



CIRCULAR ASFI/ 596 /2019
La Paz, 20 FEB. 2019

Señores

Presente

REF: MODIFICACIONES AL REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Señores:


Para su aplicación y estricto cumplimiento, se adjunta a la presente la Resolución que aprueba y pone en vigencia las modificaciones al **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, referidas a lo siguiente:

Sección 3: Administración de la Seguridad de la Información

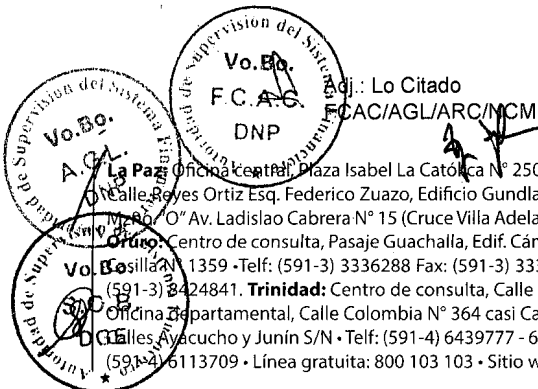
En el Artículo 17° "Custodia y conservación de datos", se precisa que las políticas y procedimientos internos de la entidad supervisada, deben prever la prohibición de destruir los documentos que respalden un proceso administrativo, judicial u otro, que se encuentre pendiente de resolución, señalándose además, que en las operaciones crediticias castigadas, se debe conservar la documentación respaldatoria, en los medios físicos y/o electrónicos que la misma determine, por el plazo mínimo de veinte (20) años computables a partir del registro contable de dicho castigo.

Las modificaciones anteriormente descritas se incorporan en el Reglamento para la Gestión de Seguridad de la Información, contenido en el Capítulo II, Título VII, Libro 3° de la Recopilación de Normas para Servicios Financieros.

Atentamente.



Lic. Vette Espinoza Vásquez
DIRECTORA GENERAL EJECUTIVA a.i.
Autoridad de Supervisión
del Sistema Financiero



Adj.: Lo Citado
F.C.A.G.
DNP



RESOLUCIÓN ASFI/ 135 /2019
La Paz, 20 FEB. 2019

VISTOS:

La Constitución Política del Estado, la Ley N° 393 de Servicios Financieros, las Resoluciones SB N° 066/2003 y ASFI/807/2018 de 4 de julio de 2003 y 28 de mayo de 2018, respectivamente, el Informe ASFI/DNP/R-26305/2019 de 6 de febrero de 2019, referido a la modificación al **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, contenido en la Recopilación de Normas para Servicios Financieros y demás documentación que ver convino y se tuvo presente.

CONSIDERANDO:

Que, el Artículo 331 de la Constitución Política del Estado, 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 con la Ley”.*

Que, el Parágrafo I del Artículo 332 de la Constitución Política del Estado 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 (ASFI).

Que, el Parágrafo I del Artículo 6 de la Ley N° 393 de Servicios Financieros, dispone que las actividades de intermediación financiera y la prestación de servicios financieros, son de interés público y sólo pueden ser ejercidas por entidades financieras autorizadas conforme a Ley.

Que, el Parágrafo I del Artículo 8 de la Ley N° 393 de Servicios Financieros, determina que: *“Es competencia privativa indelegable de la Autoridad de Supervisión del Sistema Financiero - ASFI ejecutar la regulación y supervisión financiera, con la finalidad de velar por el sano funcionamiento y desarrollo de las entidades financieras y preservar la estabilidad del sistema financiero, bajo los postulados de la política financiera, establecidos en la Constitución Política del Estado”.*

FCAC/AGL/MMV

Pág. 1 de 4



Que, el Artículo 16 de la Ley N° 393 de Servicios Financieros, señala que: *“La Autoridad de Supervisión del Sistema Financiero - ASFI, tiene por objeto regular, controlar y supervisar los servicios financieros en el marco de la Constitución Política del Estado, la presente Ley y los Decretos Supremos reglamentarios, así como la actividad del mercado de valores, los intermediarios y entidades auxiliares del mismo”.*

Que, mediante Resolución Suprema N° 24438 de 19 de octubre de 2018, el señor Presidente Constitucional del Estado Plurinacional de Bolivia designó a la Lic. Ivette Espinoza Vásquez como Directora General Ejecutiva a.i. de la Autoridad de Supervisión del Sistema Financiero.

CONSIDERANDO:

Que, el inciso t), Parágrafo I del Artículo 23 de la Ley N° 393 de Servicios Financieros, dispone entre las atribuciones de la Autoridad de Supervisión del Sistema Financiero, el emitir normativa prudencial de carácter general, extendiéndose a la regulación de normativa contable para aplicación de las entidades financieras.

Que, el Parágrafo III del Artículo 34 de la Ley N° 393 de Servicios Financieros, prevé que: *“Las entidades financieras conservarán, debidamente, los libros y documentos referentes a sus operaciones, microfilmados o registrados en medios magnéticos y electrónicos, por un periodo no menor a diez (10) años, desde la fecha del último asiento contable, sujeto a reglamentación de la Autoridad de Supervisión del Sistema Financiero – ASFI”.*

Que, el Parágrafo I del Artículo 449 de la citada Ley, determina que: *“Las entidades financieras deberán implementar sistemas, metodologías y herramientas de gestión integral de riesgos, que contemplen objetivos, estrategias, estructura organizacional, políticas y procedimientos para la prudente administración de todos los riesgos inherentes a sus actividades y operaciones; en base a la normativa que emita para el efecto la Autoridad de Supervisión del Sistema Financiero - ASFI”.*

Que, el Artículo 484 de la Ley N° 393 de Servicios Financieros, estipula que en el marco de preservar un sistema financiero sano y eficiente, ASFI conformará registros de información, detallando entre estos:

“e) Relación de deudores con créditos castigados por las entidades de intermediación financiera autorizadas, por veinte años, computables a partir del registro contable de dicho castigo; vencido este plazo opera el derecho al olvido para el prestatario, no pudiendo ser reportado con la deuda castigada. La normativa emitida por la Autoridad de Supervisión del Sistema Financiero – ASFI establecerá los requisitos y condiciones para la aplicación de este derecho”.

ACACI/AGL/MMIV

Pág. 2 de 4



Que, a través de Resolución SB N° 066/2003 de 4 de julio de 2003, la Superintendencia de Bancos y Entidades Financieras, actual Autoridad de Supervisión del Sistema Financiero, aprobó y puso en vigencia la normativa referida a los *"Requisitos Mínimos de Seguridad Informática para la Administración de Sistema de Información y Tecnologías Relacionadas en Entidades Financieras"*, al presente denominado **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, contenido en el Capítulo II, Título VII, Libro 3° de la Recopilación de Normas para Servicios Financieros (RNSF).

Que, con Resolución ASFI/807/2018 de 28 de mayo de 2018, la Autoridad de Supervisión del Sistema Financiero, aprobó y puso en vigencia las últimas modificaciones al Reglamento citado en el párrafo que antecede.

CONSIDERANDO:

Que, en virtud a lo estipulado en el Parágrafo I del Artículo 449 de la Ley N° 393 de Servicios Financieros, que señala la obligación de las entidades financieras de implementar sistemas, metodologías y herramientas de gestión integral de riesgos, que contemplen objetivos, estrategias, estructura organizacional, políticas y procedimientos para la prudente administración de todos los riesgos inherentes a sus actividades y operaciones, conforme la normativa que para el efecto emita la Autoridad de Supervisión del Sistema Financiero y con el propósito de que las entidades financieras aseguren y formalicen el deber de resguardar aquellos documentos que respalden un proceso administrativo, judicial u otro que se encuentre pendiente de resolución, es pertinente establecer en el **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, la directriz que las políticas y procedimientos internos de las entidades supervisadas precisen la prohibición de destruir este tipo de documentación.

Que, con base en lo previsto en el Parágrafo III del Artículo 34 de la Ley N° 393 de Servicios Financieros, que estipula que las entidades financieras conservarán, debidamente, los libros y documentos referentes a sus operaciones, microfilmados o registrados en medios magnéticos y electrónicos, por un periodo no menor a diez años, desde la fecha del último asiento contable, sujeto a reglamentación de la Autoridad de Supervisión del Sistema Financiero (ASFI), tomando en cuenta además, que el inciso e) del Artículo 484 de la citada Ley, señala el registro de información conformado por ASFI, referido a la relación de deudores con créditos castigados, por veinte años a partir de la fecha del registro contable del castigo y que una vez vencido dicho plazo, es aplicable el derecho al olvido para el prestatario; con el propósito de que las entidades supervisadas sustenten el registro de las operaciones que mantienen castigadas y a su vez se puedan evidenciar los respaldos de estos registros, corresponde incorporar en el **REGLAMENTO PARA LA GESTIÓN DE**

FCAC/AGL/MMV

Pág. 3 de 4



SEGURIDAD DE LA INFORMACIÓN, lineamientos para la custodia y conservación de la documentación que respalda el registro de créditos castigados, en función del plazo dispuesto en el inciso e) del Artículo 484 de la Ley N° 393 de Servicios Financieros.

Que, debido a que con la citada modificación, las entidades supervisadas requerirán ajustes en sus políticas y procedimientos, para la custodia y conservación de los documentos que respalden las operaciones castigadas, corresponde definir un plazo de transitoriedad, para la aplicación de la modificación, disponiendo su vigencia a partir del 1 de abril de 2019.

CONSIDERANDO:

Que, mediante Informe ASFI/DNP/R-26305/2019 de 6 de febrero de 2019, se determinó la pertinencia de aprobar la modificación al **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, contenido en el Capítulo II, Título VII, Libro 3° de la Recopilación de Normas para Servicios Financieros.

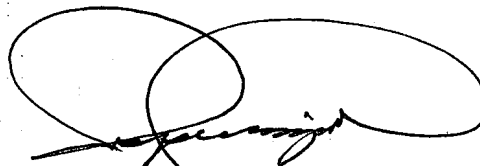
POR TANTO:

La Directora General Ejecutiva a.i. de la Autoridad de Supervisión del Sistema Financiero, en virtud de las facultades que le confiere la Constitución Política del Estado y demás normativa conexas y relacionadas.

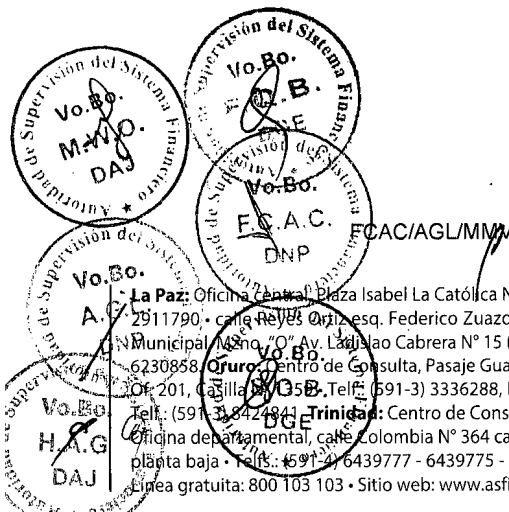
RESUELVE:

ÚNICO. - Aprobar la modificación al **REGLAMENTO PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**, contenido en el Capítulo II, Título VII, Libro 3° de la Recopilación de Normas para Servicios Financieros, de acuerdo al texto que en Anexo forma parte de la presente Resolución, disponiendo su vigencia a partir de 1 de abril de 2019.

Regístrese, comuníquese y cúmplase.



Lic. Ivette Espinoza Vásquez
DIRECTORA GENERAL EJECUTIVA a.i.
Autoridad de Supervisión
del Sistema Financiero



RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

SECCIÓN 3: ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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

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

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

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

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

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

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

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

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

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

RECOPIACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

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

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

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

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

- a. La evaluación de vulnerabilidades técnicas debe efectuarse por lo menos una (1) vez por año y ante un cambio en la infraestructura tecnológica. La ejecución de pruebas de seguridad debe considerar la realización de pruebas de intrusión controladas internas, externas, o ambas de acuerdo con los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuado por la Entidad Supervisada;
- b. El conjunto de políticas y procedimientos referido a la gestión de vulnerabilidades técnicas debe ser revisado y actualizado (si corresponde), por lo menos una (1) vez al año;
- c. La Entidad Supervisada debe exigir a la(s) empresa(s) y/o persona(s) que le preste(n) servicios de evaluación de seguridad de la información, la respectiva documentación que acredite la experiencia necesaria para realizar este tipo de trabajos; adicionalmente debe(n) garantizar que el personal que realice las pruebas de intrusión controladas sea certificado y firme un acuerdo de confidencialidad conforme se establece en el Artículo 4° de la presente Sección;
- d. El análisis de vulnerabilidades técnicas puede ser realizado por personal externo, interno o ambos, conforme con los resultados del análisis y evaluación de riesgos en seguridad de la información, efectuado por la Entidad Supervisada. Al efecto, el personal interno asignado para esta tarea debe ser ajeno al (las) área(s) de tecnologías y sistemas de información.

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

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

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

RECOPILACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

- b. Espacio acorde y suficiente para la cantidad de equipos instalados;
- c. Energía regulada de acuerdo con los requerimientos de los equipos;
- d. Cableado para el uso de los equipos de cómputo por medio de sistemas de ductos a través de piso o techo falso, de acuerdo con la necesidad de la Entidad Supervisada;
- e. No almacenar papel u otros suministros inflamables y/o equipos en desuso dentro del CPD;
- f. Instalación de los servidores y equipos de comunicación de forma independiente, debidamente asegurados, según corresponda.

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

- a. Operación y mantenimiento;
- b. Administración de accesos;
- c. Pruebas a dispositivos de seguridad para garantizar su correcto funcionamiento.

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

- a. Sistema de ventilación que mínimamente mantenga la temperatura y humedad en los niveles recomendados por los fabricantes de los equipos;
- b. Extintores de incendios (manuales y/o automáticos) u otros dispositivos según las características de los equipos;
- c. Detectores de temperatura y humedad;
- d. Equipos que aseguren el suministro de energía regulada en forma ininterrumpida;
- e. Mecanismos para el control de ingreso y salida del Centro de Procesamiento de Datos;
- f. Vigilancia a través de cámaras de CCTV (Circuito Cerrado de TV).

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

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

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

Artículo 15° - (Pruebas a dispositivos de seguridad) Los dispositivos de seguridad física detallados en el Artículo 12° de la presente Sección, deben ser probados al menos dos (2) veces por

RECOPIACIÓN DE NORMAS PARA SERVICIOS FINANCIEROS

año, de tal forma que se garantice su correcto funcionamiento. La documentación que respalde la realización de estas pruebas debe estar disponible cuando ASFI la requiera.

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

- a. Las funciones y responsabilidades de los Directivos, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual deben ser definidas y documentadas en concordancia con la PSI y con la normativa que se desprende de la misma;
- b. Asegurar que los Directivos, Consejeros, Ejecutivos, funcionarios, consultores y personal eventual estén conscientes de las amenazas y riesgos de incidentes de seguridad de la información, así como que estén capacitados para aceptar y cumplir con la PSI y con la normativa que se desprende de la misma, en el desarrollo normal de su trabajo;
- c. El establecimiento de un proceso disciplinario formal para Directivos, Consejeros, Ejecutivos y funcionarios que hubieran cometido faltas y/o violaciones a la PSI y/o a la normativa que se desprende de la misma, de la Entidad Supervisada;
- d. La determinación en el contrato, de las sanciones para consultores y personal eventual que hubieran cometido faltas y/o violaciones a la PSI y/o a la normativa que se desprende de la misma, de la Entidad Supervisada.

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

La documentación que se constituya en instrumento probatorio en un proceso administrativo, judicial u otro, que se encuentre pendiente de resolución, no debe ser objeto de destrucción, en resguardo de los derechos de las partes en conflicto, aspecto que debe ser previsto en las políticas y procedimientos internos de la Entidad Supervisada.

En las operaciones crediticias castigadas, la Entidad Supervisada debe conservar la documentación respaldatoria en los medios físicos y/o electrónicos que la misma determine, por el plazo mínimo de veinte (20) años computables a partir del registro contable de dicho castigo.

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