

CIRCULAR ASFI/ 193 /2013

La Paz, 16 SET. 2013

Señores

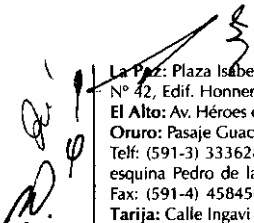

Presente.-

**REF: MODIFICACIONES DEL REGLAMENTO DE REQUISITOS
MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LA
ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y
TECNOLOGÍAS RELACIONADAS**

Señores:

Para su aplicación y estricto cumplimiento, se adjunta a la presente la Resolución que aprueba y pone en vigencia las modificaciones al **REGLAMENTO DE REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS** las cuales consideran principalmente los siguientes aspectos:

1. La denominación de "Reglamento de Requisitos Mínimos de Seguridad Informática Para la Administración de Sistemas de Información y Tecnologías Relacionadas" cambia por "Reglamento para la Gestión de Seguridad de la Información".
2. Se modifica la denominación de la Sección 1 de "Marco General" por la de "Disposiciones Generales".
3. Se elimina el Artículo 1º, Sección 1 referido a "Aspectos Generales" con la consiguiente modificación de la numeración de los artículos siguientes.
4. Se modifica el objeto del Reglamento establecido en el Artículo 1º de la Sección 1, en cuanto a la gestión de seguridad de la información que deben cumplir las entidades supervisadas sujetas al ámbito de aplicación.



La Paz: Plaza Isabel La Católica N° 2507 - Telf: (591-2) 2174444 - 2431919 - Fax: (591-2) 2430028 - Casilla N° 447 (Oficina Central) - Calle Batallón Colorados N° 42, Edif. Honnen - Telf: (591-2) 2911790 - Calle Reyes Ortiz esq. Federico Zuazo Edif. Gundlach, Torre Este, Piso 3 - Telf: (591-2) 2311818 - Casilla N° 6118 El Alto: Av. Héroes del Km. 7 N° 11, Villa Bolívar "A" - Telf: (591-2) 2821484 • Potosí: Plaza Alonso de Ibañez N° 20, Galería El Siglo, Piso 1 - Telf: (591-2) 6230858 Oruro: Pasaje Guachalla, Edif. Cámara de Comercio, Piso 3, Of. 307 - Telf: (591-2) 5117706 - 5112468 • Santa Cruz: Av. Irala N° 585 - Of. 201, Casilla N° 1359 Telf: (591-3) 3336288 Fax: (591-3) 3336289 • Cobija: Calle 16 de Julio N° 149 (frente al Kinder América) - Telf: (591-3) 8424841 • Trinidad: Calle La Paz esquina Pedro de la Rocha N°55, Piso 1 - Telf/Fax (591-3)4629659 • Cochabamba: Av. Salamanca esquina Lanza, Edif. CIC, Piso 4 - Telf: (591-4)4583800 Fax: (591-4) 4584506 • Sucre: Calle Dalence N° 184 (entre Bolívar y Nicolás Ortiz) - Telf: (591-4) 6439777 6439775 - 6439774 - Fax: (591-4) 6439776 Tarija: Calle Ingavi N° 282 esquina Méndez - Telf: (591-4) 6113709 • Línea gratuita: 800 103 103 • sitio web: www.asfi.gob.bo

5. Se mejora la redacción del Artículo 2°, Sección 1, señalando de manera inextensa las entidades supervisadas que se encuentran bajo el ámbito de aplicación del Reglamento.
6. El artículo 3°, Sección 1, referido a "Definiciones" se reestructura, mediante la incorporación, modificación y eliminación de conceptos.
7. En la Sección 1, se introduce el Artículo 4° relativo a los elementos de la seguridad de la información.
8. Se sustituye el contenido y denominación de la Sección 2 de "Requisitos Mínimos de Seguridad Informática" por la de "Planificación Estratégica, Estructura y Organización de los Recursos de Tecnología de Información (TI)".

En dicha Sección se incorpora disposiciones referidas a la planificación estratégica, estrategia de seguridad de la información, infraestructura del área de TI, estructura organizativa, Comité de Tecnología de la Información, Comité Operativo de TI y responsable de la función de seguridad de la información.

9. La Sección 3 referida a "Contrato con Proveedores de Tecnologías de Información" es reemplazada con disposiciones relativas a la "Administración de la Seguridad de la Información".

Los artículos introducidos se refieren a la implementación del análisis de riesgo tecnológico, políticas de seguridad de la información, licencia de software, acuerdo de confiabilidad, inventario de activos de información, clasificación de la información, propietarios de la información, análisis de vulnerabilidades técnicas, clasificación de áreas de tecnología de la información, características del centro de procesamiento de datos, manuales de procedimientos, protección de equipos informáticos, suministro eléctrico, seguridad de cableado de red, pruebas a dispositivos de seguridad, destrucción controlada de medios de respaldo y responsabilidad en la gestión de seguridad de la información.

10. Se modifica la denominación y contenido de la Sección 4 "Transferencias y Transacciones Electrónicas", por la de "Administración del Control de Accesos" cuyas disposiciones se refieren a: administración de cuentas de usuarios, administración de privilegios, administración de contraseñas de usuarios y a los registros de seguridad y pistas de auditoría.
11. Las disposiciones transitorias contenidas en la Sección 5, se sustituyen con las relativas a "Desarrollo, Mantenimiento e Implementación de Sistemas de Información" que abarcan las políticas y procedimientos, desarrollo y mantenimiento de programas, sistemas o aplicaciones informáticas, requisitos

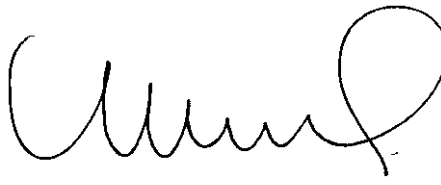
de seguridad de los sistemas, estándares para el procesos de ingeniería del software, implementación de controles, integridad y validez de la información, controles criptográficos, control de accesos al código fuente de programas, procedimientos de control de cambios, ambientes de desarrollo, prueba y producción, datos de prueba en ambientes de desarrollo, migración de sistemas de información y parches de seguridad.

12. Se introduce la Sección 6, referida a la "Gestión de Operaciones de Tecnología de Información", cuyas disposiciones se refieren a la gestión de operaciones, administración de bases de datos, respaldo o copia de seguridad y al mantenimiento preventivo de los recursos tecnológicos.
13. Se adiciona la Sección 7 denominada "Gestión en Redes y Comunicaciones" cuyo articulado se refiere a la implementación de políticas y procedimientos, estudio de capacidad y desempeño, exclusividad del área de telecomunicaciones, activos de información componentes de la red, configuración de hardware y software y la documentación técnica.
14. Se incluye la Sección 8 "Gestión de Seguridad en Transferencias y Transacciones Electrónicas", cuyas disposiciones se refieren a requisitos de los sistemas de transferencia y transacción electrónica, contrato formal y cifrado de mensajes y archivos.
15. Se incorpora la Sección 9 referida a la "Gestión de Incidentes de Seguridad de la Información", con un artículo único.
16. Se añade la Sección 10 relativa a la "Continuidad del Negocio" con disposiciones referidas al Plan de Contingencias Tecnológicas, Plan de Continuidad del Negocio y la capacitación para su aplicación, realización de pruebas, y control de dichos planes, así como el establecimiento del centro de procesamiento de datos alterno.
17. Se agrega la Sección 11 "Administración de Servicios y Contratos con Terceros Relacionados con Tecnología de la Información", cuyas disposiciones se refieren a la administración de servicios y contratos con terceros, evaluación y selección de proveedores, procesamiento de datos o ejecución de sistemas en lugar externo, contrato con proveedor de procesamiento externo, adquisición de sistemas de información, desarrollo y mantenimiento de programas, sistemas o aplicaciones a través de proveedores externos, contrato con empresas encargadas del desarrollo y mantenimiento de programas, sistemas o aplicaciones, otros servicios y acuerdo de nivel de servicio (SLA).

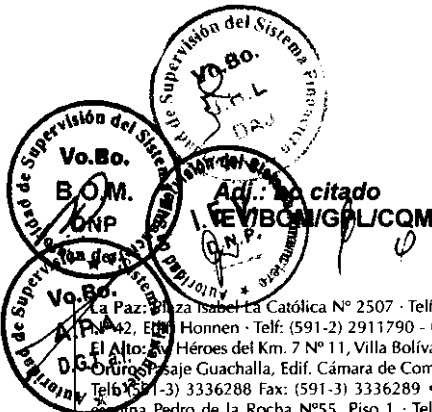
18. Se inserta la Sección 12 "Rol de la Auditoría Interna", con un artículo único, relativo a las funciones que debe cumplir la Unidad de Auditoría Interna.
19. Se introduce la Sección 13 relativa a "Otras Disposiciones" relacionadas con la responsabilidad en cuanto al cumplimiento y difusión del Reglamento, normas y estándares internacionales aplicables, herramientas informáticas, así como las sanciones derivadas de su incumplimiento e inobservancia.
20. Se incorpora la Sección 14 "Disposiciones Transitorias", en la cual se establece el plazo de adecuación y cronograma para dar cumplimiento a lo dispuesto en el Reglamento.

El Reglamento para la Gestión de Seguridad de la Información, será incorporado en el Libro 3°, Título VII, Capítulo II, de la Recopilación de Normas para Bancos y Entidades Financieras.

Atentamente,



Lenny T. Valdivia Bautista
DIRECTORA EJECUTIVA a.i.
Autoridad de Supervisión
del Sistema Financiero



La Paz: Plaza Isabel La Católica N° 2507 - Telf: (591-2) 2174444 - 2431919 - Fax: (591-2) 2430028 - Casilla N° 447 (Oficina Central) - Calle Batallón Colorados N° 42, Edif. Honnen - Telf: (591-2) 2911790 - Calle Reyes Ortiz esq. Federico Zuazo Edif. Gundlach, Torre Este, Piso 3 - Telf: (591-2) 2311818 - Casilla N° 6118
El Alto: Av. Héroes del Km. 7 N° 11, Villa Bolívar "A" - Telf: (591-2) 2821484 • Potosí: Plaza Alonso de Ibañez N° 20, Galería El Siglo, Piso 1 - Telf: (591-2) 6230858
Oruro: Pasaje Guachalla, Edif. Cámara de Comercio, Piso 3, Of. 307 - Telf: (591-2) 5117706 - 5112468 • Santa Cruz: Av. Irala N° 585 - Of. 201, Casilla N° 1359
Telf: (591-3) 3336288 Fax: (591-3) 3336289 • Cobija: Calle 16 de Julio N° 149 (frente al Kinder América) - Telf: (591-3) 8424841 • Trinidad: Calle La Paz
esquina Pedro de la Rocha N° 55, Piso 1 - Telf/Fax (591-3) 4629659 • Cochabamba: Av. Salamanca esquina Lanza, Edif. CIC, Piso 4 - Telf: (591-4) 4583800
Fax: (591-4) 4584506 • Sucre: Calle Dalence N° 184 (entre Bolívar y Nicolás Ortiz) - Telf: (591-4) 6439777 6439775 - 6439774 - Fax: (591-4) 6439776
Tarija: Calle Ingavi N° 282 esquina Méndez - Telf: (591-4) 6113709 • Línea gratuita: 800 103 103 • sitio web: www.asfi.gob.bo

RESOLUCION ASFI N° 504/2013
La Paz, 16 SET. 2013

VISTOS:

Las Resoluciones SB N° 066/2003 y SB N° 079/2003 de 04 de julio y 12 de agosto de 2003, el Informe Técnico - Legal ASFI/DNP/R-135961/2013 de 9 de septiembre de 2013, referido a las modificaciones al **REGLAMENTO DE REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS**, y demás documentación que ver convino y se tuvo presente.

CONSIDERANDO:

Que, el Artículo 331 de la Constitución Política del Estado Plurinacional de Bolivia establece que las actividades de intermediación financiera, la prestación de servicios financieros y cualquier otra actividad relacionada con el manejo, aprovechamiento e inversión del ahorro, son de interés público y sólo pueden ser ejercidas previa autorización del Estado, conforme a Ley.

Que, el parágrafo I del Artículo 332 de la Constitución Política del Estado Plurinacional de Bolivia, determina que: "Las entidades financieras estarán reguladas y supervisadas por una institución de regulación de bancos y entidades financieras. Esta institución tendrá carácter de derecho público y jurisdicción en todo el territorio boliviano", reconociendo el carácter constitucional de la Autoridad de Supervisión del Sistema Financiero.

Que, el Artículo 137 del Decreto Supremo N° 29894 de 7 de febrero de 2009, establece que la ex Superintendencia de Bancos y Entidades Financieras se denominará Autoridad de Supervisión del Sistema Financiero y asumirá además las funciones y atribuciones de control y supervisión de las actividades económicas de valores.

Que, en virtud a la normativa señalada, mediante Resolución Suprema N° 05423 de 7 de abril de 2011, el señor Presidente del Estado Plurinacional, designó a la Dra.

Lenny Tatiana Valdivia Bautista, como Directora Ejecutiva a.i. de la Autoridad de Supervisión del Sistema Financiero.

CONSIDERANDO:

Que, el Artículo 153 de la Ley N° 1488 de Bancos y Entidades Financieras, especifica que la Superintendencia de Bancos y Entidades Financieras actual Autoridad de Supervisión del Sistema Financiero, tiene como objetivo principal mantener el sistema de intermediación financiera sano, eficiente y solvente.

Que, el numeral 7 del Artículo 154 de la Ley N° 1488 de Bancos y Entidades Financieras, faculta a la Autoridad de Supervisión del Sistema Financiero, elaborar y aprobar los reglamentos de las normas de control y supervisión sobre las actividades de intermediación financiera.

Que, la Ley N° 3076 de 20 de junio de 2005, en su numeral IV, Artículo 1 señala que la Autoridad de Supervisión del Sistema Financiero, tiene competencia privativa e indelegable para emitir regulaciones prudenciales.

CONSIDERANDO:

Que, el Artículo 3 de la Ley N° 1488 de Bancos y Entidades Financieras, establece que la Superintendencia de Bancos y Entidades Financieras, actualmente Autoridad de Supervisión del Sistema Financiero, emitirá la normativa de seguridad para las operaciones y transmisiones electrónicas efectuadas por las entidades de intermediación financiera.

Que, la Resolución SB N° 066/2003 de 4 de julio de 2003, aprobó y puso en vigencia la normativa referida a los Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas en Entidades Financieras, estableciendo que las entidades de intermediación financiera y empresas de servicios auxiliares financieros deben cumplir requisitos mínimos para administrar los sistemas de información y la tecnología que los soporta.

Que, la Resolución SB N° 79/2003 de 12 de agosto de 2003, aprobó y puso en vigencia la última modificación al Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas, estableciendo un tiempo adicional para que las entidades de intermediación financiera adecúen sus sistemas conforme reglamentación emitida al efecto.

CONSIDERANDO:

Que, el constante desarrollo tecnológico, así como la utilización de las nuevas tecnologías de información y comunicación (NTIC), por parte del sistema financiero en la mayoría de sus operaciones, requieren que los riesgos inherentes a la utilización de éstas sean administrados de manera efectiva.

Que, las buenas prácticas de seguridad de la información a nivel global, establecen ciertos estándares que sirven de guía a las empresas e instituciones para que puedan gestionar adecuadamente la información y la seguridad de la misma.

Que, la ocurrencia de eventos de fraude informático muestran que la seguridad de la información en las entidades supervisadas por la Autoridad de Supervisión del Sistema Financiero (ASFI), pueden ser vulneradas y por tanto es necesario que éstas entidades conozcan, asuman, gestionen y minimicen este tipo de riesgos.

Que, la evolución tecnológica de los sistemas de seguridad de la información, ha dado lugar a la implementación de políticas de Estado para la prevención y protección de los procesos de manejo y transferencia de datos informáticos, las cuales se reflejan en la incorporación de nuevos tipos penales en la legislación vigente, referidos a la sanción punitiva por manipulación informática y la alteración, acceso y uso indebido de datos informáticos, razón por la cual, en observancia a los preceptos señalados, es necesario establecer en la normativa regulatoria, procedimientos de seguridad de la información para las entidades supervisadas por ASFI.

Que, a fin de compatibilizar y actualizar criterios técnicos insertos en el Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas, con el contenido del estándar ISO/IEC/27002 publicado el 2005, corresponde introducir en el citado Reglamento los lineamientos establecidos en el mencionado estándar ISO/IEC/27002.

Que, la propuesta de modificaciones al Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas, implica que las entidades supervisadas deben desarrollar y adecuar sus estrategias, estructura, políticas, procedimientos y conformar una base de datos que coadyuve el desarrollo de sus actividades, es necesario establecer un plazo de adecuación para la respectiva implementación.

Que, del análisis efectuado por la Autoridad de Supervisión del Sistema Financiero de las vulnerabilidades y debilidades técnicas, a las que se encuentran expuestas las entidades supervisadas, es necesario señalar la vigencia de las instrucciones dispuestas en la Carta Circular ASFI/DEP/2999/2012 de 30 de mayo de 2012, relativa a la seguridad informática "Ethical Hacking", las mismas que quedaran sin efecto, una vez concluya el plazo de adecuación para la implementación de las modificaciones

propuestas al Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas.

Que, el proyecto de modificaciones al Reglamento sobre Requisitos Mínimos de Seguridad Informática para la Administración de Sistemas de Información y Tecnologías Relacionadas, se sustenta en el análisis y las consideraciones técnicas precedentemente expuestas, y en atención a que la emisión de las mismas pueden ser efectuadas por la Autoridad de Supervisión del Sistema Financiero, en ejercicio de la competencia privativa e indelegable para emitir normativa de regulación prudencial establecida en el numeral 7 del Artículo 154 de la Ley N° 1488 de Bancos y Entidades Financieras, y el Artículo 1 de la Ley N° 3076 de 20 de junio de 2005, consiguientemente, en virtud de los preceptos señalados se ha establecido la pertinencia para aprobar las modificaciones propuestas al mencionado Reglamento.

CONSIDERANDO:

Que, mediante Informe Técnico - Legal ASFI/DNP/135961/2013 de 9 de septiembre de 2013, la Dirección de Normas y Principios establece que no existe impedimento técnico ni legal para aprobar las modificaciones propuestas al **REGLAMENTO DE REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS** de la Recopilación de Normas para Bancos y Entidades Financieras.

POR TANTO:

La Directora Ejecutiva a.i. de la Autoridad de Supervisión del Sistema Financiero, en virtud de las facultades que le confiere la Constitución Política del Estado Plurinacional de Bolivia y demás normativa conexa y relacionada.

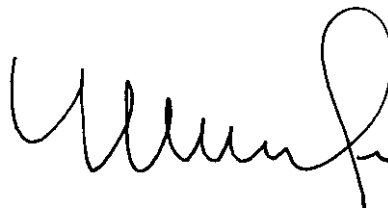
RESUELVE:

PRIMERO.- Aprobar y poner en vigencia las modificaciones al **REGLAMENTO DE REQUISITOS MÍNIMOS DE SEGURIDAD INFORMÁTICA PARA LA ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS**, bajo la denominación de **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, contenido en el Libro 3°, Título VII, Capítulo II de la Recopilación de Normas para Bancos y Entidades Financieras, conforme al texto que en Anexo forma parte de la presente Resolución.

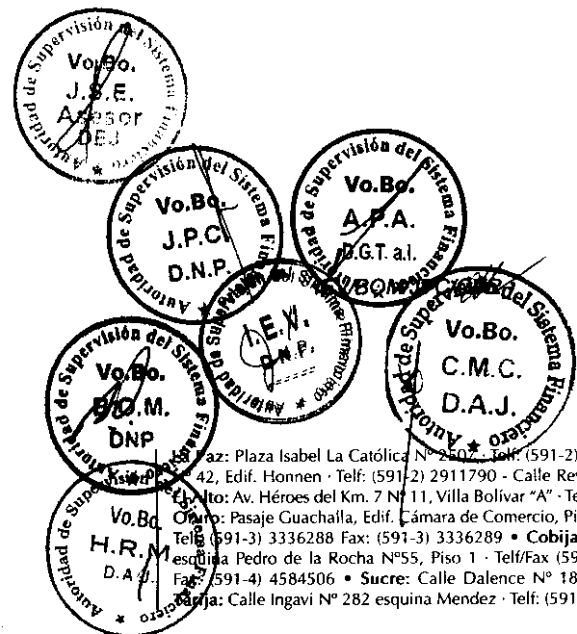
SEGUNDO.- Establecer un plazo hasta el 31 de diciembre de 2014, para que las entidades supervisadas cumplan con las disposiciones establecidas en el Reglamento para la Gestión de Seguridad de la Información.

TERCERO.- Mantener la vigencia de la Carta Circular ASFI/DEP/2999/2012 de 30 de mayo de 2012 hasta el 31 de diciembre de 2014, fecha en la cual las entidades supervisadas deben dar cumplimiento a las disposiciones establecidas en el Reglamento para la Gestión de Seguridad de la Información.

Regístrese, comuníquese y cúmplase.



Lenny T. Valdivia Bautista
DIRECTORA EJECUTIVA a.i.
Autoridad de Supervisión
del Sistema Financiero



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

SECCIÓN I: DISPOSICIONES GENERALES

Artículo 1º - (Objeto) El presente Reglamento tiene por objeto establecer los requisitos mínimos que las entidades supervisadas sujetas al ámbito de aplicación, deben cumplir para la gestión de seguridad de la información, de acuerdo a su naturaleza, tamaño y complejidad de operaciones.

Artículo 2º - (Ámbito de aplicación) Están comprendidos en el ámbito de aplicación del presente Reglamento los Bancos, Bancos de Segundo Piso, Fondos Financieros Privados, Mutuales de Ahorro y Préstamo, Cooperativas de Ahorro y Crédito Abiertas, Cooperativas de Ahorro y Crédito Societarias, Instituciones Financieras de Desarrollo, Sociedades de Arrendamiento Financiero, Cámaras de Compensación, Burós de Información Crediticia, Empresas Transportadoras de Material Monetario y/o Valores, Empresas de Servicio de Pago Móvil, Empresas Remesadoras y Almacenes Generales de Depósito, que cuenten con licencia de funcionamiento emitida por la Autoridad de Supervisión del Sistema Financiero (ASFI), en adelante la entidad supervisada.

Artículo 3º - (Definiciones) Para efectos del presente Reglamento, se usarán 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 de riesgo tecnológico:** Proceso por el cual se identifican los activos de información, sus amenazas y vulnerabilidades a los 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) **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.
- 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.

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- g) **Centro de procesamiento de datos alternativo:** Lugar alternativo provisto de equipos computacionales, equipos de comunicaciones, estaciones de trabajo, enlaces de comunicaciones, fuentes de energía, 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 o 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, es permitido.
- k) **Equipo crítico:** Corresponde al 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 información:** Es el conjunto de hardware, software, redes de comunicación, multimedia y otros, así como el sitio y ambiente que los soporta, que son establecidos para el procesamiento de las aplicaciones.
- q) **Medios de acceso a la información:** Son servidores de datos y/o aplicación, 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

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

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) **Propietario de la información:** Es el responsable designado formalmente para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.
- x) **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.
- y) **Pruebas de intrusión:** Es una prueba controlada que permite 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 o bien desde Internet, Accesos Remotos o cualquier otro medio.
- z) **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.
- aa) **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.
- bb) **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 del Banco Central de Bolivia (BCB).
- cc) **Sistema de información:** Conjunto de procedimientos de recopilación, procesamiento, transmisión y difusión de información; organizados y relacionados que interactúan entre sí para lograr un objetivo.
- dd) **Sitio externo de resguardo:** Ambiente, externo al Centro de Procesamiento de Datos, de almacenamiento de todos los medios de respaldo, documentación y otros recursos de tecnología de información catalogados como críticos, necesarios para soportar los planes de continuidad y contingencias tecnológicas.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- ee) **Software:** Equipamiento o soporte lógico de un sistema de información; 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, recibir o transferir en forma electrónica, datos, información, archivos, 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 de fondos:** 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 uno o más sistemas de información. Este puede ser funcionario de la entidad supervisada (Usuario Interno del sistema de información) o cliente (Usuario Externo del sistema de información).

Artículo 4° - (Elementos de la seguridad de la información) La información que administra la entidad supervisada, debe contener un alto grado de seguridad, considerando mínimamente lo siguiente:

- a) **Autenticación:** Permite identificar al generador de la información y al usuario de la misma.
- b) **Confiability:** 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 la accesibilidad a la información en el tiempo y la forma que esta 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:** Servicio que asegura que el emisor de una información no puede rechazar su transmisión o su contenido, y/o que el receptor pueda negar su recepción o su contenido.

**SECCIÓN 2: PLANIFICACIÓN ESTRATÉGICA, ESTRUCTURA Y ORGANIZACIÓN DE LOS
RECURSOS DE TECNOLOGÍA DE LA INFORMACIÓN (TI)**

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 su naturaleza, tamaño, complejidad de sus operaciones, procesos, estructura y análisis de riesgo tecnológico realizado. Este documento debe ser aprobado por su Directorio u Órgano equivalente.

El nivel ejecutivo de la entidad supervisada que sea responsable de tecnología de la información debe efectuar un seguimiento continuo de las tendencias tecnológicas, así como a las regulaciones emitidas por ASFI que normen su funcionamiento, 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 u Órgano equivalente.

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 tecnología de la información.

El Comité 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 sistema de información de acuerdo al tema a ser tratado, cuyo funcionamiento se sujetará a su manual de organización y funciones.

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

Artículo 6° - (Comité operativo de TI) La entidad supervisada, de acuerdo a su estructura organizativa, debe conformar un Comité Operativo de Tecnología de la Información, el cual 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 esta unidad.

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

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Artículo 7º - (Responsable de la función de 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, en forma directa, su independencia funcional y operativa del área de tecnología 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 de los procedimientos establecidos.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

SECCIÓN 3: ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Artículo 1º - (Implementación del análisis de riesgo tecnológico) La entidad supervisada es responsable de efectuar el análisis de riesgo tecnológico, 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 de riesgo tecnológico efectuado debe estar contenido en un informe dirigido al Gerente General, para su posterior presentación al Directorio u Órgano equivalente.

El análisis de riesgo tecnológico, debe constituirse en un proceso continuo por lo cual debe ser revisado y actualizado permanentemente.

Artículo 2º - (Políticas de seguridad de la información) De acuerdo con su estrategia de seguridad de la información y el análisis de riesgo tecnológico efectuado, la entidad supervisada debe tener formalizadas por escrito, actualizadas e implementadas políticas que deben estar aprobadas por el Directorio u Órgano equivalente.

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 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 3º - (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 y la custodia de las licencias.

Artículo 4º - (Acuerdo de confidencialidad) Como parte de la obligación contractual, de los Directores, Consejeros de Administración y Vigilancia, Ejecutivos, demás funcionarios, consultores y el personal eventual, 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, en las que se debe incluir el mantenimiento de confidencialidad de la información a la cual tengan acceso, inclusive después de la finalización de la relación contractual.

Artículo 5º - (Inventario de activos de información) La entidad supervisada debe contar y mantener un inventario de los activos de información, y asignar responsabilidades respecto a su protección.

Artículo 6º - (Clasificación de la información) La entidad supervisada debe establecer un esquema de clasificación de la información, de acuerdo a su criticidad y sensibilidad, 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.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Artículo 7º - (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.

Estas actividades de control deben realizarse en coordinación con la instancia responsable de seguridad de la información establecida por la entidad supervisada.

Artículo 8º - (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 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 y/o 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 prestan 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 4º de la presente Sección.

Artículo 9º - (Clasificación de áreas de tecnología de la información) 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 10º - (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:

- a) Ubicación del Centro de Procesamiento de Datos al interior de la entidad supervisada.
- b) Espacio acorde y suficiente para 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.
- f) Instalación de los servidores y los equipos de comunicación de forma independiente, debidamente asegurados, según corresponda.

Artículo 11º - (Manuales de procedimientos) La entidad supervisada debe contar con manuales de procedimientos de protección física para el Centro de Procesamiento de Datos, que considere mínimamente los siguientes aspectos:

- a) Operación y mantenimiento del Centro de Procesamiento de Datos.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- 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 según las características de los equipos.
- c) Detectores de temperatura y humedad.
- d) Equipos que aseguren el suministro de energía en forma ininterrumpida y regular.
- 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 eléctrica 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 de cableado de red) El cableado utilizado para el transporte de datos de la entidad supervisada, debe cumplir con 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 así lo requiera.

Artículo 16° - (Destrucción controlada de medios de respaldo) En el marco de lo establecido en el Artículo 94° de la Ley N° 1488 de Bancos y Entidades Financieras referido a la custodia de los documentos relacionados con sus operaciones, microfilmados o registrados en medios magnéticos y electrónicos, por un periodo no menor a diez (10) años, la entidad supervisada debe establecer procedimientos para la destrucción controlada de los medios de respaldo utilizados.

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 controlada, en resguardo de los derechos de las partes en conflicto.

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, Consejeros, Ejecutivos,

Circular SB/436/03 (07/03) Inicial
SB/443/03 (08/03) Modificación 1
SB/466/04 (04/04) Modificación 2
ASFI/193/13 (09/13) Modificación 3

Libro 3°
Título VII
Capítulo II
Sección 3
Página 3/4

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

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, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual estén conscientes de las amenazas y riesgos de incidentes de seguridad de la información, y que están 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 formal disciplinario para empleados que han cometido faltas y/o violaciones a la Política de Seguridad de la Información de la entidad supervisada.

SECCIÓN 4: ADMINISTRACIÓN DEL CONTROL DE ACCESOS

Artículo 1º - (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, 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 (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 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 y responsabilidad de hardware y software.
- f) La administración de estaciones de trabajo o PC.

Artículo 2º - (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 cuentas, deben ser objeto de revisión periódica, 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; o deben ser modificados en caso de cambio.

Artículo 3º - (Administración de contraseñas de usuarios) La entidad supervisada debe definir políticas de administración de contraseñas que respondan a su análisis de riesgo tecnológico y a buenas prácticas de seguridad de la información.

Artículo 4º - (Monitoreo de actividades de los usuarios) Para el monitoreo de las actividades de los usuarios, la entidad supervisada debe establecer un procedimiento formalizado, con el fin de detectar incidentes de seguridad de la información.

Artículo 5º - (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 de riesgo tecnológico 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 1º - (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 de riesgo tecnológico efectuado.

Artículo 2º - (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 emitida según corresponda, así como en sus políticas internas.

Artículo 3º - (Requisitos de seguridad de los sistemas de información) La instancia responsable de la seguridad de la información de la entidad supervisada, debe considerar en el diseño de los sistemas de información, el establecimiento de controles de seguridad, identificados y consensuados con las áreas involucradas.

Artículo 4º - (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, migraciones de datos preexistentes, implementación y mantenimiento de los sistemas de información.

Artículo 5º - (Implementación de controles) Para el desarrollo y mantenimiento de los sistemas de información, la entidad supervisada debe considerar como mínimo, la implementación de controles según los requerimientos regulatorios y la normativa vigente establecida por ASFI.

Artículo 6º - (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 íntegra, 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 7º - (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.

RECOPIACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Artículo 8° - (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 9° - (Procedimientos de control de cambios) La entidad supervisada debe establecer procedimientos formales (documentación, especificación, prueba, control de calidad e implementación) para el control de cambios en los sistemas de información. Se debe documentar y resguardar cada versión del código fuente de los sistemas de información.

Artículo 10° - (Ambientes de desarrollo, prueba y producción) Se debe implementar controles que garanticen la separación de los ambientes de desarrollo, prueba y producción, acorde a la segregación de funciones que debe existir en cada caso.

Artículo 11° - (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 12° - (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 realice el control de calidad durante el proceso de migración. El mismo que debe estar debidamente documentado y a disposición de ASFI.

La Unidad de Auditoría Interna debe evaluar los resultados obtenidos en el proceso de migración.

Artículo 13° - (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 – Backup) La entidad supervisada debe efectuar copias de seguridad de todos los datos e información que considere necesaria 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.
- 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.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

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

Artículo 4º - (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.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

SECCIÓN 7: GESTIÓN DE SEGURIDAD EN REDES Y COMUNICACIONES

Artículo 1º - (Políticas y procedimientos) La entidad supervisada debe contar con políticas y procedimientos para la instalación y mantenimiento del hardware y su configuración base, a fin de asegurar que proporcionen la plataforma tecnológica que permita soportar las aplicaciones relacionadas con las redes y comunicaciones, y minimice 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 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 2º - (Estudio de capacidad y desempeño) La entidad supervisada debe realizar estudios periódicos de capacidad y desempeño del hardware y las líneas de comunicación que permitan determinar las necesidades de expansión de capacidades y/o actualización de equipos en forma oportuna.

Artículo 3º - (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 4º - (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 5º - (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:

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- 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 de manera regular el estado de los elementos de configuración para confirmar la integridad de la configuración de datos actual e histórica.
- c) Revisar periódicamente, la existencia de cualquier software de uso personal o no autorizado que no se encuentre incluido en los acuerdos de licenciamiento actuales.

Artículo 6° - (Documentación técnica) La documentación técnica asociada a la infraestructura de redes y telecomunicaciones debe conservarse actualizada, resguardada y contemplar como mínimo las siguientes disposiciones:

- 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 1º - (Requisitos de los sistemas de transferencia y transacción electrónica) Para habilitar un sistema de transferencia electrónica de información o transacción electrónica de fondos 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. Adicionalmente y en forma complementaria debe dar cumplimiento de los siguientes requisitos mínimos:

- a) **Seguridad del sistema:** El sistema debe proveer un perfil de seguridad que garantice que las operaciones sólo puedan ser realizadas por personas debidamente autorizadas para ello, debiendo resguardar, además, la privacidad o 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 que es recibida por el destinatario.

Los procedimientos 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 y procedimientos de seguridad de la información indicadas en el Artículo 2º 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 a los clientes, así como del nivel de robustez del sistema de autenticación 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 Sistema Web debe ser diferente al mecanismo que permita realizar transferencias de fondos en línea.

- 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 a la 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.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- 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 dicho sistema.
- d) **Certificación:** La existencia de las páginas Web utilizadas por las entidades supervisadas, debe estar avalada en cuanto a su propiedad y seguridad de la información expuesta, por una certificadora nacional o internacional. En el caso de la certificadora nacional, ésta debe estar respaldada por una certificadora internacional.
- 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. Es decir, las instalaciones y configuraciones de los equipos, sistemas y de las redes deben garantizar la continuidad de las operaciones frente a eventos fortuitos o deliberados, para lo cual debe considerar lo previsto en la Sección 10, del presente Reglamento.
- f) **Disponibilidad de la información (informes):** Los sistemas de transacción y transferencia electrónica de fondos deben generar la información necesaria para que el cliente pueda conciliar los movimientos de dinero efectuados, tanto por terminales como por usuario habilitado, incluyendo, cuando corresponda, totales de las operaciones realizadas en un determinado período.
- g) **Registro de pistas de auditoría:** Los sistemas utilizados, además de permitir el registro y seguimiento íntegro de las operaciones 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, 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 se regirá por lo establecido en el Artículo 94° de la Ley N° 1488 de Bancos y Entidades Financieras referido a la custodia de los documentos relacionados con sus operaciones, microfilmados o registrados en medios magnéticos y electrónicos, 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:
 - i. Regionalización de operaciones electrónicas nacionales e internacionales de los clientes.
 - ii. Fijar límites monetarios en transferencias y transacciones electrónicas.
- 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 entre las partes interesadas y que consideren las medidas de seguridad que se indican en el Artículo 2° de la Sección 3 del presente reglamento.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

Artículo 2º - (Contrato formal) Debe celebrarse un contrato entre la entidad supervisada y el cliente, en el cual queden claramente establecidos los derechos y responsabilidades de cada una de las partes que intervienen en este tipo de operaciones electrónicas. Este contrato debe contener de manera enunciativa y no limitativa, los siguientes puntos:

- a) El cliente, será responsable exclusivo del uso y confidencialidad de la clave de acceso, que utilizará en sus operaciones. Además se debe indicar, que la contraseña será bloqueada automáticamente después de tres intentos fallidos, así como el procedimiento para su desbloqueo debe estar claramente especificado.
- 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 transacción electrónica de fondos.
- e) Los sistemas que permitan ejecutar transacciones con fondos, además de reconocer la validez de la operación que el cliente realice, deben controlar que los importes girados no superen el saldo disponible o el límite que para el efecto haya sido fijado por éste, 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.
- f) Todas las condiciones, características y cualquier otra estipulación determinante que conlleve el uso de este servicio.

Artículo 3º - (Cifrado de mensajes y archivos) Para que una entidad supervisada, efectúe transferencias electrónicas de información y 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 formalizado por escrito, actualizado, implementado y aprobado por el Directorio u Órgano equivalente, un procedimiento para la gestión de incidentes de seguridad de la información, en concordancia con el Plan de Contingencias definido en el Artículo 1º, Sección 10 del presente Capítulo. Este procedimiento debe contar mínimamente con 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:
 - A. Pérdida de servicio, equipo o instalaciones.
 - B. Sobrecarga o mal funcionamiento del sistema.
 - C. Errores humanos.
 - D. Incumplimiento de políticas o procedimientos.
 - E. Deficiencias de controles de seguridad física.
 - F. Cambios incontrolables en el sistema.
 - G. Mal funcionamiento del software o hardware.
 - H. Violación de accesos.
 - I. Código malicioso.
 - J. Negación de servicio.
 - K. Errores resultantes de datos incompletos o no actualizados.
 - L. Violaciones en la confidencialidad e integridad de la información.
 - M. Mal uso de los sistemas de información.
 - N. Accesos no autorizados exitosos, sin perjuicios visibles a componentes tecnológicos.
 - O. Intentos recurrentes y no recurrentes de acceso no autorizado.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- 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 1º - (Plan de contingencias tecnológicas) La entidad supervisada debe tener formalizado por escrito, actualizado, implementado y aprobado por el Directorio u Órgano equivalente, un documento denominado plan de contingencias tecnológicas, que considere mínimamente:

- a) Objetivo del plan de contingencias tecnológicas.
- b) Metodología del plan de contingencias tecnológicas que incluya lo siguiente:
 - i. Análisis de riesgo tecnológico.
 - ii. Definición de eventos que afecten la operación de los sistemas de información.
 - iii. Definición de procesos críticos relacionados a los sistemas de información.
- c) Procedimientos de recuperación de operaciones críticas para cada evento identificado en el inciso b), numeral ii) del presente artículo.
- d) Descripción de responsabilidades, funciones e identificación del personal que ejecutará el plan.
- e) Medidas de prevención.
- f) Recursos mínimos asignados para la recuperación.
- g) Convenios realizados para la recuperación.
- h) Revisión anual y evaluaciones más frecuentes del plan de contingencias tecnológicas de acuerdo con el análisis 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 2º - (Plan de continuidad del negocio - BCP) La entidad supervisada debe tener formalizado por escrito, actualizado, implementado y aprobado por el Directorio u Órgano equivalente, un plan de continuidad del negocio, que incluya al menos:

- a) Inicio del proyecto.
- b) Análisis de riesgo tecnológico.
- c) Análisis de impacto al negocio (BIA: Business Impact Analysis).
- 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 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 ejecutar las pruebas necesarias hasta cumplir con el objetivo planteado.

La entidad supervisada debe documentar la realización de las pruebas y de 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.

El alcance de las pruebas de recuperación debe considerar aplicaciones individuales, escenarios de pruebas 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 alternativo) La entidad supervisada debe contar con un mecanismo alternativo de procesamiento de información que sea consistente con su naturaleza y tamaño y esté de acuerdo al análisis 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 alternativo deberá funcionar hasta que se resuelva la contingencia.

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

Artículo 1º - (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, a fin de asegurar que los servicios y contratos requeridos 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 2º - (Evaluación y selección de proveedores) Para la contratación de proveedores externos de tecnología de información, la entidad supervisada debe poseer un procedimiento documentado y formalizado para realizar la evaluación y selección de los mismos, previo a proceder con su contratación.

Artículo 3º - (Procesamiento de datos 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 las condiciones garantizan la obtención oportuna de cualquier dato o información que necesite, para fines de la entidad supervisada o para cumplir 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 tecnologías de información el cumplimiento de las políticas y procedimientos de seguridad de la información pertinentes del presente Reglamento.
- d) Es responsabilidad de la entidad supervisada asegurar las 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:
 - i. Detalle de las actividades descentralizadas.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- ii. Descripción del entorno de procesamiento.
- iii. Lista de encargados del procesamiento.
- iv. Responsables del control de procesamiento.
- v. 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 debe remitir anualmente a ASFI hasta el 31 de marzo de cada año, un informe con carácter de declaración jurada refrendado por el auditor interno, en el que se especifique que el sistema de procesamiento de datos, cumple con los criterios establecidos en el presente Reglamento.

Artículo 4° - (Contrato con proveedor de procesamiento externo) Es responsabilidad del Directorio u Órgano equivalente y el Gerente 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, para mantener políticas y procedimientos que garanticen la seguridad de la información, el secreto bancario y la confidencialidad de la información, en conformidad con la legislación boliviana, así como para prever pérdidas, atrasos 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 en 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, en base a 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) Elección del proveedor, que permita un nivel de dependencia aceptable.
- e) Disponibilidad de código fuente.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

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 la entidad supervisada, se debe 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) Para la contratación de empresas encargadas del desarrollo y mantenimiento de sistemas de información, la entidad supervisada debe considerar al menos los siguientes aspectos:

- a) Es deber del Gerente General y de los administradores responsables, asegurarse que la empresa contratada cuente con solidez financiera, organización y personal con conocimiento y experiencia en el desarrollo de sistemas y/o en servicios financieros relacionados al giro de la entidad supervisada; asimismo, asegurarse que sus sistemas de control interno y procedimientos de seguridad de la información, responden a las características del servicio que se requiere contratar.
- b) La infraestructura tecnológica, sistemas operativos y las herramientas de desarrollo, referidos a licencias de software, que se utilizarán estén debidamente licenciados por el fabricante o representante de software.
- c) Es responsable de asegurar 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) Es responsable de exigir al proveedor de tecnologías de información que cumpla con las políticas y procedimientos de seguridad de la información señalados 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 las siguientes cláusulas:

- a) Se debe aclarar a quien pertenece la propiedad intelectual en el caso de desarrollo de programas, sistemas o aplicaciones.
- b) Se debe 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) 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) Se debe 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 debe establecer multas por atrasos en la entrega. Al mismo tiempo, indemnización por daños y perjuicios en caso de fraudes o ataques informáticos.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

- f) En caso de que el proveedor sea autorizado a ingresar en forma remota a los servidores de la entidad supervisada, debe registrarse 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 a los programas fuentes.
- h) Acorde a los cambios realizados al sistema de información, la entidad supervisada debe asegurarse de que el proveedor actualice y entregue mínimamente la siguiente documentación:
 - 1) Diccionario de datos.
 - 2) Diagrama Entidad Relación (ER).
 - 3) Manual técnico.
 - 4) Manual de usuario.
 - 5) Documentación que especifique el flujo de la información entre los módulos y los sistemas.

Artículo 8º - (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 9º - (Acuerdo de nivel de servicio - SLA) La entidad supervisada de forma previa a la contratación de un proveedor externo de tecnología de información, debe establecer un 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 SLA, pueden referirse al tipo de servicio, soporte y asistencia a clientes, provisiones para seguridad y datos, garantías del sistema y tiempos de respuesta, disponibilidad del sistema, conectividad, multas por caída del sistema y/o líneas alternas para el servicio.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS

SECCIÓN 12: ROL DE LA AUDITORÍA INTERNA

Artículo Único – (Auditoría Interna) 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 del informe elaborado por 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.

RECOPILACIÓN DE NORMAS PARA BANCOS Y ENTIDADES FINANCIERAS**SECCIÓN 13: OTRAS DISPOSICIONES**

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

Artículo 2º - (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 3º - (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 podrá evaluar a la 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 4º - (Sanciones) El incumplimiento o inobservancia al presente Reglamento dará lugar a la aplicación del Artículo 99º de la Ley N° 1488 de Bancos y Entidades Financieras y a lo dispuesto por el Reglamento de Sanciones Administrativas contenido en la RNBEF a través de proceso administrativo sancionatorio establecido en la Ley de Procedimiento Administrativo N° 2341 de 23 de abril de 2002 y en el Reglamento a la Ley de Procedimiento Administrativo para el Sistema de Regulación Financiera "SIREFI" aprobado mediante Decreto Supremo N° 27175 de 15 de septiembre de 2003.

SECCIÓN 14: DISPOSICIONES TRANSITORIAS

Artículo Único – (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.