una red (Internet), a un conjunto compartido de recursos informáticos o computacionales (redes, servidores, almacenamiento, aplicaciones o servicios) que pueden ser rápidamente provisionados y publicados con un mínimo esfuerzo de administración o de interacción con el proveedor de servicios, con un sistema de precios basado en el consumo realizado;

m. **Cortafuegos (*Firewall*)**: Dispositivo o conjunto de dispositivos (*software* y/o *hardware*) configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos de un sistema, red o redes, sobre la base de un conjunto de normas y otros criterios, de manera que sólo el tráfico autorizado, definido por la política local de seguridad, sea permitido;

n. **Encargado del tratamiento:** Proveedor de servicios de computación en la nube;

o. **Equipo crítico:** Equipo(s) de procesamiento de datos que soporta(n) las principales operaciones de la Entidad Supervisada;

p. ***Hardware*:** Conjunto de todos los componentes físicos y tangibles de un computador o equipo electrónico;

q. **Incidente de seguridad de la información**: Suceso o serie de sucesos, que tienen una probabilidad significativa de comprometer las operaciones de la Entidad Supervisada, amenazar la seguridad de la información y/o los recursos tecnológicos;

r. **Interfaz de programación de aplicaciones de la computación en la nube (*Cloud API*):** Conjunto de interfaces de programación de aplicaciones que permiten a un *software*,

solicitar datos o cálculos de uno o más servicios para el intercambio de mensajes o datos, conocido también como "Application Programming Interface";

s. **Internet:** Red de redes de alcance mundial que opera bajo estándares y protocolos internacionales;

t. **Intranet:** Red informática de una Entidad Supervisada que permite compartir información o programas;

u. **Infraestructura de tecnología de la información:** Es el conjunto de *hardware*, *software*, redes de comunicación, multimedia y otros, así como el sitio y ambiente que los soporta, que es establecido para el procesamiento de la información;

v. **Mecanismo de autenticación robusta:** Forma de verificar la identidad de los usuarios, basada en el uso de la combinación de dos de los tres factores de autenticación siguientes:

1. Algo que el usuario sabe;

2. Algo que el usuario tiene;

3. Algo que el usuario es.

w. **Medios de acceso a la información:** Son equipos servidores, computadores personales, teléfonos inteligentes, terminales tipo cajero automático, las redes de comunicación, Intranet, Internet y telefonía;

x. **Plan de contingencias tecnológicas:** Documento que contempla un conjunto de procedimientos y acciones que deben entrar en funcionamiento al ocurrir un evento que dañe parte o la totalidad de los recursos tecnológicos de la Entidad Supervisada;

y. **Plan de continuidad del negocio (*BCP: Business Continuity Planning*):** Documento que contempla la logística que debe seguir la Entidad Supervisada a objeto de restaurar los servicios y aplicaciones críticas parcial o totalmente suspendidas dentro de un tiempo predeterminado, después de una interrupción inesperada o un desastre;

z. **Portabilidad:** Característica de los servicios de computación en la nube, que establece que los datos del Responsable del tratamiento (contratista), que están en los servidores del proveedor (Encargado del tratamiento) del servicio de computación en la nube, puedan trasladarse a otro proveedor (o a sistemas locales), a elección del contratista y sin pérdida de datos ni del servicio;

aa. **Principio de menor privilegio:** Establece que cada programa y cada usuario del(los) sistema(s) de información deben operar utilizando los privilegios estrictamente necesarios para completar el trabajo asignado;

bb. **Proceso crítico:** Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de la Entidad Supervisada;

cc. **Procedimiento de enmascaramiento de datos:** Mecanismo que modifica los datos de un determinado sistema en ambientes de desarrollo y pruebas, con el fin de garantizar la confidencialidad de la información del ambiente de producción;

dd. **Procesamiento de datos o ejecución de sistemas en lugar externo**: Procesos informáticos que soportan las operaciones financieras y administrativas de la Entidad Supervisada que incluyen: el procesamiento de tarjetas electrónicas, servicios de pago móvil, custodia electrónica de valores desmaterializados en Entidades de Depósito de Valores, alojamiento de sitios web o de correo electrónico institucional en servidores administrados externamente, el hospedaje físico de servidores utilizados por la entidad en ambientes ajenos y otros procesos similares;

ee. **Propietario de la información:** Es el responsable formalmente designado para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información;

ff. **Protección física y ambiental:** Conjunto de acciones y recursos implementados para proteger y permitir el adecuado funcionamiento de los equipos e instalaciones del Centro de Procesamiento de Datos y del Centro de Procesamiento de Datos Alterno, dada su condición de áreas de exclusión;

gg. **Pruebas de intrusión (*Pen test*):** Son pruebas controladas que permiten identificar posibles debilidades de los recursos tecnológicos de la Entidad Supervisada, que un intruso podría llegar a explotar para obtener el control de sus sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores y/o dispositivos de red. Las pruebas de intrusión pueden ser realizadas a través de la intranet, desde Internet, accesos remotos o cualquier otro medio.

Las pruebas de intrusión se clasifican, dependiendo del origen del ataque, en:

1. **Externas**, cuando se busca identificar las posibles vulnerabilidades que se encontrarían ante una acción maliciosa externa;
2. **Internas**, cuando se busca identificar las vulnerabilidades ante acciones que se produzcan dentro de la propia Entidad Supervisada.

hh. **Punto de venta (POS: *Point Of Sale*):** Equipo electrónico y/o electromecánico que permite a los usuarios de servicios financieros realizar pagos, mediante el uso de sus tarjetas electrónicas, en empresas aceptantes afiliadas a una red de sistemas de pago;

ii. **Respaldo o copia de seguridad (*Backup*):** Copia de datos e información almacenada en un medio digital, que se genera en forma periódica; con el propósito de utilizar dicha información o datos, en casos de emergencia o contingencia;

jj. **Responsable del tratamiento:** Persona natural o jurídica que contrata los servicios de computación en la nube;

kk. **Seguridad de la información:** Conjunto de medidas y recursos destinados a resguardar y proteger la información, así como los activos de información, buscando mantener la confidencialidad, confiabilidad, disponibilidad e integridad de la misma;

ll. **Servicio de Pago Móvil:** Conjunto de actividades relacionadas con la emisión de billeteras móviles y procesamiento de órdenes de pago a través de dispositivos móviles, en el marco del Reglamento de Servicios de Pago, Instrumentos Electrónicos de Pago, Compensación y Liquidación emitido por el Banco Central de Bolivia (BCB);

mm. **Sistema de información:** Conjunto organizado e interrelacionado de procedimientos de recopilación, procesamiento, transmisión y difusión de información que interactúan entre sí para lograr un objetivo;

nn. **Sitio externo de resguardo:** Ambiente externo a las instalaciones de la entidad supervisada y al CPDA, donde se almacenan todos los medios de respaldo, documentación y otros recursos de tecnología de información catalogados como críticos y/o necesarios para soportar los planes de continuidad y contingencias tecnológicas;

oo. **Software:** Equipamiento o soporte lógico de un sistema de información que comprende el conjunto de los componentes lógicos que hacen posible la realización de tareas específicas. El software incluye: software de sistema, software de programación y software de aplicación;

pp. **Tarjeta electrónica**: Instrumento Electrónico de Pago (IEP) que permite al tarjetahabiente instruir órdenes de pago, retirar efectivo y/o efectuar consultas de cuentas relacionadas con la tarjeta electrónica. Se consideran tarjetas electrónicas a los siguientes IEP, autorizados por ASFI:

1. Tarjetas de débito;

2. Tarjetas de crédito;

3. Tarjetas prepagadas.

qq. **Transferencia electrónica de información:** Forma de enviar, recibir o transferir en forma electrónica, datos, información, archivos y mensajes, entre otros;

rr. **Tecnología de la información (TI):** Conjunto de procesos y productos derivados de herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión de la información;

ss. **Transacción electrónica:** Comprende a todas aquellas operaciones realizadas por medios electrónicos que originen cargos o abonos de dinero en cuentas;

tt. **Usuario del sistema de información:** Persona identificada, autenticada y autorizada para utilizar un sistema de información. Ésta puede ser funcionario de la Entidad Supervisada (Usuario Interno del sistema de información) o cliente (Usuario Externo del sistema de información).

Artículo 4° - (Criterios de la seguridad de la información) La información que genera y administra la Entidad Supervisada, debe mantener un alto grado de seguridad, debiendo cumplir mínimamente los siguientes criterios:

a. **Autenticación:** Permite identificar al generador de la información y al usuario de la misma;

b. **Confiabilidad**: Busca proveer información apropiada, precisa y veraz, para el uso de las entidades supervisadas, tanto interna como externamente, que apoye el proceso de toma de decisiones;

c. **Confidencialidad**: Garantiza que la información se encuentra accesible únicamente para el personal autorizado;

d. **Cumplimiento**: Busca promover el acatamiento de las leyes, regulaciones y acuerdos contractuales a las que se encuentran sujetos los procesos que realiza la Entidad Supervisada;

e. **Disponibilidad**: Permite el acceso a la información en el tiempo y la forma que ésta sea requerida;

f. **Integridad**: Busca mantener con exactitud la información completa tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados;

g. **No repudio:** Condición que asegura que el emisor de una información no puede rechazar su transmisión o su contenido y/o que el receptor no pueda negar su recepción o su contenido.

SECCIÓN 2: PLANIFICACIÓN ESTRATÉGICA, ESTRUCTURA Y ORGANIZACIÓN DE LOS RECURSOS DE TECNOLOGÍAS DE LA INFORMACIÓN

Artículo 1° - (Planificación estratégica) La Entidad Supervisada debe desarrollar un Plan Estratégico de Tecnología(s) de la Información (TI), que esté alineado con la estrategia institucional y que considere su naturaleza, tamaño y estructura, así como la complejidad de los procesos y operaciones que realiza y los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuados. Este documento debe ser aprobado por su Directorio u Órgano equivalente.

El nivel ejecutivo de la Entidad Supervisada que sea responsable de TI, debe efectuar un seguimiento continuo de las tendencias tecnológicas, así como a las regulaciones emitidas por ASFI, de modo que éstas sean consideradas al momento de elaborar y actualizar la planificación estratégica del área de TI.

Artículo 2° - (Estrategia de seguridad de la información) La Entidad Supervisada como parte de su Plan Estratégico de TI, debe definir la estrategia de seguridad de la información, que le permita realizar una efectiva administración y control de la información.

Artículo 3° - (Infraestructura del área de tecnologías de la información) La infraestructura del área de Tecnologías de la Información debe ser consistente con la naturaleza, tamaño y estructura de la Entidad Supervisada, así como con la complejidad de los procesos y operaciones que realiza y los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuado.

Artículo 4° - (Estructura organizativa) La Entidad Supervisada, debe establecer una estructura organizativa adecuada al tamaño, volumen y complejidad de sus operaciones, que delimite las funciones y responsabilidades relativas a la gestión de los recursos de tecnología y seguridad de la información, aspectos que deben estar contemplados en un manual de organización y funciones, aprobados por su Directorio u Órgano equivalente.

Artículo 5° - (Comité de tecnologías de la información) Este Comité es responsable de establecer las políticas, procedimientos y prioridades para la administración de información y gestión de los recursos de TI.

El Comité de TI estará conformado al menos por un miembro del Directorio u Órgano equivalente, que será quien lo presida, el Gerente General, Ejecutivos y/o funcionarios responsables de las áreas de servicios tecnológicos y de las áreas usuarias del(los) sistema(s) de información de acuerdo al tema a ser tratado, cuyo funcionamiento se sujetará a su Reglamento.

El Comité de TI debe llevar un registro en actas de los temas y acuerdos tratados en sus reuniones.

Artículo 6° - (Comité operativo de tecnologías de la información) La Entidad Supervisada, de acuerdo a su estructura organizativa, debe conformar un Comité Operativo de Tecnologías de la Información, el cuál debe estar constituido por el nivel ejecutivo y los funcionarios encargados de las diferentes áreas que constituyen el área de TI. Este Comité estará encargado de coordinar el trabajo al interior de dicha área.

La frecuencia de las reuniones del Comité Operativo de TI estará sujeta a su Reglamento. Asimismo, las decisiones y acuerdos establecidos en dicho Comité deben registrarse en actas que deben ser archivadas.

Artículo 7° - (Responsable de la función de la seguridad de la información) Con el propósito de establecer los mecanismos para la administración y el control de la seguridad de los recursos de información, la Entidad Supervisada debe definir formalmente una instancia responsable que se encargue de dicha función, de acuerdo con la naturaleza, tamaño, volumen y complejidad de sus operaciones. Esta instancia puede corresponder a una Gerencia, Jefatura, Oficial o a un Comité constituido específicamente para tratar temas relacionados a la seguridad de la información.

La ubicación jerárquica de la instancia responsable de la seguridad de la información debe garantizar, su independencia funcional y operativa del (las) área(s) de tecnologías y sistemas de información, unidades operativas y de la función de auditoría.

Adicionalmente, el responsable de la función de la seguridad de la información gestionará con las instancias que correspondan en la Entidad Supervisada, la implementación, revisión, actualización y difusión de la Política de Seguridad de la Información (PSI), así como de la normativa que se desprende de la misma.

SECCIÓN 3: ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 1° - (Implementación del análisis y evaluación de riesgos en seguridad de la información) La Entidad Supervisada es responsable de efectuar un análisis y evaluación de riesgos en seguridad de la información, acorde a su naturaleza, tamaño y complejidad de operaciones, debiendo desarrollar e implementar procedimientos específicos para este propósito, los cuales deben estar formalmente establecidos.

El(los) resultado(s) obtenido(s) de dicho análisis y evaluación de riesgos en seguridad de la información, debe(n) estar contenido(s) en un informe elaborado por el Responsable de la función de la seguridad de la información, dirigido a la Gerencia General, para su posterior presentación al Directorio u Órgano equivalente.

El análisis y evaluación de riesgos en seguridad de la información, se constituye en un proceso continuo, por lo cual debe ser revisado y actualizado por lo menos una (1) vez al año.

Artículo 2° - (Política de seguridad de la información) De acuerdo con su estrategia de seguridad de la información y con los resultados de su análisis y evaluación de riesgos en seguridad de la información, la Entidad Supervisada debe tener formalizadas por escrito, actualizadas e implementadas la Política de Seguridad de la Información (PSI) así como la normativa que se desprende de la misma, aprobadas por el Directorio u Órgano equivalente.

La PSI así como la normativa que se desprende de la misma, deben ser publicadas y comunicadas a las diferentes instancias de la Entidad Supervisada, en forma entendible y accesible.

La Entidad Supervisada, al menos una (1) vez al año, debe revisar y actualizar la PSI así como la normativa que se desprende de la misma, considerando su naturaleza, tamaño, cambios y complejidad de sus operaciones, asegurando la correcta implementación de las mejores prácticas de seguridad de la información.

Artículo 3° - (Licencias de software) Todo software utilizado por la Entidad Supervisada debe contar con las licencias respectivas.

La Entidad Supervisada, debe definir los procedimientos necesarios para la instalación, mantenimiento y administración de software, así como para el control del estado y custodia de las licencias.

Artículo 4° - (Acuerdo de confidencialidad) Como parte de la obligación contractual, de los Directores, Consejeros de Administración y Vigilancia, Ejecutivos, demás funcionarios, consultores y personal eventual, éstos deben aceptar y firmar los términos y condiciones del contrato de empleo en el cual se establecerán sus obligaciones en cuanto a la seguridad de la información, entre las que se debe incluir el mantenimiento de la confidencialidad de la información a la que tengan acceso, inclusive después de la finalización de la relación contractual.

Artículo 5° - (Inventario de activos de información) La Entidad Supervisada debe contar con un inventario de los activos de información, permanentemente actualizado y asignar responsabilidades respecto a la protección de los mismos.

Asimismo, la entidad supervisada, debe remitir a ASFI, hasta el 31 de marzo de cada año, con corte al 31 de diciembre de la gestión pasada, el detalle del software que utiliza, de acuerdo al formato contenido en el Anexo 1: Inventario de Software, del presente Reglamento.

Artículo 6° - (Clasificación de la información) La Entidad Supervisada debe establecer un esquema de clasificación de la información, de acuerdo a la criticidad y sensibilidad de esta última, estableciendo adecuados derechos de acceso a los datos administrados en sus sistemas de información, así como a la documentación física. Esta clasificación debe ser documentada, formalizada y comunicada a todas las áreas involucradas.

Artículo 7° - (Propietarios de la información) Debe asignarse la propiedad de la información a un responsable de cargo jerárquico, de acuerdo al tipo de información y a las operaciones que desarrolla la Entidad Supervisada. Además, en coordinación con la instancia responsable de seguridad de la información deben definirse los controles de protección adecuados, de acuerdo con el nivel de clasificación otorgado a la información.

Artículo 8° - (Análisis de vulnerabilidades técnicas) La Entidad Supervisada es responsable de implementar una gestión de vulnerabilidades técnicas, a cuyo efecto debe contar con políticas y procedimientos formales que le permitan identificar su exposición a las mismas y adoptar las acciones preventivas y/o correctivas que correspondan, considerando los siguientes aspectos:

a. La evaluación de vulnerabilidades técnicas debe efectuarse por lo menos una (1) vez por año y ante un cambio en la infraestructura tecnológica. La ejecución de pruebas de seguridad debe considerar la realización de pruebas de intrusión controladas internas, externas o ambas de acuerdo con los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuado por la Entidad Supervisada;

b. El conjunto de políticas y procedimientos referido a la gestión de vulnerabilidades técnicas debe ser revisado y actualizado (si corresponde), por lo menos una (1) vez al año;

c. La Entidad Supervisada debe exigir a la(s) empresa(s) y/o persona(s) que le preste(n) servicios de evaluación de seguridad de la información, la respectiva documentación que acredite la experiencia necesaria para realizar este tipo de trabajos, adicionalmente debe(n) garantizar que el personal que realice las pruebas de intrusión controladas sea certificado y firme un acuerdo de confidencialidad conforme se establece en el Artículo 4° de la presente Sección;

d. El análisis de vulnerabilidades técnicas puede ser realizado por personal externo, interno o ambos, conforme con los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuado por la Entidad Supervisada. Al efecto, el personal interno asignado para esta tarea debe ser ajeno al (las) área(s) de tecnologías y sistemas de información.

Artículo 9° - (Clasificación de áreas de exclusión) La Entidad Supervisada debe identificar y clasificar las áreas de tecnologías de la información como áreas de exclusión que requieren medidas de protección y acceso restringido.

Artículo 10° - (Características del centro de procesamiento de datos) La Entidad Supervisada debe considerar los siguientes aspectos para la instalación del ambiente destinado al Centro de Procesamiento de Datos (CPD):

a. Ubicación del CPD al interior de la Entidad Supervisada;

b. Espacio acorde y suficiente para la cantidad de equipos instalados;

c. Energía regulada de acuerdo con los requerimientos de los equipos;

d. Cableado para el uso de los equipos de cómputo por medio de sistemas de ductos a través de piso o techo falso, de acuerdo con la necesidad de la Entidad Supervisada;

e. No almacenar papel u otros suministros inflamables y/o equipos en desuso dentro del CPD;

f. Instalación de los servidores y equipos de comunicación de forma independiente, debidamente asegurados, según corresponda.

Artículo 11° - (Manuales de procedimientos del centro de procesamiento de datos) La Entidad Supervisada debe contar con manuales de procedimientos para la gestión del (los) Centro(s) de Procesamiento de Datos, que consideren mínimamente, los siguientes aspectos:

a. Operación y mantenimiento;

b. Administración de accesos;

c. Pruebas a dispositivos de seguridad para garantizar su correcto funcionamiento.

Artículo 12° - (Protección de equipos) La Entidad Supervisada debe considerar que el Centro de Procesamiento de Datos debe contar al menos con los siguientes dispositivos:

a. Sistema de ventilación que mínimamente mantenga la temperatura y humedad en los niveles recomendados por los fabricantes de los equipos;

b. Extintores de incendios (manuales y/o automáticos) u otros dispositivos según las características de los equipos;

c. Detectores de temperatura y humedad;

d. Equipos que aseguren el suministro de energía regulada en forma ininterrumpida;

e. Mecanismos para el control de ingreso y salida del Centro de Procesamiento de Datos;

f. Vigilancia a través de cámaras de CCTV (Circuito Cerrado de TV).

Artículo 13° - (Suministro eléctrico) Para el funcionamiento de equipos informáticos, se debe utilizar una acometida eléctrica independiente del resto de la instalación, para evitar interferencias y posibles interrupciones. La capacidad de autonomía de los equipos de suministro ininterrumpido de energía, debe ser consistente con el Plan de Contingencias Tecnológicas y con el Plan de Continuidad del Negocio.

La Entidad Supervisada debe establecer mecanismos y destinar recursos para garantizar el suministro ininterrumpido de energía para el funcionamiento de equipos críticos y la prestación de servicios al público.

Artículo 14° - (Seguridad del cableado de red) El cableado utilizado para el transporte de datos de la Entidad Supervisada, debe cumplir con los estándares de cableado estructurado.

Artículo 15° - (Pruebas a dispositivos de seguridad) Los dispositivos de seguridad física detallados en el Artículo 12° de la presente Sección, deben ser probados al menos dos (2) veces por año, de tal forma que se garantice su correcto funcionamiento. La documentación que respalde la realización de estas pruebas debe estar disponible cuando ASFI la requiera.

Artículo 16° - (Responsabilidad en la gestión de seguridad de la información) La Entidad Supervisada debe realizar el control y cumplimiento de lo siguiente:

a. Las funciones y responsabilidades de los Directivos, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual deben ser definidas y documentadas en concordancia con la PSI y con la normativa que se desprende de la misma;

b. Asegurar que los Directivos, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual estén conscientes de las amenazas y riesgos de incidentes de seguridad de la información, así como que estén capacitados para aceptar y cumplir con la PSI y con la normativa que se desprende de la misma, en el desarrollo normal de su trabajo;

c. El establecimiento de un proceso disciplinario formal para Directivos, Consejeros, Ejecutivos y funcionarios que hubieran cometido faltas y/o violaciones a la PSI y/o a la normativa que se desprende de la misma, de la Entidad Supervisada;

d. La determinación en el contrato, de las sanciones para consultores y personal eventual que hubieran cometido faltas y/o violaciones a la PSI y/o a la normativa que se desprende de la misma, de la Entidad Supervisada.

Artículo 17° - (Custodia y conservación de datos) Los documentos relacionados con las operaciones, microfilmados o registrados en medios magnéticos y/o electrónicos, deben ser conservados y permanecer en custodia de la Entidad Supervisada, por un periodo no menor a diez (10) años.

La documentación que se constituya en instrumento probatorio en un proceso administrativo, judicial u otro, que se encuentre pendiente de resolución, no debe ser objeto de destrucción, en resguardo de los derechos de las partes en conflicto.

Artículo 18° - (Destrucción controlada de medios) La Entidad Supervisada debe establecer procedimientos para la destrucción controlada de los medios utilizados para el almacenamiento y respaldo de la información.

SECCIÓN 4: ADMINISTRACIÓN DEL CONTROL DE ACCESOS

Artículo 1° - (Administración de cuentas de usuarios) La instancia responsable de la Seguridad de la Información debe implementar procedimientos formalizados, acordes con la Política de Seguridad de la Información (PSI) y con la normativa que se desprende de la misma, respecto a la administración de usuarios de los sistemas de información, debiendo considerar al menos:

a. La administración de privilegios de acceso a sistemas y a la red de datos (alta, baja y/o modificación);

b. La creación, modificación o eliminación de cuentas de usuarios de los sistemas de información, debe contar con la autorización de la instancia correspondiente;

c. La gestión de perfiles de acceso debe realizarse de acuerdo con el principio de menor privilegio;

d. La administración y control de usuarios internos habilitados para navegación en la intranet e Internet;

e. La asignación de responsabilidad(es) sobre el hardware y software;

f. La administración de estaciones de trabajo o computadoras personales.

Artículo 2° - (Administración de privilegios) La Entidad Supervisada debe restringir y controlar el uso y asignación de privilegios para las cuentas de usuario y de administración de los sistemas de información, aplicaciones, sistemas operativos, bases de datos, intranet, Internet y otros servicios o componentes de comunicación. Dichas asignaciones, deben ser revisadas por lo menos una (1) vez al año, mediante un procedimiento formalmente establecido.

Los privilegios de acceso a la información y a los ambientes de procesamiento de información otorgados a los Directivos, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual, deben ser removidos a la culminación de su mandato, funciones, contrato o acuerdo y deben ser modificados en caso de cambio.

Artículo 3° - (Administración de contraseñas de usuarios) La Entidad Supervisada debe definir políticas de administración de contraseñas que respondan a los resultados de su análisis y evaluación de riesgos en seguridad de la información, así como a la clasificación de la información.

Artículo 4° - (Monitoreo de actividades de los usuarios) Para el monitoreo de las actividades de los usuarios de los sistemas de información, la Entidad Supervisada debe establecer un procedimiento formalizado, a efectos de detectar e identificar incidentes de seguridad de la información.

Artículo 5° - (Registros de seguridad y pistas de auditoría) Con el objeto de minimizar los riesgos internos y externos relacionados con accesos no autorizados, pérdidas y daños de la información, la Entidad Supervisada, con base en los resultados de su análisis y evaluación de riesgos en seguridad de la información, debe implementar pistas de auditoría que contengan los datos de los accesos y actividades de los usuarios, excepciones y registros de los incidentes de seguridad de la información.

SECCIÓN 5: DESARROLLO, MANTENIMIENTO E IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

Artículo 1° - (Políticas y procedimientos) La Entidad Supervisada debe establecer políticas y procedimientos, para el desarrollo, mantenimiento e implementación, de sistemas de información considerando las características propias relacionadas a las soluciones informáticas que requiere, así como los resultados de su análisis y evaluación de riesgos en seguridad de la información.

Artículo 2° - (Desarrollo y mantenimiento de programas, sistemas de información o aplicaciones informáticas) La Entidad Supervisada que realice el desarrollo o mantenimiento de programas, sistemas de información o aplicaciones informáticas, debe garantizar que su diseño e implementación se enmarque en la legislación y normativa vigente, según corresponda, así como en sus políticas internas.

Artículo 3° - (Requisitos de seguridad de los sistemas de información) La instancia responsable de la seguridad de la información de la Entidad Supervisada, debe velar por la inclusión en el diseño de los sistemas de información, de controles de seguridad, identificados y consensuados con las áreas involucradas.

Artículo 4° - (Estándares para el proceso de ingeniería del software) De acuerdo con la estructura y complejidad de sus operaciones, la Entidad Supervisada debe contar con metodologías estándar para el proceso de adquisición, desarrollo y mantenimiento del software, que comprendan aspectos tales como: estudio de factibilidad, análisis y especificaciones, diseño, desarrollo, pruebas, migración de datos preexistentes, implementación y mantenimiento de los sistemas de información.

Asimismo, acorde con los mencionados procesos, la Entidad Supervisada debe contar mínimamente con la siguiente documentación:

a. Diccionario de datos;

b. Diagramas de diseño (Entidad-Relación, Flujo de datos, entre otros);

c. Manual técnico;

d. Manual de usuario;

e. Documentación que especifique el flujo de la información entre los módulos y los sistemas.

Artículo 5° - (Integridad y validez de la información) La Entidad Supervisada para el desarrollo y mantenimiento de los sistemas de información, debe tomar en cuenta al menos los siguientes aspectos:

a. Implementar controles automatizados que permitan minimizar errores en la entrada de datos, en su procesamiento y consolidación, en la ejecución de los procesos de actualización de archivos y bases de datos, así como en la salida de la información;

b. Verificar periódicamente que la información procesada por los sistemas de información sea integra, válida, confiable y razonable;

c. Establecer controles que limiten la modificación y la eliminación de datos en cuanto a movimientos, saldos y operaciones efectuadas por los clientes y otros.

Artículo 6° - (Controles criptográficos) En el desarrollo de los sistemas de información, la Entidad Supervisada debe implementar métodos de cifrado estándar que garanticen la confidencialidad e integridad de la información.

Artículo 7° - (Control de acceso al código fuente de los programas) El acceso al código fuente de programas y a la información relacionada con diseños, especificaciones, planes de verificación y de validación, debe ser estrictamente controlado para prevenir la introducción de funcionalidades y/o cambios no autorizados.

Artículo 8° - (Procedimientos de control de cambios) La Entidad Supervisada debe establecer procedimientos formales para el control de cambios en los sistemas de información que contemplen documentación, especificación, prueba, control de calidad e implementación. Se debe documentar y resguardar cada versión del código fuente de los sistemas de información, así como la estructura de datos anterior.

Artículo 9° - (Ambientes de desarrollo, prueba y producción) Se deben implementar controles y mecanismos que garanticen la separación física o lógica de los ambientes de desarrollo, prueba y producción, acordes con la criticidad del (los) sistema(s) involucrado(s) y la segregación de funciones que debe existir en cada caso, asegurando que los encargados del desarrollo y/o mantenimiento de sistemas no tengan acceso a los sistemas y datos en producción; así como, que las pruebas a los sistemas, previo a su uso oficial, se realicen en un entorno controlado.

Cuando las características de la Entidad Supervisada, determinen que no se pueda aplicar la segregación de funciones citada en el párrafo precedente, la Gerencia General debe autorizar de manera expresa, el acceso de los funcionarios del área de TI a los datos en producción, dicha autorización permanecerá en la Entidad Supervisada a disposición de ASFI.

La instancia responsable de la seguridad de la información de la Entidad Supervisada, a efectos de garantizar que el acceso citado en el párrafo precedente, no es utilizado para fines diferentes a los autorizados, debe realizar el seguimiento correspondiente.

Artículo 10° - (Datos de prueba en ambientes de desarrollo) Para utilizar información de producción en los ambientes de desarrollo y prueba se debe aplicar un procedimiento de enmascaramiento de datos a efectos de preservar la confidencialidad de dicha información.

Artículo 11° - (Migración de sistemas de información) El proceso de migración de un sistema de información, debe estar basado en un plan de acción y procedimientos específicos que garanticen la disponibilidad, integridad y confidencialidad de la información.

Es responsabilidad de la Gerencia General designar a la instancia que realizará el control de calidad durante el proceso de migración, el cual debe estar debidamente documentado y a disposición de ASFI.

El Auditor Interno o la Unidad de Auditoría Interna, según corresponda, deben evaluar los resultados obtenidos en el proceso de migración, cuyo informe permanecerá en la Entidad Supervisada a disposición de ASFI.

Artículo 12° - (Parches de seguridad) La actualización del software o la aplicación de un parche de seguridad, debe ser previamente autorizada en función a un procedimiento formalmente establecido. Esta autorización debe ser otorgada o no, según corresponda, considerando la estabilidad del sistema, las necesidades funcionales de la organización y los criterios de seguridad de la información establecidos en las políticas de la Entidad Supervisada. Adicionalmente, todo el software debe mantenerse actualizado con las mejoras de seguridad distribuidas o liberadas por el proveedor, previa realización de pruebas en ambientes controlados.

SECCIÓN 6: GESTIÓN DE OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN

Artículo 1° - (Gestión de operaciones) La gestión de operaciones de tecnología de la información, debe estar basada en políticas y procedimientos establecidos por la Entidad Supervisada, en las cuales se consideren al menos:

a. La planificación y documentación de los procesos y actividades que se desarrollen dentro del Centro de Procesamiento de Datos;

b. La revisión periódica de los procedimientos relacionados a la gestión de operaciones en función a los cambios operativos y/o tecnológicos.

Artículo 2° - (Administración de las bases de datos) La Entidad Supervisada debe realizar la administración de bases de datos, en función a procedimientos formalmente establecidos para este propósito, los cuales consideren mínimamente lo siguiente:

a. Instalación, administración, migración y mantenimiento de las bases de datos;

b. Definición de la arquitectura de información para organizar y aprovechar de la mejor forma los sistemas de información;

c. Establecimiento de mecanismos de control de acceso a las bases de datos;

d. Documentación que respalde las actividades de administración de las bases de datos;

e. Realización de estudios de capacidad y desempeño de las bases de datos que permitan determinar las necesidades de expansión de capacidades y/o la afinación en forma oportuna.

Artículo 3° - (Respaldo o copia de seguridad) La Entidad Supervisada debe efectuar copias de seguridad de todos los datos e información, necesarios para el continuo funcionamiento de la misma, cumpliendo al menos con las siguientes disposiciones:

a. Contar con políticas y procedimientos que aseguren la realización de copias de seguridad;

b. La información respaldada debe poseer un nivel adecuado de protección lógica, física y ambiental, en función a la criticidad de la misma;

c. Los medios de respaldo deben probarse periódicamente, a fin de garantizar la confiabilidad de los mismos con relación a su eventual uso en casos de emergencia, dichas pruebas deben ser documentadas y efectuadas en los periodos definidos por la instancia responsable de la seguridad de la información;

d. El ambiente físico destinado al resguardo de la información crítica, debe contar con condiciones físicas y ambientales suficientes para garantizar mínimamente la protección contra daños, deterioro y hurto;

e. El sitio externo de respaldo donde se almacenan las copias de seguridad debe mantener al menos diez (10) años de información crítica de la Entidad Supervisada;

f. Cualquier traslado físico de los medios digitales de respaldo, debe realizarse con controles de seguridad adecuados, que eviten una exposición no autorizada de la información contenida en los mismos;

g. Se debe realizar el etiquetado de todos los medios de respaldo y mantener un inventario actualizado de los mismos.

Artículo 4° - (Mantenimiento preventivo de los recursos tecnológicos) La Entidad Supervisada debe realizar periódicamente el mantenimiento preventivo de los recursos tecnológicos que soportan los sistemas de información y de los recursos relacionados, mediante el establecimiento formal y documentado de un procedimiento que incluya el cronograma correspondiente.

SECCIÓN 7: GESTIÓN DE SEGURIDAD EN REDES Y COMUNICACIONES

Artículo 1° - (Políticas y procedimientos) La Entidad Supervisada debe contar con políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base, con el propósito de asegurar que proporcionen la plataforma tecnológica que permita soportar las aplicaciones relacionadas con las redes y telecomunicaciones y minimicen la frecuencia e impacto de las fallas de desempeño de las mismas.

Asimismo, debe desarrollar políticas y procedimientos para la correcta administración de la infraestructura de redes y telecomunicaciones. Para este efecto, la Entidad Supervisada debe considerar lo siguiente:

a. Garantizar que los planes de adquisición de hardware y software reflejen las necesidades identificadas en el Plan Estratégico de TI;

b. Garantizar la protección de los datos que se trasmiten a través de la red de telecomunicaciones, mediante técnicas de cifrado estándar a través de equipos o aplicaciones definidas para tal fin;

c. Asegurar que las redes de voz y/o datos cumplan con estándares de cableado estructurado;

d. Definir los niveles de acceso de los usuarios del sistema de información a las redes y servicios de red, en función de las autorizaciones predefinidas;

e. Controlar el acceso a los puertos de diagnóstico;

f. Establecer controles de acceso para redes compartidas, particularmente respecto a aquellas que se extienden a usuarios fuera de la Entidad Supervisada.

Artículo 2° - (Estudio de capacidad y desempeño) La Entidad Supervisada debe realizar estudios periódicos de capacidad y desempeño del hardware y de las líneas de comunicación que permitan determinar las necesidades de expansión de capacidades y/o actualización de equipos en forma oportuna.

Artículo 3° - (Exclusividad del área de telecomunicaciones) El ambiente físico en el que se encuentran instalados los equipos de telecomunicaciones debe ser de uso exclusivo para el fin señalado, con excepción del destinado a los equipos de seguridad o procesamiento de información.

Artículo 4° - (Activos de información componentes de la red) Los equipos como concentradores, multiplexores, puentes, cortafuegos (f*irewall*), enrutadores, conmutadores y componentes del cableado estructurado de la red, deben instalarse sobre estructuras dedicadas para equipos de telecomunicación.

Artículo 5° - (Configuración de hardware y software) La Entidad Supervisada, debe establecer un registro formal que contenga toda la información referente a los elementos de configuración del hardware, software, parámetros, documentación, procedimientos y herramientas para operar, acceder y utilizar los sistemas de información. Asimismo, debe considerar los siguientes aspectos:

a. Contar con procedimientos formalmente establecidos para: Identificar, registrar y actualizar los elementos de configuración existentes en el repositorio de configuraciones;

b. Revisar y verificar por lo menos una (1) vez al año, el estado de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica;

c. Revisar mínimamente una (1) vez al año, la existencia de cualquier software de uso personal o no autorizado, que no se encuentre incluido en los acuerdos de licenciamiento vigentes de la Entidad Supervisada.

Artículo 6° - (Documentación técnica) La documentación técnica asociada a la infraestructura de redes y telecomunicaciones debe conservarse actualizada, resguardada y contener como mínimo lo siguiente:

a. Características, topología y diagrama de red;

b. Descripción de los elementos de cableado;

c. Planos de trayectoria del cableado y ubicación de puntos de salida;

d. Diagrama del sistema de interconexión de cables de red, distribución de regletas y salidas;

e. Certificación del cableado estructurado de la red.

SECCIÓN 8: GESTIÓN DE SEGURIDAD EN TRANSFERENCIAS Y TRANSACCIONES ELECTRÓNICAS

Artículo 1° - (Requisitos de los sistemas de transferencias y transacciones electrónicas) Para habilitar un sistema de transferencia electrónica de información o transacciones electrónicas mediante banca electrónica o servicios de pago móvil, la Entidad Supervisada debe adquirir e implementar los elementos de hardware y software necesarios para la protección y control de su plataforma tecnológica. Asimismo, debe cumplir con los siguientes requisitos mínimos:

a. **Seguridad del sistema:** El sistema tiene que proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, resguardando además, la confidencialidad de la información transmitida o procesada por ese medio.

Dicho sistema, debe contener los mecanismos físicos y lógicos de seguridad para controlar y detectar cualquier alteración o intervención a la información transmitida, entre el punto en que ésta se origina y aquel en el que es recibida por el destinatario.

Los procedimientos en este ámbito, deben asegurar que tanto el originador como el destinatario, en su caso, conozcan la autoría de las transacciones o mensajes y la conformidad de su recepción, aplicando la(s) política(s) de seguridad de la información indicada(s) en el Artículo 2° de la Sección 3 del presente Reglamento, incluyendo métodos de cifrado estándar de datos, que permitan asegurar su confiabilidad, no repudio, autenticidad e integridad.

La Entidad Supervisada, es responsable de implementar mecanismos de control de acceso y/o contraseñas adicionales para los clientes, así como de autenticación robusta para aquellas transacciones que sean realizadas a través de Internet, caso contrario no se podrá atribuir ninguna responsabilidad a un usuario del sistema en el caso de que se materialice un fraude a través de estos sistemas de transacciones y transferencias electrónicas.

El mecanismo de acceso y/o contraseña al (los) sistema(s) vía web debe ser diferente al mecanismo que permita realizar transacciones y/o transferencias electrónicas;

b. **Canal de comunicación:** La Entidad Supervisada debe mantener permanentemente abierto y disponible un canal de comunicación que permita al cliente realizar consultas y solicitar el bloqueo de cualquier operación que intente efectuarse utilizando sus medios de acceso al sistema de información o claves de autenticación. Cada sistema que opere en línea y en tiempo real, debe permitir dicho bloqueo también en tiempo real.

Toda información relacionada a transferencia y transacciones electrónicas, debe contemplar en los canales de comunicación mecanismos de cifrado estándar durante todo el flujo operativo de los sistemas de información tanto al interior como al exterior de la Entidad Supervisada;

c. **Difusión de políticas de seguridad:** La Entidad Supervisada debe difundir sus políticas de seguridad relativas al tema de transferencias y transacciones electrónicas tanto al interior de la misma, como a los clientes externos que utilizan dichos sistemas;

d. **Certificación digital:** Los certificados digitales que utilice la Entidad Supervisada, así como la existencia de sitios web de ésta, tienen que estar avalados en cuanto a su propiedad y seguridad de la información expuesta, por una entidad certificadora autorizada por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT);

e. **Continuidad operativa:** La Entidad Supervisada, debe contar con procesos alternativos que puedan asegurar la continuidad de todos los procesos definidos como críticos relacionados con los servicios de transferencias y transacciones electrónicas. En este sentido, las instalaciones y configuraciones de los equipos, sistemas y las redes de telecomunicaciones deben garantizar la continuidad de las operaciones frente a eventos fortuitos o deliberados, para lo cual se debe considerar lo previsto en la Sección 10, del presente Reglamento;

f. **Disponibilidad de la información:** Los sistemas de transacción y transferencia electrónica deben generar la información necesaria para que el cliente pueda conciliar los movimientos efectuados en su(s) cuenta(s), a través de terminales ATM y POS, así como de los sistemas disponibles en la web, en un determinado período, reflejando las fechas en que se realizaron las transacciones;

g. **Registro de pistas de auditoría:** Los sistemas utilizados, además de permitir el registro y seguimiento íntegro de las transferencias y/o transacciones electrónicas realizadas, deben generar 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 operadores, emisores y receptores, cuentas y montos involucrados, así como la identificación de terminales desde las cuales se realizaron.

La conservación de esta información debe efectuarse, por un periodo no menor a diez (10) años;

h. **Verificación y control de transacciones y transferencias electrónicas:** La Entidad Supervisada debe implementar mínimamente las siguientes medidas de seguridad:

1. Regionalización de las operaciones electrónicas nacionales e internacionales para los clientes;

2. Fijar límites monetarios en transferencias y transacciones electrónicas;

3. Detección, alerta y si corresponde, bloqueo automatizado de operaciones sospechosas de fraude.

i. **Acuerdos privados**: Para la realización de transacciones y/o transferencias de información entre entidades supervisadas, BCB, ASFI, usuarios y todas las que estén relacionadas con la actividad de intermediación financiera, deben celebrarse acuerdos privados que estén debidamente firmados y protocolizados, que consideren las políticas de seguridad establecidas a partir de lo dispuesto en el Artículo 2° de la Sección 3 del presente reglamento.

Artículo 2° - (Contrato) Los derechos y responsabilidades de cada una de las partes que intervienen en las transacciones y/o transferencias electrónicas, deben establecerse claramente en

el contrato que éstas suscriban para el efecto. De manera enunciativa, dicho contrato debe especificar mínimamente los siguientes aspectos:

a. Responsabilidad exclusiva del cliente, del uso y confidencialidad de la clave de acceso, que utilizará en sus operaciones electrónicas, señalando explícitamente que la contraseña será bloqueada automáticamente después de tres intentos fallidos, así como el procedimiento para solicitar su desbloqueo;

b. Detalle de las operaciones que puede efectuar el cliente;

c. El horario de prestación del servicio, conjuntamente el procedimiento alternativo en caso de que el servicio no esté disponible;

d. Las medidas de seguridad que ha tomado la Entidad Supervisada para la transferencia electrónica de información y transacciones electrónicas efectuadas;

e. Los medios o mecanismos electrónicos que permitan reconocer la validez de las transferencias y/o transacciones electrónicas que el cliente realice, así como la implementación de controles internos que posibiliten establecer que los importes no superen el saldo disponible;

f. El límite fijado para la realización de las transferencias y/o transacciones electrónicas, salvo la existencia previa de contratos de anticipo o adelanto en cuenta, debiendo cumplir para tal efecto con las formalidades del Código de Comercio y reglamentación vigente;

g. Detección, alerta y si corresponde, bloqueo automatizado de operaciones sospechosas de fraude;

h. Todas las condiciones, características y cualquier otra estipulación determinante que conlleve el uso de este servicio.

Artículo 3° - (Cifrado de mensajes y archivos) Para que la Entidad Supervisada, efectúe transferencias y/o transacciones electrónicas de fondos, debe tener implementado un sistema de cifrado estándar que garantice como mínimo que las operaciones realizadas por los usuarios internos o externos de los sistemas de información sean efectuadas en un ambiente seguro y no puedan ser observadas por usuarios no autorizados.

SECCIÓN 9: GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Artículo Único - (Gestión de incidentes de seguridad de la información) La Entidad Supervisada debe tener un procedimiento para la gestión de incidentes de seguridad de la información formalizado, actualizado e implementado; aprobado por el Directorio u Órgano equivalente, en concordancia con el Plan de Contingencias Tecnológicas establecido en el Artículo 1°, Sección 10 del presente Reglamento, el cual debe especificar mínimamente lo siguiente:

a. **Responsabilidades y procedimientos:** La Gerencia General debe establecer formalmente las responsabilidades y procedimientos para asegurar una rápida, efectiva y ordenada respuesta a los incidentes de seguridad de la información;

b. **Registro, cuantificación y monitoreo de incidentes de seguridad de la información:** La Entidad Supervisada debe establecer los mecanismos necesarios que permitan identificar la tipología, los volúmenes y los costos de los incidentes de seguridad de la información, así como las medidas asumidas para mitigarlos, garantizando que éstos sean registrados, cuantificados y monitoreados. De igual manera, debe ejecutar las acciones correctivas oportunas;

c. **Clasificación de incidentes de seguridad de la información:** La Entidad Supervisada debe considerar al menos las siguientes categorías:

1. Pérdida de servicio;

2. Pérdida de equipo o instalaciones;

3. Sobrecargo o mal funcionamiento del sistema;

4. Errores humanos;

5. Incumplimiento de políticas o procedimientos;

6. Deficiencias de controles de seguridad física;

7. Cambios incontrolables en el sistema;

8. Mal funcionamiento del software;

9. Mal funcionamiento del hardware;

10. Código malicioso;

11. Negación de servicio;

12. Errores resultantes de datos incompletos o no actualizados;

13. Violaciones en la confidencialidad e integridad de la información;

14. Mal uso de los sistemas de información;

15. Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos;

16. Intentos recurrentes y no recurrentes de acceso no autorizado.

d. Registro de incidentes de seguridad de la información: La Entidad Supervisada para efectos de control, seguimiento y solución, debe mantener una base de datos para el registro de los incidentes de seguridad de la información que considere la clasificación establecida en el inciso c del presente Artículo.

SECCIÓN 10: CONTINUIDAD DEL NEGOCIO

Artículo 1° - (Plan de contingencias tecnológicas) La Entidad Supervisada debe contar con un Plan de Contingencias Tecnológicas formalizado, actualizado e implementado; aprobado por el Directorio u Órgano equivalente, que mínimamente considere:

a. Objetivo;

b. Metodología para su elaboración que al menos, contemple lo siguiente:

1. Análisis y evaluación de riesgos en seguridad de la información;

2. Definición de eventos que afecten la operación de los sistemas de información;

3. Definición de procesos críticos relacionados a los sistemas de información.

c. Procedimientos de recuperación de operaciones críticas para cada evento identificado;

d. Descripción de responsabilidades, funciones e identificación del personal que ejecutará el plan;

e. Medidas de prevención;

f. Recursos mínimos asignados para la recuperación de los servicios y sistemas;

g. Convenios realizados para la recuperación de los servicios y sistemas;

h. Revisión anual y evaluaciones frecuentes del Plan de Contingencias Tecnológicas de acuerdo con los resultados del análisis y evaluación de riesgos en seguridad de la información realizado y/o los incidentes de seguridad de información acontecidos;

i. Pruebas al Plan de Contingencias Tecnológicas;

j. Situaciones no cubiertas y supuestos.

Artículo 2° - (Plan de continuidad del negocio) La Entidad Supervisada debe contar con un Plan de Continuidad del Negocio (BCP) formalizado, actualizado e implementado; aprobado por el Directorio u Órgano equivalente, que mínimamente considere:

a. Inicio del proyecto;

b. Los resultados del Análisis y evaluación de riesgos en seguridad de la información, efectuado;

c. Análisis de impacto al negocio (BIA);

d. Desarrollo de estrategias para el BCP;

e. Respuesta ante emergencias;

f. Desarrollo e implementación del BCP;

g. Programa de concientización y capacitación;

h. Mantenimiento y ejercicio del BCP;

i. Comunicación de crisis.

Artículo 3° - (Capacitación en la aplicación de los planes de contingencias tecnológicas y de continuidad del negocio) La Entidad Supervisada debe asegurarse que todas las partes involucradas en los planes de contingencias tecnológicas y de continuidad del negocio, asistan de forma regular a sesiones de capacitación respecto a los procesos, sus roles y responsabilidades en caso de presentarse algún incidente de seguridad de la información.

Artículo 4° - (Pruebas de los planes de contingencias tecnológicas y continuidad del negocio) La Entidad Supervisada debe efectuar al menos una (1) prueba al año de cada escenario o evento considerado en los planes de contingencias tecnológicas y continuidad del negocio, debiendo los resultados de ambas pruebas ser exitosas en toda su dimensión, caso contrario se deben ejecutar las acciones correctivas que correspondan y ejecutar las pruebas necesarias hasta cumplir con el objetivo planteado.

La Entidad Supervisada debe documentar la realización de las pruebas y la implementación de los planes de acción correctivos o preventivos que correspondan. El cronograma de realización de pruebas, conforme a los planes de contingencias tecnológicas y de continuidad del negocio para la gestión que se planifica, debe ser aprobado por el Directorio u Órgano equivalente, hasta el 20 de diciembre del año anterior a su ejecución y permanecer en la entidad supervisada a disposición de ASFI, para ser presentado cuando ésta así lo requiera.

El alcance de las pruebas de contingencias tecnológicas y de continuidad del negocio, debe considerar aplicaciones individuales, escenarios de prueba integrados, pruebas de punta a punta y pruebas integradas con el(los) proveedor(es). El resultado de éstas debe estar disponible para ASFI.

Artículo 5° - (Control de los planes de contingencias tecnológicas y de continuidad del negocio) La Entidad Supervisada a través de los funcionarios involucrados en las pruebas y ejecución de los planes de contingencias tecnológicas y de continuidad del negocio, es responsable de mantener los niveles de seguridad definidos para cada etapa del mismo.

Artículo 6° - (Establecimiento del centro de procesamiento de datos alterno) La Entidad Supervisada debe contar con un mecanismo alterno de procesamiento de información que sea consistente con su naturaleza y tamaño, acorde con los resultados de su análisis y evaluación de riesgos en seguridad de la información y con la criticidad de sus operaciones, el cual le permita dar continuidad a los servicios que ofrece. En caso de ocurrir una contingencia que interrumpa las operaciones del Centro de Procesamiento de Datos principal (CPD), el Centro de Procesamiento de Datos Alterno (CPDA) deberá funcionar hasta que se resuelva la contingencia.

Cuando la Entidad Supervisada por sus características, no cuente con ambientes para la instalación del CPDA, en una ubicación geográfica diferente a aquella en la que se encuentra el CPD, puede hacerlo en un espacio donde no preste servicios, localizado en otra área geográfica, preservando que cumpla con los requisitos de seguridad física y tecnológica que deben tener las áreas de exclusión.

SECCIÓN 11: ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS RELACIONADOS CON TECNOLOGÍA DE LA INFORMACIÓN

Artículo 1° - (Administración de servicios y contratos con terceros) La Entidad Supervisada debe contar con políticas y procedimientos para la administración de servicios y contratos con terceros, con el propósito de asegurar que los servicios contratados sean provistos en el marco de un adecuado nivel de servicios que minimicen el riesgo relacionado y se enmarquen en las disposiciones contenidas en el presente Reglamento según corresponda.

La Gerencia General debe establecer formalmente las responsabilidades y procedimientos para la administración de servicios y contratos con terceros.

Artículo 2° - (Evaluación y selección de proveedores) Para la contratación de proveedores de tecnología de información, la Entidad Supervisada debe poseer un procedimiento documentado, formalizado, actualizado e implementado; aprobado por el Directorio u Órgano equivalente, para realizar la evaluación y selección de los mismos, previo a proceder con su contratación.

Artículo 3° - (Procesamiento de datos tercerizado o ejecución de sistemas en lugar externo) Para la contratación de empresas encargadas del procesamiento de datos o ejecución de sistemas en lugar externo, la Entidad Supervisada debe considerar al menos los siguientes aspectos:

a. Es deber del Directorio u Órgano equivalente, Gerencia General y demás administradores responsables, asegurarse que la empresa proveedora cuente con la experiencia y capacidad necesarias para el procesamiento de datos relacionados al giro de la Entidad Supervisada y que respondan a las características del servicio que se desea contratar;

b. La infraestructura tecnológica y los sistemas que se utilizarán para la comunicación, almacenamiento y procesamiento de datos, deben ofrecer la seguridad suficiente para resguardar permanentemente la continuidad operacional, la confidencialidad, integridad, exactitud y calidad de la información y los datos. Asimismo, se debe verificar que éstos garanticen la obtención oportuna de cualquier dato o información necesarios para cumplir con los fines de la Entidad Supervisada o con los requerimientos de las autoridades competentes, como es el caso de la información que en cualquier momento puede solicitar ASFI;

c. Es responsabilidad de la Entidad Supervisada, verificar y exigir al proveedor de tecnología de la información el cumplimiento de las políticas y procedimientos de seguridad de la información correspondientes;

d. Es responsabilidad de la Entidad Supervisada, asegurar la adopción de medidas necesarias que garanticen la continuidad operacional del procesamiento de datos, en caso de cambio de proveedor externo u otro factor no previsto;

e. En caso de que el procesamiento de datos se realice fuera del territorio nacional, la Entidad Supervisada debe comunicar esta situación a ASFI, adjuntando la siguiente documentación:

1. Detalle de las actividades descentralizadas;

2. Descripción del entorno de procesamiento;

3. Lista de encargados del procesamiento;

4. Responsables del control de procesamiento;

5. Informe del Gerente General, dirigido al Directorio u Órgano equivalente, que señale el cumplimiento de lo dispuesto en los incisos precedentes.

Dicha documentación debe permanecer actualizada en la Entidad Supervisada, a disposición de ASFI;

f. El Gerente General de la entidad supervisada, hasta el 31 de marzo de cada año, debe presentar al Directorio u Órgano Equivalente, un informe con carácter de declaración jurada refrendado por el Auditor Interno, detallando los servicios de procesamiento de datos o ejecución de sistemas a cargo de terceros, indicando el nombre de cada uno de sus proveedores.

Asimismo, el mencionado informe deberá especificar que los servicios prestados por los proveedores que no cuentan con licencia de funcionamiento otorgada por ASFI, cumplen con los criterios de seguridad de la información establecidos en el Artículo 4° de la Sección 1 del presente Reglamento.

El citado Informe permanecerá en la Entidad Supervisada para su presentación a ASFI, cuando ésta así lo requiera.

Artículo 4° - (Contrato con proveedor de procesamiento externo) Es responsabilidad del Directorio u Órgano equivalente y de la Gerencia General de la Entidad Supervisada, la suscripción del (los) contrato(s) con la(s) empresa(s) proveedora(s) de los servicios de procesamiento, el (los) que entre otros aspectos debe(n) precisar mínimamente, lo siguiente:

a. La naturaleza y especificaciones del (los) servicio(s) de procesamiento contratado(s);

b. La responsabilidad que asume(n) la(s) empresa(s) proveedora(s), para mantener políticas y procedimientos que garanticen la seguridad, reserva y confidencialidad de la información, en conformidad con la legislación boliviana, así como de prever pérdidas, no disponibilidad o deterioros de la misma;

c. La responsabilidad que asume(n) la(s) empresa(s) proveedora(s) en caso de ser vulnerados sus sistemas, ya sea por ataques informáticos internos y/o externos, deficiencias en la parametrización, configuración y/o rutinas de validación inmersas en el código fuente;

d. La facultad de la Entidad Supervisada, para practicar evaluaciones periódicas a la(s) empresa(s) proveedora(s) del servicio, directamente o mediante auditorías independientes.

La Entidad Supervisada debe mantener los documentos y antecedentes de los contratos suscritos con empresas proveedoras de servicios de tecnología(s) de información a disposición de ASFI.

Artículo 5° - (Adquisición de sistemas de información) La Entidad Supervisada debe evaluar la necesidad de adquirir programas, sistemas o aplicaciones en forma previa a la adquisición, con base en un análisis que considere como mínimo lo siguiente:

a. Fuentes alternativas para la compra;

b. Revisión de la factibilidad tecnológica y económica;

c. Análisis y evaluación de riesgos en seguridad de la información;

d. Análisis de costo-beneficio;

e. Método de selección del proveedor, que permita un nivel de dependencia aceptable;

f. Disponibilidad del código fuente;

g. Cumplimiento de los requisitos de seguridad de la información establecidos por la Entidad Supervisada.

Si la funcionalidad del (los) producto(s) ofrecido(s), no satisface(n) los requisitos de seguridad de la información establecidos por la Entidad Supervisada, se deben reconsiderar los riesgos y controles asociados, previo a la adquisición del (los) producto(s).

Artículo 6° - (Desarrollo y mantenimiento de programas, sistemas o aplicaciones a través de terceros) La contratación de empresas encargadas del desarrollo y mantenimiento de sistemas de información, es responsabilidad de la Entidad Supervisada que al efecto, debe considerar al menos los siguientes aspectos:

a. Que la(s) empresa(s) contratada(s) cuente(n) con solidez financiera, personal con conocimiento y experiencia en el desarrollo de sistemas y/o en servicios relacionados al giro de la Entidad Supervisada. Asimismo, asegurar que sus sistemas de control interno y procedimientos de seguridad de la información, responden a las características del servicio que se requiere contratar;

b. Que la infraestructura tecnológica, sistemas operativos y las herramientas de desarrollo, que se utilizarán, estén debidamente licenciados por el fabricante o su representante;

c. La adopción de medidas que garanticen la continuidad del desarrollo y mantenimiento de sistemas, en caso de cambio de proveedor u otro factor no previsto;

d. Que el(los) proveedor(es) de tecnologías de información cumpla(n) con las directrices de seguridad de la información señalados en el Artículo 1° de la presente Sección;

e. Requisitos de seguridad establecidos por la Entidad Supervisada.

Artículo 7° - (Contrato con empresas encargadas del desarrollo y mantenimiento de programas, sistemas o aplicaciones) El contrato con empresas de desarrollo externo debe contener como mínimo, cláusulas destinadas a:

a. Aclarar a quien pertenece la propiedad intelectual en el caso de desarrollo de programas, sistemas o aplicaciones;

b. Indicar en detalle la plataforma de desarrollo, servidores, sistemas operativos y las herramientas de desarrollo, tales como lenguaje(s) de programación y sistema(s) de gestión de base de datos;

c. Especificar que el proveedor debe tener el contrato del personal que participa en el proyecto, actualizado y con cláusulas de confidencialidad para el manejo de la información. Adicionalmente, debe enviar al cliente –entidad supervisada– el currículo de todos los participantes en el proyecto, indicando al menos antecedentes profesionales y personales;

d. Indicar los tiempos de desarrollo por cada etapa en un cronograma y plan de trabajo, incluyendo las pruebas de programas;

e. Con la finalidad de proteger a la Entidad Supervisada, junto a las cláusulas normales de condiciones de pago se deben establecer multas por atrasos en la entrega de productos o provisión de servicios. Al mismo tiempo, indemnización por daños y perjuicios atribuibles al proveedor;

f. Establecer que en caso de que el proveedor sea autorizado a ingresar en forma remota a los servidores de la Entidad Supervisada, debe regirse y cumplir las políticas y procedimientos de la misma en lo referido a la seguridad de la información;

g. Al término del proyecto, al adquirir un producto previamente desarrollado y/o cuando el proveedor no esté en disponibilidad de continuar operando en el mercado, la Entidad Supervisada debe asegurarse el acceso oportuno al código fuente de los programas;

h. Garantizar que, en concordancia con los cambios realizados al sistema de información, programa o aplicación, el proveedor actualice y entregue mínimamente la siguiente documentación:

1. Diccionario de datos;

2. Diagramas de diseño (Entidad Relación, Flujo de datos, entre otros);

3. Manual técnico;

4. Manual de usuario;

5. Documentación que especifique el flujo de la información entre los módulos y los sistemas.

Artículo 8° - (Otros servicios) La Entidad Supervisada podrá tercerizar otros servicios como el mantenimiento de equipos, soporte de sistemas operativos, hospedaje de sitios web, a cuyo efecto debe incluir en su(s) contrato(s) o acuerdo(s) al menos los siguientes aspectos:

a. Tipo de servicio;

b. Soporte y asistencia;

c. Seguridad de datos;

d. Garantía y tiempos de respuesta del servicio;

e. Disponibilidad del servicio;

f. Multas por incumplimiento.

Artículo 9° - (Acuerdo de nivel de servicio) La Entidad Supervisada, de forma previa a la contratación de un proveedor externo de tecnología de información, debe establecer un Acuerdo de Nivel de Servicio (SLA), documento que será parte del contrato respectivo, acorde con los resultados de su análisis y evaluación de riesgos en seguridad de la información y con la criticidad de sus operaciones.

Los parámetros del SLA, deben referirse al tipo de servicio, soporte y asistencia a clientes, provisiones para seguridad y datos, garantías del sistema y tiempos de respuesta, disponibilidad del servicio o sistema, conectividad, multas por caída del sistema y/o líneas alternas para el servicio, según corresponda.

Artículo 10° - (Servicio de computación en la nube) La Entidad Supervisada, previo a la contratación de servicio(s) de computación en la nube, debe solicitar la no objeción a ASFI en forma escrita, adjuntando para su evaluación el "Proyecto de implementación del servicio de computación en la nube", el cual tiene que reflejar mínimamente, el cumplimiento de los siguientes aspectos:

a. Que no se vulnerará el Derecho a la Reserva y Confidencialidad, establecida en el Artículo 472 de la Ley N°393 de Servicios Financieros;

b. Que no se encuentra dentro de las Limitaciones y Prohibiciones, establecidas en los Títulos II, III y IV de la Ley N°393 de Servicios Financieros, referidos a "Servicios Financieros y Régimen de Autorizaciones", que pueden realizar las entidades supervisadas por ASFI;

c. Que el proveedor del servicio cumpla con los requisitos de seguridad de la información dispuestos en el presente Reglamento;

d. Que el proveedor del servicio cumpla con la normativa y legislación del Estado Plurinacional de Bolivia, existiendo la posibilidad de poder ser examinado por ASFI y/o empresas de auditoría externa bolivianas;

e. Que en su análisis y evaluación de riesgos en seguridad de la información, se justifique la pertinencia de contratar el servicio de computación en la nube;

f. Que en las cláusulas del contrato se contemplen los aspectos señalados en los incisos a, b, c y d del presente Artículo.

ASFI podrá objetar la implementación del servicio de computación en la nube, cuando el proyecto presentado, incumpla con lo señalado en los incisos a, b, c, d y f y/o considere insuficiente el análisis y evaluación de riesgos en seguridad de la información, en lo referido a la pertinencia de contratar el servicio de computación en la nube (inciso e).

A efectos de realizar la evaluación del citado proyecto, la Entidad Supervisada debe remitir adjunto a éste copia del borrador del contrato, así como otra documentación que considere pertinente.

Artículo 11° - (Protección de datos en la nube) La Entidad Supervisada debe contar con políticas y procedimientos a efectos de definir los criterios que garanticen el debido tratamiento, protección y privacidad de datos personales cuando se utilicen los servicios de computación en la nube, considerando la normativa nacional en actual vigencia y los referentes internacionales en esta materia.

Artículo 12° - (Nivel de riesgo del servicio de computación en la nube) La entidad supervisada, antes de contratar los servicios de computación en la nube, debe realizar un diagnóstico del nivel de riesgo y la sensibilidad de la información y/o los recursos tecnológicos a ser expuestos, el cual debe estar contenido en el "Proyecto de implementación del servicio de computación en la nube".

SECCIÓN 12: ROL DE LA AUDITORÍA INTERNA

Artículo Único – (Auditoría Interna) El Auditor Interno o la Unidad de Auditoría Interna es un elemento clave en la gestión de seguridad de la información, debiendo entre otras, cumplir con las siguientes funciones:

a. Verificar el cumplimiento del presente Reglamento, en los doce meses precedentes, debiendo la Entidad Supervisada remitir a ASFI hasta el 15 de enero de cada año, el informe elaborado. Dicha labor podrá realizarse a través, de evaluaciones internas y/o externas;

b. Emitir un informe sobre la ejecución de las pruebas de intrusión solicitadas en el Artículo 8° de la Sección 3, del presente Reglamento y comunicar el resultado del análisis de vulnerabilidades a ASFI, hasta el 15 de noviembre de cada año, adjuntando para el efecto, copia del informe ejecutivo del evaluador y el plan de acción correspondiente, para subsanar las debilidades identificadas durante el examen;

c. Emitir un informe sobre el resultado de las pruebas realizadas a los planes de contingencias tecnológicas y de continuidad del negocio, mismo que debe permanecer en la Entidad Supervisada a disposición de ASFI;

d. Refrendar el informe sobre procesamiento de datos o ejecución de sistemas en lugar externo, establecido en el inciso f, Artículo 3° de la Sección 11 del presente Reglamento;

e. Incluir en su Plan Anual de Trabajo la verificación del cumplimiento de las políticas y procedimientos relativos a la protección de datos en la nube, establecidos en el Artículo 11° Sección 11 del presente Reglamento, si la Entidad Supervisada contrató dicho servicio.

SECCIÓN 13: OTRAS DISPOSICIONES

Artículo 1° - (Responsabilidad) El cumplimiento, implementación y difusión interna del presente Reglamento, es responsabilidad del Directorio u Órgano equivalente y de la Gerencia General de la Entidad Supervisada.

Artículo 2° - (Normas y estándares internacionales aplicables) En caso de existir situaciones no previstas en el presente Reglamento, la Entidad Supervisada, tiene que aplicar normas y/o estándares internacionales de tecnologías de información y seguridad de la información, debiendo identificar la referencia de la(s) norma(s) y/o estándares utilizados en sus políticas.

Artículo 3° - (Herramientas informáticas) Para realizar evaluaciones de seguridad de la información y auditoría de sistemas a entidades supervisadas, ASFI podrá utilizar herramientas informáticas cuando lo considere pertinente.

Asimismo, ASFI evaluará a cada Entidad Supervisada de acuerdo a su naturaleza, tamaño y complejidad de sus operaciones, aplicando normas y/o estándares internacionales de tecnologías de información y seguridad de la información.

Artículo 4° - (Régimen de sanciones) La inobservancia del presente Reglamento, dará lugar al inicio del proceso administrativo sancionatorio.

SECCIÓN 14: DISPOSICIONES TRANSITORIAS

Artículo 1° - (Adecuación y cronograma) La Entidad Supervisada debe cumplir con las disposiciones establecidas en el presente Reglamento hasta el 31 de diciembre de 2014.

La Entidad Supervisada debe elaborar un cronograma para el cumplimiento y adecuación a la presente normativa, el cual debe ser aprobado por su Directorio u Órgano equivalente y permanecer a disposición de ASFI.

Artículo 2° - (Plazo de adecuación) Las modificaciones e incorporaciones al presente Reglamento, aprobadas en el mes de mayo de 2016, entran en vigencia a partir del 3 de octubre de 2016, debiendo la Entidad Supervisada considerar los siguientes aspectos:

a. El citado plazo no aplica para lo dispuesto en el inciso d, Artículo 1°, Sección 8 del citado Reglamento, referido a la certificación digital.

ASFI comunicará oportunamente a la entidad supervisada, el plazo que aplicará para dicho propósito, en función a las disposiciones que emita la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT);

b. Las disposiciones referidas a las medidas de seguridad que la entidad supervisada debe implementar para la verificación y control de transacciones y transferencias electrónicas dispuestas en el inciso h, Artículo 1°, Sección 8 del presente Reglamento, entran en vigencia a partir del 1 de febrero de 2017.

CONTROL DE VERSIONES

L03T07C02		Secciones														Anexos
Circular	**Fecha**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**1**
ASFI/543/2018	15/05/2018		*													
ASFI/536/2018	16/04/2018										*	*				
ASFI/505/2017	04/12/2017	*		*	*	*	*					*				*
ASFI/423/2016	30/09/2016														*	
ASFI/395/2013	14/06/2016	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
ASFI/193/2013	16/09/2013	*	*	*	*	*	*	*	*	*	*	*	*	*	*	
SB/466/2004	29/04/2004			*	*	*										
SB/443/2003	12/08/2003		*	*	*	*										
SB/436/2003	04/07/2003	*		*	*	*										

CAPÍTULO III: REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD FÍSICA

SECCIÓN 1: ASPECTOS GENERALES

Artículo 1° - (Objeto) El presente Reglamento tiene por objeto establecer lineamientos y condiciones para la Gestión de Seguridad Física, que deben implementar las Entidades de Intermediación Financiera (EIF) y las Empresas de Servicios Financieros Complementarios para la prestación de servicios a sus clientes y usuarios.

Artículo 2° - (Ámbito de aplicación) Se encuentran sujetos al ámbito de aplicación del presente Reglamento, los Bancos, Entidades Financieras de Vivienda, Cooperativas de Ahorro y Crédito Abiertas, Cooperativas de Ahorro y Crédito Societarias, Instituciones Financieras de Desarrollo, Empresas de Arrendamiento Financiero, Empresas de Servicios de Pago Móvil, Casas de Cambio, Empresas de Giro y Remesas de Dinero, Empresas Administradoras de Tarjetas Electrónicas y Empresas de Transporte de Material Monetario y Valores, que cuenten con licencia de funcionamiento otorgada por la Autoridad de Supervisión del Sistema Financiero (ASFI), denominadas en adelante entidades supervisadas.

Artículo 3° - (Definiciones) Para efectos de las disposiciones, contenidas en el presente Reglamento, se considerarán las siguientes definiciones:

a. **Área de exclusión:** Área de acceso restringido identificada en las instalaciones de la entidad supervisada;

b. **Botón de pánico:** Dispositivo electrónico que genera una señal de auxilio no audible que comunica la ocurrencia de un incidente de seguridad física a la central de monitoreo;

c. **Bóveda principal:** Área destinada a la custodia y atesoramiento del material monetario y/o valores;

d. **Bóveda auxiliar:** Área destinada a la custodia y atesoramiento transitorio del material monetario y/o valores, durante la atención de las operaciones y/o al cierre del día;

e. **Caja fuerte bóveda:** Equipo físico destinado a la custodia y atesoramiento del material monetario y/o valores;

f. **Caja fuerte auxiliar:** Equipo físico destinado a la custodia y atesoramiento transitorio de una parte del material monetario y/o valores;

g. **Caja tipo buzón:** Permite el atesoramiento transitorio de material monetario y/o valores con ubicación en el área de ventanillas de atención al público;

h. **Camino de ronda:** Recorrido que el guardia privado o policía de seguridad, realiza a lo largo de los pasillos, salidas de emergencia, gradas, áreas de carga o descarga, garajes, áreas comunes y otras áreas, con el objeto de velar por la integridad física de las personas y la seguridad de los activos de la entidad;

i. **Circuito cerrado de televisión:** Sistema de transmisión de imágenes compuesto por un número determinado de cámaras que transmiten las señales capturadas a uno o más monitores, que forman un conjunto cerrado y limitado, en adelante CCTV;

j. **Central de monitoreo:** Área de exclusión donde están instaladas las centrales para la recepción de señales provenientes de los sistemas de alarma y almacenamiento de las grabaciones de las cámaras de Circuito Cerrado de TV (CCTV);

k. **Corresponsal financiero:** Puede ser corresponsal financiero:

   1. La Entidad de Intermediación Financiera con Licencia de Funcionamiento;
   2. La Cooperativa de Ahorro y Crédito Societaria con Certificado de Adecuación y previa autorización de ASFI;
   3. La Institución Financiera de Desarrollo con Certificado de Adecuación;
   4. La Empresa de Transporte de Material Monetario y/o Valores y la Casa de Cambio con Personalidad Jurídica, que cuenten con Licencia de Funcionamiento.

l. **Corresponsal no financiero:** Es la persona natural o jurídica legalmente constituida que no realiza actividades de intermediación financiera o de servicios financieros complementarios;

m. **Contacto magnético:** Dispositivo electrónico que se activa al separar un contacto eléctrico de un imán, rompiendo el campo magnético y activando el sistema de alarma, utilizado para el control de apertura de puertas y ventanas;

n. **Detector inercial:** Dispositivo electrónico que activa el sistema de alarma ante la detección de vibraciones en el suelo o paredes;

o. **Diagnóstico de seguridad física:** Resultado del análisis que se realiza a la infraestructura, entorno y medidas de seguridad física de una entidad supervisada, que tiene como fin conocer las características específicas, vulnerabilidades y amenazas a las que están expuestas las instalaciones, operaciones y/o servicios de la entidad supervisada;

p. **Empresa privada de vigilancia:** Empresa privada autorizada por la instancia competente para prestar servicios remunerados de seguridad física a entidades financieras y empresas de servicios financieros complementarios, que incluyen la provisión de guardias, sistemas de alarma, monitoreo y/o vigilancia motorizada entre otros;

q. **Equipo anti-skimming:** Equipo instalado en el cajero automático que previene el robo de identidad y reduce el fraude;

r. **Gestión de seguridad física:** Conjunto de objetivos, políticas, procedimientos, planes y acciones que implementa la entidad supervisada con el objeto de proteger la integridad física de las personas, así como los activos que se encuentren bajo su custodia, en el interior o fuera de sus instalaciones, asimismo, la seguridad de su personal cuando estos realicen operaciones y servicios fuera de las dependencias de la entidad;

s. **Guardia privado:** Personal dependiente de una empresa privada de vigilancia, autorizada por la instancia competente, que vigila, protege y custodia la integridad física de las personas y/o activos asignados;

t. Grupo electrógeno: Equipo generador de electricidad por medio de un motor de combustión interna, que garantiza el suministro ininterrumpido de energía para los sistemas eléctricos de seguridad física;

u. Incidente de seguridad física: Cualquier evento o acontecimiento que causa daños o pérdidas de vidas humanas, activos e imagen institucional de la entidad supervisada;

v. Medidas de seguridad física: Son los procesos físicos, humanos y tecnológicos adoptados por la entidad supervisada que en forma aislada o combinada, minimizan, retardan, impiden y/o neutralizan riesgos de incidentes de seguridad física y sus consecuencias;

w. Nivel de riesgo ante incidentes de seguridad física: Es el grado de exposición a daños o pérdidas ocasionadas por incidentes de seguridad física;

x. Particionado: Es el procedimiento por el cual se divide un sistema de alarma en dos o más áreas de forma que puedan activarse o desactivarse en forma independiente;

y. Personal de Vigilancia: Personal de la Policía Boliviana o de Empresas Privadas de Vigilancia autorizadas por la instancia competente, que brinda seguridad a las personas en las instalaciones y los activos de la entidad;

z. Plan de seguridad física: Documento aprobado por la instancia competente, que establece los cursos de acción, medios y recursos que serán implementados para proporcionar seguridad física en las instalaciones de la entidad supervisada, así como a las operaciones y servicios que realice;

aa. Policía de seguridad: Personal de la Policía Boliviana provisto de armas de fuego, que presta servicios de protección y/o custodia de la integridad física de las personas y/o activos asignados;

bb. Punto de Atención Financiero (PAF): Espacio físico habilitado por una entidad supervisada, que cuenta con las condiciones necesarias para realizar operaciones de intermediación financiera o servicios financieros complementarios, según corresponda, en el marco de la Ley N° 393 de Servicios Financieros (LSF), de acuerdo a lo establecido en la Recopilación de Normas para Servicios Financieros (RNSF);

cc. Sensor infrarrojo: Dispositivo electrónico que emite un rayo infrarrojo continuo, cuya interferencia por elementos extraños, activa el sistema de alarma;

dd. Sensor de ruptura de cristal: Dispositivo electrónico que detecta las frecuencias del sonido que producen los vidrios al astillarse, a través de un micrófono instalado en su interior;

ee. Sensor sísmico: Dispositivo electrónico que detecta golpes o vibraciones, instalados en el suelo o paredes alrededor de bóveda(s) o caja(s) fuerte(s) bóveda;

ff. Sirenas de Alarma: Dispositivo que emite sonidos y luces de alarma u otros elementos disuasivos que alerten a los transeúntes o personal de vigilancia de un incidente de seguridad física;

gg. Skimming: Robo de información de tarjetas de débito o crédito al momento de efectuar una transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento;

hh. Vigilancia motorizada: Patrullaje disuasivo realizado por unidades motorizadas a las instalaciones de la entidad supervisada;

ii. Transporte de material monetario y/o títulos valores: Traslado físico de material monetario y/o valores, de un PAF a otro;

jj. Unidad de Seguridad Física: Unidad organizacional dependiente de la instancia ejecutiva que corresponda, responsable de operativizar e informar sobre la gestión de seguridad física en la entidad supervisada. Su tamaño y estructura interna debe estar en relación con el nivel de riesgo, incidentes de seguridad física y volumen de operaciones de los PAF;

kk. Zona rural: Espacio geográfico del territorio boliviano, que no incluye las zonas urbanas y peri urbanas, en el que se desarrolla predominantemente actividad agropecuaria, bajo la forma de vida comunitaria de las familias que habitan en ella.

SECCIÓN 2: GESTIÓN DE SEGURIDAD FÍSICA

Artículo 1° - (Gestión de Seguridad Física) La entidad supervisada, debe constituir un sistema para la Gestión de Seguridad Física, que permita identificar, monitorear, controlar y mitigar en forma preventiva o correctiva, impidiendo y/o neutralizando los riesgos a incidentes de seguridad física y sus consecuencias.

Artículo 2° - (Nivel de riesgo) La entidad supervisada, debe realizar un diagnóstico de seguridad física que identifique el nivel de riesgo ante incidentes de seguridad física al que se encuentran expuestas sus instalaciones, considerando mínimamente las zonas geográficas de riesgo identificadas por la autoridad competente en temas de seguridad ciudadana y el valor monetario de los activos que se encuentran bajo su resguardo.

Para la aplicación de las medidas específicas de seguridad física establecidas en la Sección 4 del presente Reglamento, la entidad supervisada, debe clasificar el nivel de riesgo de sus PAF ubicados en las zonas rurales y urbanas en las categorías de riesgo alto, medio o bajo, considerando mínimamente los aspectos mencionados en el párrafo anterior.

ASFI podrá instruir, a la entidad supervisada, modificar el nivel de riesgo determinado para sus PAF ubicados en zonas rurales y urbanas en función a la ocurrencia de incidentes de seguridad física o como producto de la supervisión realizada por las Direcciones correspondientes.

Artículo 3° - (Políticas) La entidad supervisada debe contar con políticas de seguridad física aprobadas por el Directorio u Órgano equivalente, orientadas a priorizar el fortalecimiento de la seguridad física en sus instalaciones, operaciones y/o servicios, las mismas que deben incluir referencias de la(s) Norma(s) Internacional(es) de seguridad física adoptada(s) por la entidad. Dichas políticas deben considerar los siguientes principios, según se enuncian en orden de prioridad:

- **a.** Protección a la vida de las personas que se encuentren dentro de las instalaciones de las Entidades Supervisadas y de su personal cuando estos realicen operaciones y/o servicios fuera de las mismas;
- **b.** Protección de los activos propios y en custodia, incluida la documentación e información en medios impresos o electrónicos;
- **c.** Protección de la imagen institucional.

La entidad supervisada debe implementar políticas de capacitación en seguridad física para todo su personal, sin exclusiones.

Asimismo, las entidades supervisadas que cuenten con puntos de atención financiera ubicados en zonas rurales, deben contar con políticas de seguridad física específicas que consideren las características y condiciones de estas zonas, así como a los servicios financieros rurales que se presten.

Artículo 4° - (Manuales de funciones y procedimientos) La entidad supervisada debe contar con manuales de funciones y de procedimientos de seguridad física, que establezcan mínimamente el

personal responsable y la periodicidad para su realización. Los manuales de funciones y procedimientos mínimos que debe considerar la entidad supervisada son:

a. Manuales de funciones para:

1. Personal de vigilancia y vigilancia motorizada, que incluya la prohibición de que el mencionado personal realice actividades no relativas a la seguridad física;

2. Miembros del Comité de Seguridad Física y Personal de la Unidad de Seguridad Física, que establezca la interacción con áreas relacionadas;

3. Personal de la entidad supervisada y personal de vigilancia, que interactúa en la recepción, envío y transporte del material monetario y/o valores.

b. Manuales de procedimientos para:

1. Asistencia a personas afectadas por incidentes de seguridad física ocurridos en instalaciones de la entidad supervisada que debe ser inmediata, adecuada y en base a capacitación previa;

2. Resguardo de la privacidad en las transacciones financieras realizadas por clientes y usuarios en ventanillas de atención al público;

3. Administración de llaves de ingreso a las instalaciones de la entidad supervisada, acceso a las áreas de exclusión, claves de sistemas de alarma y claves de equipos de atesoramiento según corresponda. Las claves señaladas deben ser modificadas al menos cada seis (6) meses o cuando se realice el cambio del personal encargado; Pruebas de funcionamiento de los sistemas de seguridad, que incluya el inventario de equipos e instalaciones sujetos a revisión;

4. Mantenimiento preventivo y correctivo de los sistemas de atesoramiento, dispositivos de protección, sistemas de monitoreo y alarmas, al menos una vez al año;

5. Transporte de material monetario y/o valores por parte del personal de la entidad supervisada y personal de vigilancia, cuando corresponda;

6. Abastecimiento de material monetario en los cajeros automáticos u otros Puntos de Atención Financiera, cuando corresponda;

7. Ubicación, construcción, instalación y manejo de bóveda(s) y caja(s) fuerte(s) bóveda;

8. Instalación de medidas de seguridad física en los ambientes destinados a cajeros automáticos;

9. Funcionamiento de centrales de monitoreo que incluya tiempo de almacenamiento, modalidad y resguardo de las grabaciones de monitoreo, para atención de denuncias y reclamos de los usuarios o clientes;

10. Activación y atención de sistemas de alarma.

Artículo 5° - (Estructura organizacional) La entidad supervisada, debe establecer una estructura organizacional adecuada al nivel de riesgo y número de PAF en funcionamiento, ubicados en zonas rurales y urbanas, que delimite las funciones y responsabilidades relativas a la gestión de seguridad física.

Artículo 6° - (Unidad de Seguridad Física) La entidad supervisada que cuente con un patrimonio contable igual o mayor a UFV30.000.000,00 (Treinta Millones de Unidades de Fomento a la Vivienda) o su equivalente, debe contar con una Unidad de Seguridad Física, que será responsable de operativizar y monitorear la gestión de seguridad física, emitir reportes e informes para las instancias de decisión, proponer medidas preventivas o correctivas que se requieran para fortalecer la seguridad física en las instalaciones de la entidad supervisada, entre otras tareas operativas.

Cuando corresponda, las tareas de la Unidad de Seguridad Física serán asignadas por el Comité de Seguridad Física a otra unidad organizacional de la entidad supervisada.

Cuando la Entidad Supervisada sea una ETM, debe contar con un Jefe de Operaciones, independientemente del patrimonio contable, conforme a lo establecido en el Reglamento Operativo para Empresas Privadas de Vigilancia aprobado mediante Resolución Ministerial N° 21 de 4 de febrero de 2013 y modificado mediante la Resolución Ministerial N° 168 de 16 de agosto de 2013, ambas emitidas por el Ministerio de Gobierno.

Artículo 7° - (Comité de Seguridad Física) La entidad supervisada debe conformar un Comité de Seguridad Física, que será responsable de analizar y evaluar las situaciones de riesgo de vulneración a los sistemas de seguridad física, así como las medidas preventivas y correctivas que debe poner en consideración del Directorio u órgano equivalente para su aprobación.

El Comité estará conformado mínimamente por un Director, el Gerente General y un Gerente del área relacionada o instancia equivalente (con derecho a voz y voto) y el responsable de la Unidad de Seguridad Física u Órgano equivalente con derecho a voz, cuando corresponda.

El Comité debe llevar un registro en actas de los temas y acuerdos tratados en sus reuniones.

Artículo 8° - (Responsabilidades y funciones del Directorio) El Directorio u Órgano equivalente es responsable de la gestión de seguridad física en la entidad supervisada, debiendo cumplir, entre otras, las siguientes funciones:

- **a.** Aprobar, revisar, actualizar y realizar el seguimiento a las estrategias, políticas, procedimientos y planes de seguridad física, mínimamente una vez al año y cuando corresponda;
- **b.** Aprobar los manuales de funciones y procedimientos relativos a la gestión de seguridad física, así como asegurar que se encuentren debidamente actualizados;
- **c.** Designar a los miembros del Comité de seguridad física;
- **d.** Disponer la conformación de una Unidad de Seguridad Física y designar al responsable de la misma, cuando corresponda.

Artículo 9° - (Responsabilidades y funciones de la Gerencia General) La Gerencia General es responsable de la implementación y cumplimiento de las políticas, estrategias, planes, manuales y procedimientos, aprobados por el Directorio u Órgano equivalente para la gestión de seguridad física, así como de implementar las acciones correctivas o preventivas que se requieran. También es responsable del cumplimiento estricto de las disposiciones contenidas en el presente Reglamento.

Artículo 10° - (Brigada de auxilio) La entidad supervisada, debe capacitar un grupo de funcionarios por cada PAF identificado con riesgo alto, para ejecutar procedimientos de asistencia orientados a proteger la vida de las personas afectadas por incidentes de seguridad física. Dichos funcionarios deben interactuar con el personal de vigilancia según procedimiento predefinido.

Artículo 11° - (Gestión de seguridad física para las Casas de Cambio Unipersonales) Las casas de cambio unipersonales deben contar mínimamente con procedimientos destinados a afrontar incidentes de seguridad física, considerando al menos los señalados en los numerales 1 al 6, y 8 del inciso b, Artículo 4°, Sección 2 del presente Reglamento (en lo que corresponda).

Los procedimientos establecidos por las casas de cambio unipersonales deben considerar en orden de prioridad, los principios descritos en el Artículo 3° de la presente Sección. Las disposiciones restantes contenidas en la misma, no son de aplicación obligatoria para las casas de cambio unipersonales, sin embargo, no se restringe su aplicación voluntaria.

Artículo 12° - (Transporte de material monetario y valores por cuenta propia) Las Entidades de Intermediación Financiera que ante la ausencia de una ETM con Licencia de Funcionamiento otorgada por la Autoridad de Supervisión del Sistema Financiero, realicen el transporte de material monetario y valores, por cuenta propia, en el marco de lo establecido en el segundo párrafo del Artículo 4, Sección 1 del Reglamento para Empresas de Transporte de Material Monetario y Valores, deben realizar una evaluación de riesgos inherentes a dicho transporte cuyos resultados deben estar plasmados en un informe, el cual debe estar a disposición de ASFI.

En casos de transporte de material monetario y valores a los puntos de atención financiera en zonas rurales, la entidad supervisada además debe incorporar en su informe, la evaluación de riesgos concernientes a la localidad donde están instalados los citados PAF.

Artículo 13° - (Gestión de seguridad física para las Empresas Administradoras de Tarjetas Electrónicas) Las Empresas Administradoras de Tarjetas Electrónicas deben contar mínimamente con procedimientos destinados a afrontar incidentes de seguridad física, considerando al menos los señalados en los numerales 1 y 2 del inciso a y numerales 1, 3, 4, 5, 9 y 10 del inciso b, Artículo 4°, Sección 2 del presente Reglamento.

SECCIÓN 3: MEDIDAS GENERALES DE SEGURIDAD FÍSICA

Artículo 1° - (Clasificación de áreas de exclusión) Con base en un análisis de riesgo ante incidentes de seguridad física, la entidad supervisada debe identificar las áreas de exclusión que requieran medidas de máxima seguridad. El citado análisis, debe estar plasmado en un informe, el cual estará a disposición de ASFI.

Artículo 2° - (Equipos de atesoramiento) La entidad supervisada, en función al nivel de riesgo al que se encuentran expuestos sus PAF, debe contar con equipos de atesoramiento que cumplan con estándares de calidad establecidos en la Norma Internacional, definida en sus políticas, respecto a la resistencia contra ataques por medios mecánicos, eléctricos, explosivos u otros.

A continuación se detalla la lista referencial de equipos de atesoramiento que pueden ser utilizados por la entidad supervisada:

a. **Bóveda principal:** Construida de hormigón reforzado, provista de puerta de bóveda con cerraduras de retardo y control horario;

b. **Bóveda auxiliar:** Construida de hormigón armado reforzado, provista de puerta de bóveda con cerraduras de retardo y control horario, con ubicación diferente a la bóveda principal, sin embargo ambas se encuentran instaladas en el mismo PAF;

c. **Caja fuerte bóveda:** Equipo con estructura blindada, anclada al piso y provista de cerradura de retardo;

d. **Caja fuerte auxiliar:** Equipo con estructura blindada, anclada al piso, y provista de cerradura de retardo, con ubicación diferente a la caja fuerte bóveda, sin embargo ambas se encuentran instaladas en el mismo PAF;

e. **Caja tipo buzón:** Equipo, con estructura blindada, con cerradura de retardo y anclada al piso, ubicada en el área de ventanillas de atención al público.

Artículo 3° - (Ventanillas de atención al público) El área de ventanillas de atención al público debe contar con dispositivos de control que permitan el acceso solo a personas autorizadas.

En los PAF identificados con nivel de riesgo alto, ubicados en ciudades capitales de departamento y adicionalmente en las ciudades que tengan una población mayor a 100.000 habitantes y localidades fronterizas, las ventanillas de atención al público deben contar con vidrios con resistencia balística u otro material de igual consistencia que cumpla estándares de calidad internacional, definidos en las políticas de seguridad física de cada entidad supervisada.

Artículo 4° - (Condiciones para el personal de vigilancia) La entidad supervisada es la responsable de que el personal de vigilancia contratado, cuente mínimamente con el siguiente equipamiento para la prestación de sus servicios:

a. **Policía de seguridad:** arma de fuego, chaleco antibalas con una resistencia balística mínima a proyectiles calibre 9mm y 44magnum, certificada al menos por el fabricante,

así como otros implementos adecuados a las funciones asignadas según se establece en el Anexo 1;

b. **Guardia privado:** mínimamente arma(s) de defensa, chaleco antibalas con una resistencia mínima a proyectiles calibre 9mm y 44magnum, certificada al menos por el fabricante, así como otros implementos adecuados a las funciones según se establece en el Anexo 1.

Artículo 5° - (Dotación de personal de vigilancia) En los PAF ubicados en localidades que no cuenten con suficiente disponibilidad de personal de vigilancia en los Batallones de Seguridad Física, Comandos Departamentales de la Policía Boliviana o Empresas Privadas de Vigilancia, autorizadas por la instancia competente, la entidad supervisada debe contar como mínimo con un (1) policía de seguridad o un (1) guardia privado. Adicionalmente, en caso de que no exista personal de vigilancia en la localidad, la entidad debe adoptar medidas de seguridad que suplan la carencia del personal de vigilancia, según lo establecido en sus políticas de seguridad física.

Los recintos para cajeros automáticos que cuenten con más de dos (2) equipos sean estos de una o de diferentes entidades supervisadas, deben contar al menos con un (1) guardia privado. Las entidades supervisadas podrán suscribir, entre sí, convenios para que el personal de vigilancia brinde protección a todos los cajeros automáticos ubicados en el recinto. El personal de vigilancia que preste el servicio en los recintos de cajeros automáticos debe realizarlo las veinticuatro (24) horas del día, siete (7) días a la semana de forma ininterrumpida.

De acuerdo a la ubicación física del cajero automático, la entidad supervisada debe habilitar casetas para la permanencia del personal de vigilancia instaladas a una distancia no menor de dos (2) metros ni mayor a diez (10) metros de éste. Las casetas podrán ser fijas o plegables según se establece en el Anexo 2.

La entidad supervisada debe asegurarse que el personal de vigilancia cuente con la capacitación y los conocimientos básicos, según se establece en el Anexo 3.

Artículo 6° - (Dotación adicional de personal de vigilancia) Respecto a los PAF donde se verifique la necesidad de brindar mayor seguridad para la atención a los clientes y usuarios, ASFI se reserva el derecho de exigir personal de vigilancia adicional al establecido por la entidad supervisada.

Artículo 7° - (Horarios) El personal de vigilancia debe permanecer en ejercicio de sus funciones en el PAF, durante el tiempo que disponga el manual de funciones del personal de vigilancia definido por la entidad supervisada, el mismo que al menos debe abarcar el tiempo de atención al público o de permanencia de funcionarios en las instalaciones del PAF.

Artículo 8° - (Sistema de alarma) La entidad supervisada debe contar con un sistema de alarma debidamente particionado, zonificado, interconectado a una central de monitoreo de alarma y habilitados para detectar incidentes de seguridad física en áreas de atención al público y áreas de exclusión que hubieran sido identificadas, de acuerdo a lo señalado en el Artículo 1° de la presente Sección.

Artículo 9° - (Dispositivos para la seguridad física) En función al nivel de riesgo y la clasificación de las áreas de exclusión, la entidad supervisada debe implementar dispositivos para la seguridad física entre los cuales podrá considerar, en relación a su funcionalidad, los siguientes:

a. Sistemas para control de accesos biométricos;

b. Sensores infrarrojos;

c. Contactos magnéticos;

d. Sensores de ruptura de cristal;

e. Detectores inerciales;

f. Sensores sísmicos;

g. Detectores de humo;

h. Botones de pánico;

i. Sirenas de alarmas;

j. Grupo electrógeno;

k. Extintores de incendio (portátiles).

Artículo 10° - (Central de monitoreo) La entidad supervisada, debe controlar desde una Central de Monitoreo propia o tercerizada, en forma permanente e ininterrumpida los sistemas de alarma instalados en los PAF, debiendo reportar a las autoridades competentes la ocurrencia de incidentes de seguridad física de forma oportuna, así como resguardar la información de monitoreo de los sistemas de CCTV en medios de grabación adecuados para su almacenamiento.

La entidad supervisada es responsable de velar por la adecuada prestación del servicio tercerizado y el resguardo de la información que se genere, dando cumplimiento a los requisitos establecidos por el Reglamento Operativo para Empresas Privadas de Vigilancia.

Adicionalmente, la entidad supervisada que cuente con más del 50% de sus PAF identificados con nivel de riesgo alto, debe contar con una Central de Monitoreo de respaldo funcionando en una ubicación geográfica diferente.

La Central de Monitoreo debe funcionar de forma ininterrumpida durante veinticuatro (24) horas al día, siete (7) días a la semana.

Artículo 11° - (Sistema de circuito cerrado de televisión) La entidad supervisada, debe contar con sistemas de CCTV propios o tercerizados, acorde a la distribución y cantidad de cámaras instaladas en sus PAF. Las grabaciones de las cámaras de seguridad, deben permitir la identificación de personas, actividades u otros, ocurridos en incidentes de seguridad física.

La entidad supervisada debe priorizar la ubicación de cámaras de seguridad en las áreas de ventanillas de atención al público, cajeros automáticos y accesos al PAF, bóvedas, camino de ronda y áreas de exclusión, según corresponda.

La entidad supervisada debe mantener el registro efectuado por el sistema de vigilancia y monitoreo, por un período no menor a ciento ochenta (180) días.

Artículo 12° - (Vigilancia motorizada) La entidad supervisada debe contar con unidades motorizadas a cargo de personal que realice la vigilancia de los PAF *in situ*, de acuerdo a planes definidos para el efecto, los cuales deben incluir al menos la ruta de recorrido y rol de turnos, dando prioridad a los PAF con niveles de riesgo alto ubicados en ciudades capitales de departamento y adicionalmente en las ciudades con una población mayor a 100.000 habitantes.

Artículo 13° - (Medidas generales de seguridad física para las Casas de Cambio Unipersonales) Las disposiciones contenidas en la presente Sección, no son de aplicación obligatoria para las Casas de Cambio unipersonales, excepto por el Artículo 3° y el inciso k del Artículo 9° de la presente Sección, sin embargo, no se restringe la aplicación voluntaria de las mencionadas disposiciones.

SECCIÓN 4: MEDIDAS ESPECÍFICAS DE SEGURIDAD FÍSICA

Artículo 1° - (Medidas específicas) La entidad supervisada, adicionalmente a lo establecido en la Sección 3 del presente Reglamento, debe implementar las medidas de seguridad específicas contenidas en la presente Sección.

Las oficinas externas y feriales, se regirán por lo establecido en el Artículo 5° de la presente Sección.

Artículo 2° - (Oficinas centrales o sucursales) La entidad supervisada en función al nivel de riesgo al que se encuentran expuestas su oficina central y sucursales, debe implementar mínimamente las siguientes medidas específicas de seguridad física:

Requisitos de Seguridad Física	Niveles de Seguridad		
	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Equipos de Atesoramiento			
Bóveda Principal	-	☑	☑
Bóveda Auxiliar	-	-	☑
Caja Fuerte Bóveda	☑	-	-
Caja Fuerte Auxiliar		☑	
Puertas de Acceso Áreas de Exclusión	☑	☑	☑
1 Caja fuerte tipo buzón anclada por ventanilla	-	-	☑
1 Caja fuerte tipo buzón anclada por área de ventanillas	☑	☑	-
Personal de Vigilancia			
Un (1) Policía de Seguridad o un (1) Guardia Privado	☑	☑	-
Dos (2) Policías de Seguridad	-	-	☑

☑ = Indispensable -= No indispensable

Adicionalmente, la entidad supervisada debe contar al menos con un (1) policía de seguridad o un (1) guardia privado por cada puerta de acceso a la oficina central o sucursal, en correlación a lo dispuesto en el Artículo 5° de la Sección 3 del presente Reglamento.

Las oficinas centrales o sucursales que no manipulen material monetario y/o valores en sus instalaciones, no están obligadas a contar con equipos de atesoramiento.

Artículo 3° - (Agencias fijas) La entidad supervisada en función al nivel de riesgo al que se encuentran expuestas sus agencias fijas debe implementar mínimamente las siguientes medidas específicas de seguridad física:

Requisitos de Seguridad Física	Niveles de Seguridad		
	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Equipos de Atesoramiento			
Caja Fuerte Bóveda	☑	☑	☑
Caja Fuerte Auxiliar	-	-	☑
Puerta de Acceso Áreas de Exclusión	☑	☑	☑
1 Caja fuerte tipo buzón anclada por ventanilla	-	-	☑
1 Caja fuerte tipo buzón anclada por área de ventanillas	☑	☑	-
Personal de Vigilancia			
Un (1) Policía de Seguridad	-	-	☑
Un (1) Policía de Seguridad o Un (1) Guardia Privado	-	☑	-
Un (1) Guardia Privado	☑	-	-

☑ = Indispensable -= No indispensable

Artículo 4° - (Agencia móvil) La entidad supervisada debe implementar en sus agencias móviles, las medidas de seguridad física señaladas en el Reglamento Operativo para las Empresas Privadas de Vigilancia, en lo referido a Banca Móvil.

Artículo 5° - (Oficina externa y oficina ferial) En función al tipo de operaciones que realizan y el nivel de riesgo al que se encuentran expuestas las oficinas externas y feriales, la entidad supervisada determinará la implementación de sistemas de alarma, monitoreo y condiciones para la instalación de ventanillas, según corresponda, a lo señalado en la Sección 3 del presente Reglamento.

Adicionalmente, de acuerdo al volumen del material monetario que circule en los PAF, la entidad supervisada debe contar con equipos de atesoramiento para el adecuado resguardo de los activos, así como con personal de vigilancia, para la protección de la integridad física de las personas que se encuentran en sus instalaciones.

Artículo 6° - (Ventanilla de cobranza) La entidad supervisada en función al nivel de riesgo al que se encuentran expuestas sus ventanillas de cobranza, debe contar al menos con el siguiente personal de vigilancia:

a. Un (1) policía de seguridad, cuando la ventanilla de cobranza sea identificada con un nivel de riesgo alto en correlación al Artículo 5° de la Sección 3 del presente Reglamento;

b. Un (1) policía de seguridad o un (1) guardia privado cuando la ventanilla de cobranza sea identificada con un nivel de riesgo medio o bajo.

Cuando la ventanilla de cobranza se encuentre instalada en instituciones públicas o privadas que cuenten con personal de vigilancia, la entidad supervisada podrá suscribir convenios para compartir el servicio de vigilancia, siendo responsabilidad de la entidad supervisada velar por el cumplimiento de las tareas establecidas en el manual de funciones del personal de vigilancia aprobado por las instancias correspondientes.

Artículo 7° - (Corresponsales financieros y no financieros) La entidad financiera contratante de la Corresponsalía, es responsable de velar por el cumplimiento de las medidas de seguridad física generales y especificas contenidas en el presente Reglamento, según corresponda al tipo de corresponsal y en función al nivel de riesgo y tipo de operaciones realizadas en los puntos de atención contratados.

Artículo 8° - (Cajero automático) Para la instalación y funcionamiento de cajeros automáticos, independientemente si estos son internos o externos, la entidad de intermediación financiera debe cumplir con los siguientes requerimientos mínimos:

a. **Medidas de seguridad física del cajero automático externo:** Los cajeros automáticos externos deben contar con una de las siguientes medidas de seguridad:

1. Ser instalado en recinto;

2. Contar con personal de vigilancia si no cuenta con recinto.

a.1 Cajero automático con recinto: Los recintos en los que se encuentran instalados los cajeros automáticos, debe contar con:

i. Vidrios templados y/o laminados que permitan observar el interior del recinto, desde el exterior y viceversa, para detectar eventuales amenazas, sea contra la máquina o contra el usuario;

ii. El vidrio a utilizarse en las puertas de ingreso, así como aquel que forme parte de la estructura del recinto de los cajeros automáticos, debe ser templado y/o laminado;

iii. La puerta de acceso debe contar con un dispositivo de cierre interno, de tipo mecánico, que impida el acceso de terceros al interior del recinto cuando el usuario se encuentre operando el cajero automático. De la misma forma, los cajeros automáticos con recinto ubicados en zonas con niveles de alto riesgo deberán contar con mecanismos automáticos de autenticación que restrinjan el acceso de personas no autorizadas a dichos ambientes o formas alternativas que impidan el acceso de personas no autorizadas al recinto, para precautelar la seguridad de los consumidores financieros. Estas formas alternativas deben estar fundamentadas con un Informe del Gerente General, el cual debe estar a disposición de ASFI cuando así lo requiera.

a.2 Cajero automático sin recinto: La entidad supervisada debe contratar personal de vigilancia, ya sea un policía de seguridad o guardia privado y habilitar casetas según lo establecido en el Artículo 4°, Sección 3, del presente Reglamento.

b. Circuito cerrado de televisión: La entidad supervisada debe instalar una cámara en el interior del cajero automático que permita captar las imágenes de los tarjetahabientes al momento de realizar la operación, no debiendo dirigir la cámara hacia el teclado de los cajeros. Una vez que ingrese un cliente y durante el tiempo de permanencia en dicho ambiente, la entidad deberá contar con grabaciones continuas de las acciones realizadas por la persona y debe mantener el registro efectuado cumpliendo las disposiciones establecidas en el Artículo 11 de la Sección 3 del presente Reglamento. De la misma manera, la entidad supervisada debe instalar una cámara exterior, para la vigilancia del perímetro externo de cajeros automáticos con recinto identificados con riesgo alto;

c. Dispositivos de seguridad: Los cajeros automáticos internos o externos deben contar con dispositivos que permitan privacidad en el registro de operaciones de los clientes o usuarios de tarjetas de débito o crédito. Los dispositivos mínimos de seguridad son los siguientes:

1. Pantalla. Debe estar instalada en ángulos apropiados o contar con medidas antirreflectantes, que eviten que la acción del reflejo del sol afecte la privacidad de operación por parte del usuario;

2. Iluminación. El espacio donde se encuentra ubicado el cajero automático, debe estar adecuadamente iluminado;

3. **Protector de teclado.** Todos los cajeros automáticos deben contar con protectores de teclado para evitar que durante el marcado de la clave, esta pueda ser vista por terceras personas;
4. **Equipo anti–skimming.** El cajero automático debe contar con equipos anti – skimming en la ranura de ingreso de la tarjeta para garantizar las operaciones de los tarjetahabientes;
5. **Accesorios.** Los cajeros automáticos deben contar con accesorios adicionales de aseo y decoración y deben prevenir, desde su diseño e instalación, la comisión de actos de vandalismo a través de elementos de cierre y fijación, que eviten su retiro o la instalación de artefactos explosivos.

d. **Elementos disuasivos y teléfonos de información:** Los cajeros automáticos deben contar con carteles y señales que anuncien que el cajero automático cuenta con medidas de seguridad, así como con los números telefónicos de emergencia para comunicarse con la Entidad Supervisada a la que pertenecen y con la empresa de liquidación y compensación de tarjetas de pago; estos números deben ser de fácil identificación tanto en el ambiente del recinto como en la pantalla del cajero automático;

e. **Cerradura de la caja fuerte:** La puerta de la caja fuerte del cajero automático, debe poseer un mecanismo adicional a la cerradura que permita el bloqueo automático de ésta ante un incidente de seguridad física;

f. **Anclaje:** El cajero automático debe encontrarse sólidamente anclado al piso;

g. **Protección del cableado:** Todo el cableado para el funcionamiento del cajero automático y el sistema de alarmas deben estar debidamente protegidos para evitar posibles accidentes o actos de sabotaje, debiendo inclusive proteger los compartimientos del sistema de comunicación.

Artículo 9° - (Casas de cambio) Las Casas de Cambio con Personalidad Jurídica, deben identificar el nivel de riesgo ante incidentes de seguridad física al que se encuentran expuestas su oficina central y agencias de cambio de acuerdo a lo establecido en el Artículo 2°, Sección 2 del presente Reglamento e implementar mínimamente las medidas específicas de seguridad física, señaladas a continuación:

Requisitos de Seguridad Física	Niveles de Seguridad		
	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Equipos de Atesoramiento			
Caja Fuerte Bóveda	☑	☑	☑
Personal de Vigilancia			
Un (1)Policía de Seguridad	-	-	☑
Un (1) Policía de Seguridad o Un (1) Guardia Privado	-	☑	-
Un (1) Guardia Privado	☑	-	-

☑ = Indispensable -= No indispensable

Artículo 10° - (Empresas de giro y remesas de dinero) Las Empresas de Giro y Remesas de Dinero, deben identificar el nivel de riesgo ante incidentes de seguridad física al que se encuentran expuestos sus puntos de atención financiero de acuerdo a lo establecido en el Artículo 2°, Sección

2, del presente Reglamento e implementar mínimamente las medidas específicas de seguridad física, señaladas a continuación:

Requisitos de Seguridad Física	Niveles de Seguridad		
	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Equipos de Atesoramiento			
Caja Fuerte Bóveda	☑	☑	☑
Personal de Vigilancia			
Un (1)Policía de Seguridad	-	-	☑
Un (1) Policía de Seguridad o Un (1) Guardia Privado	-	☑	-
Un (1) Guardia Privado	☑	-	-

☑ = Indispensable -= No indispensable

Artículo 11° - (Empresas de transporte de material monetario y valores) La Empresa de Transporte de Material Monetario y Valores (ETM) que brinda servicio al Sistema Financiero o la Entidad de Intermediación Financiera con servicio propio de transporte de material monetario y valores (ESPT), debe cumplir con las medidas de seguridad señaladas en el Reglamento Operativo para Empresas Privadas de Vigilancia, para la prestación de sus servicios.

Adicionalmente, la ETM que realiza la custodia de material monetario y valores en sus oficinas, determinará la implementación de equipos de atesoramiento, ambientes específicos para el procesamiento de efectivo (cuando corresponda), sistemas de alarmas, monitoreo y dotación de personal de vigilancia, en función a lo establecido en la Política de Seguridad Física aprobada por el Directorio u Órgano equivalente considerando el nivel de riesgo.

Finalmente, la entidad supervisada para realizar el transporte de material monetario y/o valores entre localidades que no sean ciudades capitales de departamento, debe implementar las medidas de seguridad física que considere necesarias en función a los riesgos asociados al traslado de material monetario y/o valores a dichas áreas, tomando en cuenta al menos los siguientes aspectos:

- **a.** Preservación de la seguridad de la vida de las personas;
- **b.** Accesibilidad a la localidad;
- **c.** Zonas geográficas de riesgo identificadas por la autoridad competente en temas de seguridad ciudadana;
- **d.** Montos o valor de material monetario y/o valores a ser trasladado.

Artículo 12° - (Local compartido) La entidad supervisada, en función al tipo de servicios que realice y el nivel de riesgo al que se encuentra expuesto el local compartido, determinará la implementación de medidas de seguridad, en el marco de lo dispuesto en la Sección 3 del presente Reglamento, de conformidad al acuerdo establecido con la entidad financiera que le comparte el espacio físico.

Artículo 13° - (Empresas Administradoras de Tarjetas Electrónicas) Las Empresas Administradoras de Tarjetas Electrónicas, deben identificar el nivel de riesgo ante incidentes de seguridad física al que se encuentran expuestos sus puntos de atención financiero de acuerdo a lo establecido en el Artículo 2° de la Sección 2 del presente Reglamento e implementar mínimamente las medidas específicas de seguridad física, señaladas a continuación:

Requisitos de Seguridad Física	Niveles de Seguridad		
	Riesgo Bajo	Riesgo Medio	Riesgo Alto
Equipos de Atesoramiento			
Caja Fuerte Bóveda	☑	☑	☑
Personal de Vigilancia			
Un (1)Policía de Seguridad	-	-	☑
Un (1) Policía de Seguridad o Un (1) Guardia Privado	-	☑	-
Un (1) Guardia Privado	☑	-	-

☑ = Indispensable -= No indispensable

SECCIÓN 5: OTRAS DISPOSICIONES

Artículo 1° - (Empresas de arrendamiento financiero) En función a la política de seguridad física aprobada por el Directorio u Órgano equivalente, la empresa de arrendamiento financiero es responsable de velar porque las transacciones de efectivo realizadas con sus clientes, a través de PAF de entidades de intermediación financiera, cuenten con las medidas de seguridad física necesarias según lo establecido en el presente Reglamento.

Artículo 2° - (Empresas de servicio de pago móvil) En función a la Política de Seguridad Física aprobada por el Directorio u Órgano equivalente, la Empresa de Servicio de Pago Móvil (ESPM), es responsable de la implementación de medidas de seguridad física adecuadas para la prestación de sus servicios en las instalaciones de los corresponsales contratados, según lo establecido en el Artículo 7° de la Sección 4 del presente Reglamento.

Artículo 3° - (Reportes de información) La entidad supervisada debe contar con mecanismos que permitan el flujo de información adecuado para la toma de decisiones oportunas, relativas a la gestión de seguridad física en sus instalaciones.

Artículo 4° - (Resguardo de la información de seguridad física) La entidad supervisada debe disponer de la custodia en la bóveda o caja fuerte, de los planes de seguridad física, planos o croquis que contengan referencias sobre los sistemas de seguridad implementados, estando prohibida la obtención de copias o fotocopias que no hubieran sido reportadas por escrito al Comité de seguridad física.

Artículo 5° - (Situaciones de fuerza mayor) Por motivos fundados, razones de fuerza mayor o situaciones de riesgo imprevistas que impidan la continuidad en la prestación del servicio del personal de vigilancia, la entidad supervisada podrá utilizar el personal de las Fuerzas Armadas del Estado Plurinacional de Bolivia, previa autorización de las instancias competentes del Gobierno, debiendo comunicar oportunamente estas medidas a la Autoridad de Supervisión del Sistema Financiero.

Artículo 6° - (Sanciones) El incumplimiento o inobservancia al presente Reglamento dará lugar al inicio del proceso administrativo sancionatorio.

SECCIÓN 6: ROL DE LA UNIDAD DE AUDITORÍA INTERNA

Artículo Único - (Rol de auditoría interna) La Unidad de Auditoria Interna debe desempeñar un rol independiente en la Gestión de Seguridad Física, debiendo, mínimamente cumplir con las siguientes funciones:

a. Verificar la implementación de lo dispuesto en las políticas, procedimientos y planes diseñados para la Gestión de Seguridad Física;

b. Verificar que la Unidad de Seguridad Física cumpla con las obligaciones y responsabilidades encomendadas;

c. Elevar informes al Directorio u órgano equivalente, a través de su Comité de Auditoría o Consejo de Vigilancia, según corresponda, acerca de los resultados obtenidos y las recomendaciones sugeridas, derivadas de las revisiones;

d. Efectuar seguimiento de las observaciones y/o recomendaciones emitidas y comunicar los resultados obtenidos al Directorio u Órgano equivalente, a través de su Comité de Auditoría o Consejo de Vigilancia, según corresponda.

SECCIÓN 7: DISPOSICIONES TRANSITORIAS

Artículo 1° - (Plazo de implementación) Las entidades supervisadas deben adecuarse a lo determinado en el presente Reglamento en un plazo no mayor a dieciocho (18) meses, a partir de su emisión.

Artículo 2° - (Plazo de implementación de seguridad para cajeros automáticos) Las entidades supervisadas deben cumplir con lo establecido en el Artículo 8° de la Sección 4 del presente Reglamento, hasta el 31 de diciembre de 2016.

CONTROL DE VERSIONES

L03T07C03		Secciones							Anexos
Circular	**Fecha**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	
ASFI/546/2018	22/05/2018					*			
ASFI/476/2017	17/08/2017	*	*						
ASFI/381/2016	30/03/2016	*	*		*	*		*	
ASFI/353/2015	30/11/2015	*			*			*	
ASFI/290/2015	26/03/2015				*				
ASFI/251/2014	22/07/2014	*	*	*	*	*	*		**1**
ASFI/188/2013	19/07/2013			*					
ASFI/178/2013	23/05/2013	*	*	*	*				
ASFI/146/2012	17/10/2012	*	*	*	*	*		*	**1, 2, 3**