TÍTULO I

REQUISITOS DE SEGURIDAD

TABLA DE CONTENIDO

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

SECCIÓN 1: DISPOSICIONES GENERALES

Artículo 1° - (Objeto) El presente Reglamento tiene por objeto establecer los requisitos mínimos que las entidades supervisadas inscritas en el Registro del Mercado de Valores (RMV), deben cumplir para la gestión de seguridad de la información, de acuerdo a su naturaleza, tamaño y complejidad de operaciones.

Artículo 2° - (Ámbito de aplicación) Están comprendidas en el ámbito de aplicación del presente Reglamento, las Agencias de Bolsa, Sociedades Administradoras de Fondos de Inversión, Entidades de Depósito de Valores, Bolsas de Valores, Sociedades de Titularización y Calificadoras de Riesgo constituidas en Bolivia, inscritas en el Registro del Mercado de Valores, que cuenten con autorización de funcionamiento emitida por la Autoridad de Supervisión del Sistema Financiero (ASFI), denominadas en adelante como entidades supervisadas.

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

a. **Activo de información:** En seguridad de la información, corresponde a 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*):** Contrato en el que 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. **Análisis y evaluación de riesgos en seguridad de la Información:** Proceso por el cual se identifican los activos de información, las amenazas y vulnerabilidades a las que se encuentran expuestos, con el fin de generar controles que minimicen los efectos de los posibles incidentes de seguridad de la información;

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

e. **Cajeros automáticos:** Máquinas equipadas con dispositivos electrónicos o electromecánicos que permiten a los usuarios de servicios financieros realizar compras y/o rescate de cuotas en efectivo, consultas de saldos, transferencias de fondos entre cuentas o pagos de servicios, mediante el uso de un Instrumento Electrónico de Pago (IEP). Los cajeros automáticos son también conocidos por su sigla en inglés: ATM (Automated Teller Machine);

f. **Centro de procesamiento de datos (CPD):** Ambiente físico clasificado como área de exclusión, donde están ubicados los recursos utilizados para el procesamiento de información;

g. **Centro de procesamiento de datos alterno:** Lugar alternativo provisto de equipos computacionales, equipos de comunicación, estaciones de trabajo, enlaces de comunicaciones, fuentes de energía y accesos seguros que se encuentran instalados en una ubicación geográfica distinta al Centro de Procesamiento de Datos;

h. **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;

i. **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 equipo computacional o red;

j. **Cortafuegos (*Firewall*)**: Dispositivo o conjunto de dispositivos (software y/o hardware) configurados para permitir, limitar, cifrar, 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;

k. **Equipo crítico:** Equipo de procesamiento de datos que soporta las principales operaciones de la entidad supervisada;

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

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

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

o. **Intranet:** Red interna de computadoras que haciendo uso de tecnología de Internet, permite compartir información o programas;

p. **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 las aplicaciones;

q. **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;

r. **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;

s. **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 interrumpidas dentro de un tiempo predeterminado, después de una interrupción o desastre;

t. **Principio de menor privilegio:** Establece que cada programa y cada usuario del sistema de información debe operar utilizando los privilegios estrictamente necesarios para completar el trabajo;

u. **Proceso crítico:** Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de la entidad supervisada;

v. **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;

w. **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;

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

y. **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;

z. **Pruebas de intrusión:** 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 red interna, desde Internet, accesos remotos o cualquier otro medio;

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

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

cc. **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;

dd. Sitio externo de resguardo: Ambiente externo al Centro de Procesamiento de Datos, donde se almacenan todos los medios de respaldo, documentación y otros recursos de tecnología de información catalogados como críticos, necesarios para soportar los planes de continuidad del negocio y contingencias tecnológicas;

ee. 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;

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

gg. Tecnología de 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;

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

ii. 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 los 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 de la Información (TI), que esté alineado con la estrategia institucional y que considere la naturaleza, tamaño, complejidad de las operaciones, procesos, estructura, análisis y evaluación de riesgos en seguridad de la información realizado. Este documento debe ser aprobado por su Directorio.

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 TI) La infraestructura del área de tecnología de la información debe ser consistente con la naturaleza, tamaño y complejidad de las operaciones que realiza la entidad supervisada.

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.

Artículo 5° - (Comité de tecnología 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 tecnologías de la información.

Este Comité estará conformado al menos por: un miembro del Directorio, 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 sistema 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 tecnología de la información) La entidad supervisada, de acuerdo a su estructura organizativa, debe conformar un Comité Operativo de Tecnología de la Información, el cuál debe estar constituido por el nivel ejecutivo y los funcionarios encargados de las diferentes áreas que constituyen la unidad de TI. Este Comité estará encargado de coordinar el trabajo al interior de dicha unidad.

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 y estar archivadas.

Artículo 7° - (Responsable de la función de la seguridad de la información) Con el fin de establecer los mecanismos para la administración y el control de la seguridad sobre el acceso lógico y físico a los distintos ambientes tecnológicos y recursos de información, la entidad supervisada debe establecer 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 área 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, así como 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 fin, que deben estar formalmente establecidos.

El resultado obtenido del análisis y evaluación de riesgos en seguridad de la información efectuado, debe estar contenido en un informe dirigido a la Gerencia General, para su posterior presentación al Directorio.

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° (Políticas de seguridad de la información) De acuerdo con su estrategia de seguridad de la información y el análisis y evaluación de riesgos en seguridad de la información efectuado, la entidad supervisada debe tener formalizadas por escrito, actualizadas e implementadas las políticas aprobadas por el Directorio.

Las políticas de seguridad de la información, 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 las políticas de seguridad de la información, 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 la custodia de licencias.

Artículo 4° (Acuerdo de confidencialidad) Como parte de las obligaciones contractuales, de los Directores, 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 y mantener actualizado un inventario de los activos de información y asignar responsabilidades respecto a su protección.

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 su 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, según el tipo de información y 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 y de acuerdo al nivel de clasificación otorgada 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.

La evaluación de vulnerabilidades técnicas, debe efectuarse por lo menos una (1) vez por año y ante un cambio significativo en la infraestructura tecnológica. La ejecución de pruebas de seguridad debe considerar la realización de pruebas de intrusión controladas internas y externas.

El conjunto de políticas y procedimientos que constituyen la gestión de vulnerabilidades técnicas deben ser revisados y actualizados permanentemente.

La entidad supervisada debe exigir a las empresas y/o personas que le presten servicios de evaluación de seguridad de la información, la respectiva documentación que acredite la experiencia necesaria para realizar este tipo de trabajos, adicionalmente, debe 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.

Artículo 9° (Clasificación de áreas de tecnología de la información) La entidad supervisada debe identificar y clasificar las áreas de tecnología de la información como áreas de exclusión que requieren medidas de protección y acceso restringido.

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

- **a.** Ubicación del Centro de Procesamiento de Datos al interior de la entidad supervisada;
- **b.** Espacio acorde y suficiente a la cantidad de equipos instalados;
- **c.** Energía regulada de acuerdo a 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 a 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 de protección física) La entidad supervisada debe contar con manuales de procedimientos de protección física para el Centro de Procesamiento de Datos, que consideren mínimamente, los siguientes aspectos:

a. Operación y mantenimiento del Centro de Procesamiento de Datos;

b. Administración de accesos;

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

Artículo 12° (Protección de equipos informáticos) 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 Televisión).

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 los 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° (Destrucción controlada de medios de respaldo) La entidad supervisada debe establecer procedimientos para la destrucción controlada de los medios de almacenamiento de respaldo utilizados.

Artículo 17° (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, E jecutivos, funcionarios, consultores y personal eventual, deben ser definidas y documentadas en concordancia con la Política de Seguridad de la Información;
- **b.** Se debe asegurar que los Directivos, Ejecutivos, funcionarios, consultores y personal eventual, estén conscientes de las amenazas y riesgos de incidentes de seguridad de la información, y que estén capacitados para aceptar y cumplir con la Política de Seguridad de la Información en el desarrollo normal de su trabajo;
- **c.** Debe existir un proceso disciplinario formal para Directivos, Ejecutivos, funcionarios, consultores y personal eventual que han cometido faltas y/o violaciones a la Política de Seguridad de la Información de la entidad supervisada.

Artículo 18° (Custodia y conservación de datos) Los documentos relacionados con sus operaciones, microfilmados o registrados en medios magnéticos y/o electrónicos, deben ser conservados y permanecer en custodia por un período no menor a diez (10) años.

La documentación que se constituya en instrumento probatorio en un proceso administrativo, judicial u otras instancias, que se encuentren pendientes de resolución, no debe ser objeto de destrucción controlada, en resguardo de los derechos de las partes en conflicto.

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 a la Política de Seguridad de la Información, para la administración de usuarios de los sistemas informáticos, 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 al 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 sobre 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, 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 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, con el fin de detectar 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 el 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 y el análisis y evaluación de riesgos en seguridad de la información efectuado.

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.

Artículo 5° - (Integridad y validez de la información) La entidad supervisada en 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, operaciones concretadas 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 debe implementar controles que garanticen la separación de los ambientes de desarrollo, prueba y producción, acordes a la segregación de funciones que debe existir en cada caso.

Artículo 10° - (Datos de prueba en ambientes de desarrollo) Para utilizar información de producción en los ambientes de desarrollo y pruebas, 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 y registrar los resultados obtenidos en el proceso de migración, cuyo informe permanecerá 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 los 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 que considere 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 la 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 TELECOMUNICACIONES

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 transmiten 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 de los sistemas 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 las líneas de telecomunicación, 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 (firewall), 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 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 en vigencia para el cableado estructurado de la red por empresas autorizadas.

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 transferencias electrónicas o transacciones electrónicas debidamente autorizadas por ASFI, 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 debe proveer un perfil de seguridad que garantice que las transferencias y/o transacciones electrónicas sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, 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, debiendo utilizar las políticas de seguridad de la información indicadas 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 del nivel de robustez del sistema de autenticación para aquellas transacciones y/o transacciones electrónicas, 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 sistema 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 transferencias 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:** La existencia de sitios web de las entidades supervisadas, debe estar avalada en cuanto a su propiedad y seguridad de la información expuesta, por una certificadora nacional o internacional, debidamente autorizada por la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT).

Los certificados digitales emitidos por entidades certificadoras extranjeras deben ser homologados por una certificadora nacional;

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 cuenta, tanto por terminales ATM como en los sistemas disponibles en la web, en un determinado período;

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.

i. **Acuerdos privados**: Para la realización de transacciones y/o transferencias de información entre entidades supervisadas, deben celebrarse acuerdos privados que estén debidamente firmados y protocolizados, que consideren los lineamientos de seguridad establecidos a partir de lo dispuesto en el Artículo 2° de la Sección 3 del presente Reglamento.

Artículo 2° - (Contrato formal) 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 estos suscriban para el efecto. De manera enunciativa, dicho contrato debe contener mínimamente las siguientes condiciones:

a. El cliente será responsable exclusivo del uso y confidencialidad de la clave de acceso, que utilizará en sus operaciones electrónicas. Además, se debe indicar que la contraseña será bloqueada automáticamente después de tres intentos fallidos, así como el procedimiento para solicitar su desbloqueo;

b. El tipo de operaciones que puede efectuar el cliente;

c. El horario y consideraciones de cierre diario de cada entidad supervisada, junto al 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 permitan establecer que los importes no superen el saldo disponible o el límite que para el efecto haya sido fijado;

f. 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 una entidad supervisada, efectúe transferencias y/o transacciones electrónicas, 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, implementado y aprobado por el Directorio, en concordancia con el Plan de Contingencias 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 que los tipos, volúmenes y costos de los incidentes de seguridad de la información 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. Violación de accesos;

11. Código malicioso;

12. Negación de servicio;

13. Errores resultantes de datos incompletos o no actualizados;

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

15. Mal uso de los sistemas de información;

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

17. 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 al menos 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, implementado y aprobado por el Directorio, que considere mínimamente:

- **a.** Objetivo;
- **b.** Metodología que incluya lo siguiente:
  - **1.** Análisis y evaluación de riesgo tecnológico;
  - **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 el análisis y evaluación de riesgo tecnológico efectuado 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, implementado y aprobado por el Directorio, que incluya al menos:

- **a.** Inicio del proyecto;
- **b.** Análisis y evaluación de riesgos en seguridad de la información;
- **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, reciban sesiones de capacitación de forma regular 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 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 realizar 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 remitido a ASFI para su conocimiento, hasta el 20 de diciembre del año anterior a su ejecución, cuando esta fecha coincida con un día feriado, sábado o domingo, el plazo se extenderá hasta el siguiente día hábil.

El alcance de las pruebas de contingencia tecnológica y de continuidad del negocio, debe considerar aplicaciones individuales, escenarios de prueba integrados, pruebas de punta a punta y pruebas integradas con el proveedor. 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, tamaño y esté de acuerdo al análisis y evaluación de riesgo tecnológico realizado y a 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, el centro alterno deberá funcionar hasta que se resuelva la contingencia.

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 externos de tecnología de información, la entidad supervisada debe contar con un procedimiento documentado, formalizado, actualizado, implementado y aprobado por el Directorio, 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 tercerizado o ejecución de sistemas en lugar externo, la entidad supervisada debe considerar al menos los siguientes aspectos:

a. Es deber del Directorio y de la Gerencia General, 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, que señale el cumplimiento de lo dispuesto en los numerales precedentes.

Dicha documentación debe permanecer actualizada en la entidad supervisada, a disposición de ASFI;

f. El Gerente General de la entidad supervisada, debe remitir a ASFI hasta el 31 de marzo de cada año o el siguiente día hábil en caso de feriado o fin de semana, 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.

Artículo 4° - (Contrato con proveedor de procesamiento externo) Es responsabilidad del Directorio y de la Gerencia General de la entidad supervisada, la suscripción del contrato con la empresa proveedora de los servicios de procesamiento, el que entre otros aspectos debe especificar lo siguiente:

a. La naturaleza y especificaciones del servicio de procesamiento contratado;

b. La responsabilidad que asume la empresa proveedora, de 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 la empresa proveedora de tecnologías 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 empresa proveedora 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 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 de riesgo tecnológico y de costo-beneficio;

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

e. Disponibilidad del código fuente.

Asimismo, los contratos con el proveedor deben indicar los requisitos de seguridad establecidos por la entidad supervisada. Si la funcionalidad del producto ofrecido, no satisface los requisitos de seguridad de la información establecidos por ésta, se deben reconsiderar los riesgos y controles asociados antes de adquirir el producto.

Artículo 6° - (Desarrollo y mantenimiento de programas, sistemas o aplicaciones a través de proveedores externos) La contratación de empresas encargadas del desarrollo y mantenimiento de sistemas de información, es responsabilidad de la entidad supervisada y debe considerar al menos los siguientes aspectos:

a. Que la empresa contratada cuente con solidez financiera, personal con conocimiento especializado y experiencia en el desarrollo de sistemas y/o 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 de sistemas, en caso de cambio de proveedor externo u otro factor no previsto;

d. Exigir al proveedor de tecnologías de información que cumpla con las directrices de seguridad de la información contempladas en el Artículo 1° de la presente Sección.

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 de programación y sistema 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 los 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 consecuentes de negligencia u omisión atribuible 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. Asegurar que 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 acorde a 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, etc.);

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, para los cuales debe considerar 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), en el contrato respectivo, de acuerdo a su análisis de riesgo tecnológico y de acuerdo a la criticidad de sus operaciones.

Los parámetros del Acuerdo de Nivel de Servicio, deben referirse al tipo de servicio, soporte y asistencia a clientes, previsiones para seguridad y datos, garantías del sistema y tiempos de respuesta, disponibilidad del sistema, conectividad, multas por caídas del sistema y/o líneas alternas para el servicio.

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, o el siguiente día hábil en caso de feriado o fin de semana, el informe elaborado. Dicha labor podrá realizarse a través de evaluaciones internas y/o externas;

b. Verificar la ejecución de las pruebas solicitadas en el Artículo 8° de la Sección 3, del presente Capítulo y comunicar el resultado del análisis de vulnerabilidades a ASFI, hasta el 15 de noviembre de cada año o el siguiente día hábil en caso de feriado o fin de semana, a través de un informe elaborado por el Auditor Interno o la Unidad de Auditoría Interna;

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 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.

SECCIÓN 13: OTRAS DISPOSICIONES

Artículo 1° - (Responsabilidad) El cumplimiento, implementación y difusión interna del presente Reglamento es responsabilidad del Directorio y 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, debe 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 procedimiento 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 30 de noviembre de 2016.

La entidad supervisada debe elaborar un plan de acción que detalle las acciones a seguir y cuente con un cronograma enmarcado en el plazo establecido por ASFI, para el cumplimiento y adecuación a la presente normativa, el cual debe ser aprobado por su Directorio y permanecer a disposición de la Autoridad de Supervisión del Sistema de Financiero.

La entidad supervisada, debe remitir el citado plan de acción a ASFI hasta el 31 de diciembre de 2015 y de manera trimestral informes de avance que muestren el grado de cumplimiento.

Artículo 2° - (Auditor Interno) Las funciones a ser desarrolladas por el Auditor Interno o la Unidad de Auditoría Interna, conforme lo establecido en la Sección 12 del presente Reglamento, son aplicables para la gestión 2017 y posteriores, debiendo la entidad supervisada remitir por primera vez, los informes señalados en los incisos a y b, Artículo Único de la citada sección, de acuerdo al siguiente detalle:

1. Hasta el 15 de noviembre de 2017, el informe dispuesto en el inciso b;
2. Hasta el 15 de enero de 2018, el informe determinado en el inciso a.

CONTROL DE VERSIONES

Fecha	Versión	Circular	Resolución	Sección nueva o modificada	RNMV
18/12/2017	Modificación 2	ASFI/507/2017	ASFI/1121/2016	1, 3, 4 , 5, 6, 11	Capítulo I
29/11/2016	Modificación 1	ASFI/433/2016	ASFI/1121/2016	14	Capítulo I
14/10/2015	Inicial	ASFI/336/2015	ASFI/838/2015		Capítulo I