NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO PARA INSTITUCIONES DE MICROFINANZAS

RESOLUCIÓN No. CD-CONAMI-017-01AGO21-2014, Aprobado el 21 de Agosto del 2014

Publicado en La Gaceta No. 177 del 19 de Septiembre del 2014

El Consejo Directivo de la Comisión Nacional de Microfinanzas,

CONSIDERANDO:

I

Que el artículo 47, numeral 4), de la Ley No. 769, Ley de Fomento y Regulación de las Microfinanzas, publicada en La Gaceta, Diario Oficial No. 128, del 11 de julio de 2011, referente a las obligaciones de la junta directiva, señala que, dicho órgano de administración, tiene entre sus responsabilidades velar porque se implementen e instruir para que se mantengan en adecuados funcionamiento y ejecución, las políticas, sistemas y procesos que sean necesarios para una correcta administración, evaluación y control de los riesgos inherentes al negocio; estableciendo dicho artículo la facultad del Consejo Directivo de dictar normas de aplicación general en las que se establezca la forma en que se implementarán las responsabilidades antes enunciadas.

II

Que el artículo 51, numeral 6) de la precitada Ley No. 769, establece, en sus partes conducentes, que las estrategias, políticas y directrices escritas que regulan el gobierno corporativo de las Instituciones de Microfinanzas (IMF) deben incluir, al menos, políticas sobre procesos integrales que incluyan la administración de los diversos riesgos a que pueda estar expuesta la institución, así como, sistemas de información adecuados y un comité para la gestión de dichos riesgos.

III

Que entre los riesgos a los que pueden estar expuestas las IMF en sus operaciones, se encuentra el riesgo operacional, entendido como el riesgo de pérdidas generadas por deficiencias o fallas en los procesos internos, en la Tecnología de la Información (TI), en las personas o por ocurrencia de eventos externos.

IV

Que es necesario establecer lineamientos mínimos a seguir por parte de las IMF para la identificación, mediación, monitoreo y control de los riesgos asociados a la Tecnología de Información (TI), en aras de contribuir a la estabilidad del sistema microfinanciero.

V

Que de acuerdo a las consideraciones antes expuestas y con base a las facultades establecidas en el artículo 6, numeral 5) y 17), artículo 12 numeral 4) y artículo 23, de la Ley 769, Ley de Fomento y Regulación de las Microfinanzas, y sus reformas.

En uso de sus facultades,

RESUELVE

Fuente: http://www.leybook.com/doc/16935

Dictar la siguiente:

NORMA SOBRE GESTIÓN DE RIESGO TECNOLÓGICO PARA INSTITUCIONES DE MICROFINANZAS

RESOLUCIÓN N°CD-CONAMI-017-01AGO21-2014

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Objeto.- La presente norma tiene por objeto establecer los requisitos mínimos que deben cumplir las Instituciones de Microfinanzas para la gestión de los riesgos asociados a la Tecnológico de Información, de acuerdo a la naturaleza, complejidad, volumen y perfil de riesgo de sus operaciones, con el fin de controlar o mitigar el posible impacto negativo de dichos riesgos.

Artículo 2. Alcance.- Las disposiciones de la presente norma son aplicables, sin excepciones, a las Instituciones de Microfinanzas (IMF) sujetas al registro, regulación, supervisión, vigilancia y fiscalización de la Comisión Nacional de Microfinanzas (CONAMI).

Artículo 3. Definiciones.- Los términos utilizados en la presente norma, deben ser interpretados de acuerdo con las siguientes definiciones:

1. Activo de la información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

2. Administración Integral de riesgos: Consiste en detectar oportunamente los riesgos que pueden afectar a la empresa, para generar estrategias que se anticipen a ellos y los conviertan en oportunidades de rentabilidad para la empresa.

3. Alta Gerencia: La persona que en las instituciones ocupe el cargo de ejecución principal (Presidente Ejecutivo, Director General, Director Ejecutivo, Gerente General) o sus equivalentes.

4. Base de Datos: Serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de la institución.

5. Bitácora: Registro manual o electrónico que provee información necesaria para identificar e investigar alguna actividad, problema o incidente.

6. Cableado estructurado: Es el conjunto de elementos pasivos, flexible, genérico e independiente, que sirve para interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes sistemas de control, comunicación y manejo de la información, sean estos de voz, datos, videos, así como equipos de conmutación y otros sistemas de administración.

7. CONAMI: Comisión Nacional de Microfinanzas, constituida por la Ley como órgano regulador y supervisor de las Instituciones de Microfinanzas.

8. Continuidad del negocio: Estado continuo e ininterrumpido de operación de un negocio.

Fuente: http://www.leybook.com/doc/16935

9. Días: Días calendarios, salvo que expresamente se establezca que se refiere a días hábiles.

10. Ejecutivo Principal: Funcionario de la IMF que tiene a su cargo la dirección diaria de las operaciones de la institución.

11. Evento: Suceso o serie de sucesos, internos o externos a la institución, originados por la misma causa, que ocurren durante un mismo período de tiempo.

12. Gobierno de TI: Estructura de relaciones y procesos para dirigir y controlar la institución con el objetivo de lograr sus metas, agregando valor mientras exista un balance entre los riesgos y beneficios de TI y sus procesos.

13. IFIM: Instituciones Financieras Intermediaria de Microfinanzas. Entendiéndose como tal, a toda persona jurídica de carácter mercantil o sin fines de lucro, que se dedicare de alguna manera a la intermediación de recursos para el microcrédito y a la prestación de servicios financieros y/o auxiliares, tales como bancos, sociedades financieras, cooperativas de ahorro y crédito, asociaciones, fundaciones y otras sociedades mercantiles.

14. IMF o Institución: Institución de Microfinanzas. Se considerará como IMF a las IFIM constituidas como persona jurídica sin fines de lucro o como sociedades mercantiles, distintas de los bancos y sociedades financieras, cuyo objeto fundamental sea brindar servicios de microfinanzas y posean un Patrimonio o Capital Social Mínimo, igual o superior a Cuatro Millones Quinientos mil Córdobas (C$4 5000,000.00), o en su equivalente en moneda dólar de los Estados Unidos de América según tipo de cambio oficial, y que el valor bruto de su cartera de microcréditos represente al menos el cincuenta por ciento de su activo total.

15. Incidente: Circunstancia o suceso que ocurre de manera inesperada y que puede afectar al desarrollo de un asunto o negocio, aunque no forme parte de él.

16. Información: Cualquier forma de registro electrónico, óptico, magnético o en otros medios, susceptible de ser procesada, distribuida y almacenada.

17. Hardware: Conjunto de todos los componentes físicos y tangibles de un computador o equipo eléctrico.

18. Junta Directiva: Principal órgano de administración de la IMF.

19. Ley: Ley No. 769, Ley de Fomento y Regulación de las Microfinanzas, y sus reformas, publicadas en La Gaceta, Diario Oficial No. 128, del 11 de julio de 2011.

20. Mejores Prácticas Aplicables: Se refiere a los marcos de referencia de control, estándares internacionales, u otros estudios que ayuden a monitorear y mejorar las actividades críticas de la tecnología de información, aumentar el valor de negocio, y reducir riesgos, tales como; COSO, COBIT, ITIL, ISO 17799, ISO 9001, CMM, entre otros.

21. Plan de Contingencia de TI: Documento aprobado por la junta directiva de la institución, en el que se detalla la estrategia de recuperación del procesamiento de los sistemas de información, con el fin de no afectar el funcionamiento normal de la institución. Tiene como objetivo asegurar un nivel aceptable de operatividad de los procesos críticos, ante fallas mayores internas o externas.

22. Políticas: Conjunto de prácticas establecidas por la junta directiva de la institución, por medio de las

cuales se definen los cursos de acción a seguir por la administración.

23. Presidente Ejecutivo. Presidente Ejecutivo de CONAMI.

24. Proceso crítico: Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de la IMF.

25. Procedimiento: Método o sistema estructurado para ejecutar instrucciones. Lista detallada de la secuencia lógica y consistente de actividades y cursos de acción, por medio de las cuales se asegura el cumplimiento de una función operativa.

26. Rack: Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones.

27. Recuperación: La restauración de operaciones específicas del negocio a un nivel suficiente para cumplir con las obligaciones de la institución, después de ocurrida una interrupción.

28. Riesgo: La probabilidad que se produzca un hecho generador de pérdidas que afecten el valor económico de la institución.

29. Riesgo Tecnológico: Pérdida potencial ocasionada por interrupción, falla o daño que se derivan del uso o dependencia en el hardware, software, sistema, aplicaciones, redes y cualquier otro canal de distribución de Información que una organización dispone para prestar sus servicios.

30. Tecnología de Información (TI): Hardware, Software, Sistemas de Información, Investigacion Tecnológica, Redes Locales, Bases de Datos, Ingeniería de Software, Telecomunicaciones, Servicios y Organización de Informática.

31. Sistemas de Información: Se refiere a cualquier sistema computacional que se utilice para obtener, almacenar, manipular, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información.

32. Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

CAPÍTULO II

CRITERIOS DE INFORMACIÓN

Artículo 4. Criterios.- Para efectos de la presente norma se deben tomar en consideración los siguientes criterios de información para el control y gestión de las tecnologías de información y sus riesgos asociados:

1. Confiablidad: Los sistemas deben brindar información correcta, completa, oportuna y exacta, que será utilizada en la operación de la institución y en la toma de decisiones, la preparación de estados financieros e información gerencial y su remisión a terceros.

2. Confidencialidad: Se debe brindar protección a la información sensible contra divulgación no autorizada.

3. Cumplimiento: Se tienen que cumplir aquellas leyes, reglamentos y acuerdos contractuales a los

Fuente: http://www.leybook.com/doc/16935

cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

4. Disponibilidad: Los recursos y la información deben estar disponibles en tiempo y forma, cada vez que sean requeridos por los usuarios.

5. Efectividad: La información y los procesos deben ser relevante y pertinentes para el proceso del negocio, además de presentarse en forma correcta, coherente, completa y que pueda utilizarse oportunamente.

6. Eficiencia: El proceso de la información debe realizarse mediante una óptima (más productiva y económica) utilización de los recursos.

7. Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

8. No repudio: Servicio que asegura que el emisor de una información, así no puede rechazar su transmisión o su contenido, y/o que el receptor pueda negar su recepción o su contenido.

CAPÍTULO III

RESPONSABILIDAD DE LA JUNTA DIRECTIVA Y DE LA ALTA GERENCIA, ESTRUCTURA ORGANIZACIONAL Y PLANEACIÓN DE TI

Artículo Responsabilidades de la Junta Directiva.- La Junta Directiva de la IMF será responsable de velar porque se implemente e instruir para que se mantenga un adecuado funcionamiento y ejecución de las políticas, sistemas y procesos que sean necesarios para una correcta administración, evaluación y control de los riesgos de TI inherentes al negocio. A tal efecto, la Junta Directiva deberá, como mínimo;

1. Aprobar los objetivos, lineamientos y políticas generales de seguridad de la información y de gestión de los riesgos de TI, las cuales deberán ser consistentes con el tamaño y naturaleza de la institución, y con la complejidad y volumen de sus operaciones y servicios.

2. Aprobar un manual para la gestión de los riesgos de TI, y sus correspondientes modificaciones.

3. Aprobar los planes estratégicos de TI.

4. Aprobar los planes de contingencia de TI.

5. Aprobar la incursión de la institución en nuevos proyectos de TI.

6. Proveer los recursos necesarios para la implementación de las políticas de gestión de riesgos de TI, y el cumplimiento de las disposiciones requeridas en la presente norma.

7. Administrar adecuadamente los riesgos de TI

8. Garantizar que la auditoría interna verifique la existencia y cumplimiento de los requerimientos establecidos en la presente norma para una adecuada gestión de los riesgos de TI.

Estas responsabilidades podrán delegadas en un Comité de Riesgos de TI o en el Comité de Riesgos de

Fuente: http://www.leybook.com/doc/16935

la IMF al que debe integrar al responsable de TI. Este comité debe estar integrado, al menos, por un miembro de la Junta Directiva que no sea el ejecutivo principal, el responsable de TI y el jefe de Riesgos de la institución. El comité deberá informar, al menos trimestralmente a la Junta Directiva, acerca de la gestión de riesgos de TI delegada al mismo.

Los asuntos tratados y acuerdos que se tomen en las sesiones del comité, deberán constar en un Libro de Actas, el cual debe estar a disposición de los Entes Fiscalizadores tanto internos como externos.

Artículo 6. Responsabilidades del Ejecutivo Principal.- El Ejecutivo Principal de la IMF tendrá las siguientes responsabilidades mínimas en cuanto a la gestión de los riesgos de TI:

1. Velar por la implementación de los objetivos, lineamientos y políticas aprobadas por la Junta Directiva para la gestión de los riesgos de TI;

2. Velar por el cumplimiento de los objetivos, lineamientos y políticas antes referidas;

3. Informar a la Junta Directiva, al menos trimestralmente, acerca de los resultados de la implementación y ejecución del proceso de gestión de los riesgos de TI.

4. Tomar acción inmediata y adoptar las medidas correctivas necesarias en caso de que las políticas de gestión de los riesgos de TI no se cumplan, o se cumplan parcialmente o en forma incorrecta;

5. Asegurar la disponibilidad, capacidad y desempeño de los sistemas de información requeridos para la continuidad de procesos críticos del negocio;

6. Analizar y evaluar las propuestas de incursión de la institución en nuevos proyectos de TI, e informar a la Junta Directiva los resultados de su análisis sobre dichas propuestas

7. Presentar a la Junta Directiva propuestas de actualización de las políticas y manuales de gestión de los riesgos de TI, al menos, una vez al año;

8. Proponer a la Junta Directiva y velar por que la institución cuente con la adecuada estructura organizacional para la gestión de los riesgos de TI, y la estrategia de asignación de recursos para su implantación; y

9. Asegurar que se implementen las recomendaciones derivadas de los informes de auditoría e inspecciones de la CONAMI para una adecuada gestión de los riesgos de TI.

10. Otras que le asigne la Junta Directiva.

Artículo 7. Estructura organizacional y procedimientos.- Las IMF deben contar con una estructura organizacional adecuada al tamaño, volumen y complejidad de sus operaciones, que delimite las funciones y responsabilidades relativas a la gestión de los riesgos de TI y seguridad de la información, aspectos que deben estar contenidos en el manual de organización y funciones de la institución, aprobado por su Junta Directiva.

Dicha estructura debe contar con independencia, autoridad y adecuada segregación de funciones ante las áreas a las que brinda servicios, excluyendo la posibilidad de que una sola persona controle procesos u Operaciones críticos relacionados a TI.

La IMF deberá definir procedimientos formales para la contratación de nuevo personal de tecnología de

Fuente: http://www.leybook.com/doc/16935

la información e implementar los controles necesarios para garantizar que el personal de TI lleve a cabo únicamente las funciones correspondientes a sus respectivos puestos.

La institución que por su tamaño o naturaleza de negocio no pueda contar con esta estructura organizacional, podrá solicitar al Presidente Ejecutivo ser exonerada total o parcialmente del cumplimiento de las disposiciones establecidas en el presente artículo. En este caso, mientras la institución se encuentre exonerada y no cuente con un responsable de TI, las responsabilidades correspondientes a este rol recaerán en el ejecutivo principal.

Artículo 8. Planeación de TI.- Las IMF deberán contar con un Plan Estratégico de TI que esté documentado, aprobado por la Junta Directiva, alineado con la estrategia institucional, y que considere su naturaleza, tamaño, complejidad de las operaciones, procesos, estructura y análisis de riesgo tecnológico realizado. Dicho plan deberá considerar, al menos, los siguientes aspectos:

1. El apoyo de TI a las áreas usuarias relevantes.

2. La definición de cómo la TI dará soporte a los programas de inversión de la institución;

3. La definición de un plan de infraestructura tecnológica.

4. El cumplimiento de una política preestablecida de adquisición y mantenimiento de la infraestructura tecnológica.

5. El presupuesto de la inversión de TI.

6. La definición de cómo se cumplirán y medirán los objetivos planteados

7. Los requerimientos legales y regulatorios.

El coordinador o responsable de la estructura organizacional a la que se refiere el artículo 7 precedente, deberá presentar al Ejecutivo Principal, informes trimestrales de avance en la ejecución de su plan estratégico y presupuesto de TI.

Artículo 9. Actualización de planes.- Los planes estratégicos de TI deberán ser evaluados y actualizados, a] menos, anualmente, en términos de su contribución a los objetivos de la institución, su funcionalidad, estabilidad, complejidad, costos, fortalezas y debilidades.

CAPÍTULO IV
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Articulo 10. Requerimientos para la adquisición, desarrollo y mantenimiento de sistemas de información.- Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las IMF deberán contar, al menos, con lo siguiente:

1. Procedimiento formalizado para la aprobación de nuevos sistemas de información, donde se definan las instancias y niveles de aprobación de los mismos de acuerdo a la naturaleza y alcance de] proyecto.

2. Procedimiento formalizado para la administración del ciclo de vida del desarrollo de los sistemas de información, lo cual aplica para toda IMF cuyo desarrollo de sistemas se efectúe internamente. Los mismos deben contar con aspectos tales como: requerimientos del usuario, requerimientos de hardware y

Fuente: http://www.leybook.com/doc/16935

software, definición e implementación de pistas de auditorías, plan de pruebas y capacitación a usuarios, existencia de ambientes separados de desarrollo y producción, criterios finales de aceptación y actualización oportuna de información técnica y de usuarios.

3. Procedimiento formalizado de control de cambios a producción para proteger los programas de aplicación de cambios no autorizados. En situaciones donde se requiera llevar a cabo cambios de emergencia para resolver problemas del sistema y para posibilitar la continuidad de un procesamiento critico, deben existir procedimientos para asegurar que se puedan realizar los arreglos de emergencia sin comprometer la integridad del sistema.

4. En caso de adquisición de sistemas de información, la IMF deberá realizar un análisis previo a la adquisición que contemple, como mínimo, lo siguiente:

4.1 Fuentes alternativas para la compra;
4.2 Análisis costo-beneficio;
4.3 Revisión de la factibilidad tecnológica;
4.4 Elección del proveedor que permita un nivel de dependencia aceptable; y
4.5 Disponibilidad del código fuente.

Asimismo, los contratos con el proveedor deberán indicar los requisitos de seguridad establecidos por la IMF.

5. En caso de desarrollo y mantenimiento de sistemas de información a través de proveedores externos, la IMF deberá asegurarse, en caso de obtener el código fuente, que el proveedor actualice y entregue, como mínimo, la siguiente documentación:

5.1 Diccionario de datos.
5.2 Diagrama Entidad – Relación (ER).
5.3 Manual técnico y de usuario.
5.4 Documentación que especifique el flujo de la información entre los módulos y sistemas.

En caso que la IMF no obtenga el código fuente, ésta deberá asegurarse que el proveedor entregue, al menos, el manual técnico y de usuario.

Asimismo, el contrato que la IMF suscriba con el proveedor deberá considerar, como mínimo, los siguientes aspectos:

• Aclarar a quien pertenece la propiedad intelectual.

• Indicar la plataforma de desarrollo, especificaciones de servidores, sistemas operativos, herramientas de desarrollo y base de datos.

• Incluir cláusulas de confidencialidad para el personal que participa en el proyecto.

• Indicar los tiempos de desarrollo por cada etapa en un cronograma y plan de trabajo incluyendo las fases de prueba.

• Junto a las condiciones normales de pago, se deben establecer multas por atrasos en la entrega.

6. Procedimientos de migración de sistemas de información, el cual debe estar basado en un plan de acción y procedimientos específicos que garanticen la disponibilidad, integridad y confidencialidad de la

información conforme los criterios establecidos en el artículo 4 de la presente norma. Es responsabilidad del Ejecutivo Principal, designar a la instancia que realice el control de calidad durante el proceso de migración, mismo que debe estar debidamente documentado. La Unidad de Auditoría interna debe evaluar los resultados obtenidos en el proceso de migración.

CAPÍTULO V
GESTIÓN DE OPERACIONES DE TI

Articulo 11. Requerimientos para la gestión de operaciones de TI.- Con el objeto de garantizar que la infraestructura de Ti que soporta las operaciones sea administrada, monitoreada y documentada de forma adecuada, las IMF deberán contar, al menos, con lo siguiente:

1. Procedimientos formalizados para la administración de procesos críticos relacionados con la gestión de operaciones de Ti, igualmente para el manejo de incidentes de seguridad.

2. Documentación de los procesos de administración de las bases de datos que contemple, como mínimo, lo siguiente:

2.1 instalación, administración, migración y mantenimiento.
2.2 Mecanismos de control de acceso
2.3 Revisión periódica de capacidad y desempeño de las bases de datos.
3. Controles documentados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia.

4. Inventarios actualizados de hardware, licencias de software, diagramas de red y comunicaciones

5. Controles para la detección y desinfección de virus informáticos, software malicioso y actualización de parches de seguridad

6. Controles para el acceso y restricción de la navegación a Internet conforme a los perfiles de usuarios.

7. Copias de seguridad de todos los datos e información que considere necesaria para el continuo funcionamiento de la institución, cumpliendo, al menos, con los siguientes aspectos:

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

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

7.3 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.

7.4 Contar con copias de respaldo y procedimientos de restauración resguardados físicamente en otra ubicación distinta del CPD.

7.5 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.

7.6 Los respaldos y medios de almacenamiento que contengan material sensitivo, que estén dañados, deben ser físicamente destruidos o sobrescritos en forma segura en vez de utilizar las funciones de borrado estándar.

Fuente: http://www.leybook.com/doc/16935

CAPÍTULO VI
ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN

Artículo 12. Requerimientos para la administración de la seguridad de la información.- Con el objeto de garantizar que el sistema de administración de la seguridad de la información satisfaga las necesidades de la IMF para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones deben cumplir, al menos, con lo siguiente:

1. Políticas y procedimientos de seguridad de la información: En dichas políticas deberán estar claramente definidos los objetivos, ámbito y responsabilidades. Las políticas mínimas de seguridad deben ser:

1.1 Políticas sobre la seguridad del acceso a los sistemas de información: que defina cómo serán identificados y autenticados todos los usuarios, los requerimientos estándares de control de acceso, y los eventos a auditarse en los sistemas.

1.2 Políticas sobre el uso adecuado de los equipos de cómputo: que defina quien puede hacer uso de los mismos y cómo pueden ser utilizados.

1.3 Políticas sobre el uso de Internet: que defina quienes pueden tener acceso y cómo debe ser el uso apropiado a este recurso.

1.4 Políticas sobre el uso de correo electrónico y correo gratuito: que defina quienes pueden tener acceso y cómo debe ser el uso apropiado a este recurso.

2. Acuerdos de confidencialidad: Como parte de sus obligaciones contractuales con la IMF, los Directores, altos ejecutivos, demás funcionarios, empleados y consultores eventuales, deberán suscribir acuerdos de confidencialidad respecto a la información de la institución a la cual tengan acceso, inclusive después de la finalización de la relación contractual.
3. Inventario de activos de información: La IMF deberá contar con un inventario periódico de activos físicos y activos de información. Dicha información deberá ser clasificada de acuerdo a su criticidad y sensibilidad, estableciéndose 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 por Junta Directiva y comunicada a todas las áreas involucradas.

4. Centro de procesamiento de datos (CPD): La IMF debe contar con un CPD que reúna, al menos, las siguientes características:

4.1 Zona de acceso restringida, al cual solo debe tener acceso el personal informático autorizado.

4.2 Servidores y equipos de comunicación instalados en gabinetes para servidores o racks debidamente aterrizados y asegurados;

4.3 Cableado estructurado para el uso de los equipos de cómputo;

4.4 Sistema de climatización que como mínimo mantenga la temperatura y humedad en los niveles recomendados por los fabricantes;

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

4.6 Sensores de temperatura y humedad y detectores de humo con mecanismos de alertas;

Fuente: http://www.leybook.com/doc/16935

4.7 Equipos que aseguren el suministro de energía de manera que permitan el apagado controlado de los equipos en caso de fallas de energía;

4.8 Mecanismos para el control de ingreso y salida del CPD con su respectivo registro.

CAPÍTULO VII
ADMINISTRACIÓN DE SERVICIOS Y CONTRATOS CON TERCEROS RELACIONADOS CON TI

Artículo 13. Requerimientos para la administración de servicios y contratos con terceros relacionados con TI.- Con el objeto de garantizar que los recursos y servicios de TI provistos por terceros se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las IMF deberán contar, al menos, con lo siguiente:

1. Procedimiento formalizado para la evaluación y selección del proveedor de servicios, previo a su contratación, que considere los siguientes criterios mínimos:

1.1 Experiencia y competencia técnica del proveedor para implementar los servicios requeridos;

1.2 Fortaleza financiera del proveedor (estados financieros y cualquier otra información relevante);

1.3 Reputación comercial, quejas, cumplimiento y litigios pendientes del proveedor;

1.4 Controles internos;

1.5 Planes de contingencia, incluyendo pruebas de recuperación tecnológica;

1.6 Dependencia del proveedor de servicios primario con subcontratistas;

1.7 Cobertura de seguros; y

1.8 Ubicación geográfica del proveedor.

2. Contrato formalizado con el proveedor de servicios, que establezca claramente el objeto y el alcance de los servicios, los productos o resultados esperados, los plazos de entrega, los derechos y obligaciones de las partes, entre otros aspectos.
3. Requerimientos contractuales específicos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad del proveedor de servicios de TI en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información.

4. Requerimientos contractuales específicos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación técnica y de usuario, a fin de reducir la dependencia de la IMF con el proveedor de servicios de TI y los eventos de riesgo operacional que esto origina.

5. Requerimientos contractuales específicos que faculten a la IMF y a la CONAMI, en caso de ser necesario, a practicar evaluaciones periódicas en el proveedor de servicios de TI, directamente o mediante auditorías independientes en la parte que se relaciona al servicio provisto. Lo anterior será requerido sólo cuando la IMF contrate su Centro de Procesamiento de Datos con un tercero.

Artículo 14.- Responsabilidades de la IMF en la contratación de servicios con terceros.- La IMF

Fuente: http://www.leybook.com/doc/16935

tendrá la responsabilidad directa, absoluta e indelegable por los servicios que contrate con terceros, debiendo validar y garantizar en todo momento que tanto los servicios, como el proveedor contratado, se ajusten a los requerimientos establecidos en la presente norma

CAPÍTULO VIII
PLANES DE CONTINGENCIA

Articulo 15. Plan de contingencias de TI.- La IMF deberá contar con un plan de contingencias de TI aprobado por la Junta Directiva, que considere, como mínimo, los siguientes aspectos:

1. Objetivo del plan

2. Metodología del plan que, al menos, incluya lo siguiente:

2.1 Identificación de los recursos críticos de TI.

2.2 Identificación del impacto por la interrupción de los servicios críticos de TI.

2.3 Definición de los tiempos de interrupción del servicio permisibles.

3. Desarrollo de procedimientos de recuperación de operaciones criticas para cada evento identificado de acuerdo a las prioridades de recuperación.

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

6. Medidas de prevención.

7. Recursos mínimos asignados para la recuperación.

8. Programación y ejecución anual de pruebas identificadas en el Plan de Contingencia. Así como su actualización conforme los resultados obtenidos, nuevos riesgos identificados e incidentes de seguridad de información acontecidos. Los resultados de esta ejecución deberán ser comunicados al Presidente Ejecutivo.

CAPÍTULO IX
ADMINISTRACIÓN INTEGRAL DE RIESGO TECNOLÓGICO

Artículo 16. Evaluación del riesgo tecnológico.- La IMF deberá implementar procedimientos internos que permitan autoevaluarse de acuerdo con esta norma. Los resultados de dicha evaluación y la evaluación del nivel de exposición de riesgo tecnológico deben presentarse, al menos, una vez al año a la Junta Directiva de la institución.

Artículo 17. Metodología de administración integral de riesgo tecnológico.- La IMF deberá aprobar formalmente y documentar una metodología de administración de riesgo tecnológico que considere los análisis de riesgo de forma cuantitativa o cualitativa.

Artículo 18. Análisis cuantitativo o cualitativo de riesgo.- El análisis cuantitativo o cualitativo de riesgo tecnológico debe considerar la realización de las siguientes actividades mínimas:

1. Para el análisis cuantitativo:

1.1 La conformación de una base de datos histórica de eventos de pérdida o frustración de ganancia producto de la materialización de riesgos tecnológicos

Fuente: http://www.leybook.com/doc/16935

1.2 La determinación de la Frecuencia de ocurrencia de dichos eventos.

1.3 La determinación de su impacto o severidad.

1.4 La estimación y aprovisionamiento del valor en riesgo en base a información histórica razonable.

2. Para el análisis cualitativo:

2.1 La identificación y categorización de los riesgos.

2.2 La determinación de los riesgos inherentes a cada proceso que involucre el uso de tecnología de la información, describiendo su composición en amenazas y/o vulnerabilidades, su probabilidad de ocurrencia e impacto.

2.3 La identificación de controles que mitiguen los riesgos identificados, su clasificación (Por ejemplo: de detección, disuasivos, preventivos, y/o correctivos), su nivel de efectividad y cumplimiento.

2.4 La determinación del riesgo residual resultante de la aplicación de los controles a los riesgos inherentes.

2.5 La determinación de niveles aceptables de riesgo.

2.6 La identificación y seguimiento a planes de mejora cuando se requiera.

2.7 La realización de matrices y/o mapas de riesgo o severidad.

CAPÍTULO X
INFRACCIONES E IMPOSICIÓN DE SANCIONES

Artículo 19. Sanciones.- El Presidente Ejecutivo podrá imponer las sanciones previstas en las disposiciones del Capítulo IV, del Título IV de la Ley, conforme lo establecido en la presente norma.

El cumplimiento de la sanción por el infractor no significa la convalidación de la situación irregular, debiendo el infractor cesar de inmediato los actos u omisiones que dieron lugar a la sanción.

Artículo 20. Multas a las IMF.- El Presidente Ejecutivo impondrá multa a las IMF entre quinientos y diez mil unidades de multa, El valor de cada unidad de multa será el equivalente en moneda nacional a un dólar de los Estados Unidos de América, conforme al tipo de cambio oficial establecido por el Banco Central de Nicaragua, vigente a la fecha de la imposición de la sanción.

Las multas consignadas en la presente norma, serán pagadas a la Tesorería General de la República.

Artículo 21. Categorías de infracciones.- Las infracciones se clasifican en leves, moderadas y graves, de acuerdo con su nivel de gravedad, sus efectos y consecuencias, conforme a lo señalado en la presente norma.

1. Leves:

1.1 No contar con controles documentados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia.

Fuente: http://www.leybook.com/doc/16935

1. 2 No contar con planes de mantenimiento preventivo conforme a lo recomendado por los proveedores o los mínimos requeridos para prevenir daños.
1.3 No contar con inventarios actualizados de hardware, licencias de software, diagramas de red y comunicaciones.

1.4 No contar con controles para la detección y desinfección de virus informáticos, software malicioso y actualización de parches de seguridad.

1.5 No contar con controles para el acceso y restricción de la navegación a Internet conforme a los perfiles de usuarios.

1.6 Cualesquiera otras infracciones de igual o similar gravedad que se cometan a las disposiciones establecidas en la presente norma y/o a las instrucciones del Presidente Ejecutivo.

2. Moderadas:

2. 1 Reincidir en la comisión de infracciones leves.

2.2 No contar con procedimientos formalizados para la aprobación de nuevos sistemas de información o, teniéndolos, no reúnan las condiciones establecidas en el artículo 10 de la presente norma.

2.3 No contar con un procedimiento formalizado para la administración del ciclo de vida del desarrollo de sistemas de información o, teniéndolo, no reúnan las condiciones establecidas en el artículo 10 de la presente norma.

2.4 No contar con un procedimiento formalizado de control de cambios a producción conforme lo establecido en el artículo 10 de la presente norma.

2.5 Adquirir sistemas de información sin ajustarse a lo establecido en el artículo 10 de la presente norma.

2.6 Desarrollar y mantener sistemas de información a través de proveedores externos sin ajustarse a lo establecido en el artículo 10 de la presente norma

2.7 No contar con procedimientos de migración de sistemas de información o, teniéndolo, no reúna las condiciones establecidas en el artículo 10 de la presente norma.

2.8 No contar con procedimientos formalizados para la administración de procesos críticos relacionados con la gestión de operaciones de TI, así como, para el manejo de incidentes de seguridad

2.9 No contar con la documentación requerida para los procesos de administración de las bases de datos conforme a lo establecido en el artículo ll de la presente norma.

2.10 No contar con políticas y procedimientos de seguridad de la información, o teniéndolas, no reúnan las condiciones establecidas en el artículo 12 de la presente norma.

2.11 No contar con acuerdos de confidencialidad respecto a la información de la institución.

2.12 No contar con un inventario de activos de información o, teniéndolo, no reúna las condiciones previstas en el artículo 12 de la presente norma

Fuente: http://www.leybook.com/doc/16935

2.13 No contar con un centro de procesamiento de datos o, teniéndolo, no reúna las características establecidas en el artículo 12 de la presente norma.

2.14 No contar con un procedimiento formalizado para la evaluación y selección de proveedores de servicios de TI conforme a lo establecido en el artículo 13 de la presente norma, o teniéndolo, incumpla dicho procedimiento

2.15 No tener contratos formalizados con sus proveedores de servicios de TI o, teniéndolos, no contengan los requerimientos previstos en el artículo 13 de la presente norma.

2.16 No informar al Presidente Ejecutivo la ocurrencia de eventos de TI conforme a lo establecido en el artículo 28 de la presente norma.
2.17 Cualesquiera otras infracciones de igual o similar gravedad que se cometan a las disposiciones establecidas en la presente norma y/o a las instrucciones del Presidente Ejecutivo.

3. Graves:

3.1 Reincidir en la comisión de infracciones moderadas.

3 2 Incumplir instrucciones emitidas por el Presidente Ejecutivo.

3.3 El incumplimiento por parte de la Junta Directiva de las responsabilidades asignadas en el artículo 5 de la presente norma.

3.4 No contar con una metodología integral para la administración de riesgos de TI, que cumpla con lo establecido en el Capítulo IX de la presente norma.

3.5 No contar con un Plan Estratégico de TI, o teniéndolo, no reúna las características previstas en el artículo 8 de la presente norma, o se encuentre desactualizado.

3.6 No tener copias de seguridad de todos los datos e información que considere necesaria para el continuo funcionamiento de la misma o, teniéndolas, no reúnan las condiciones previstas en el artículo II de la presente norma.

3.7 No contar con procedimientos de activación, gestión y revisión de bitácoras, pistas de auditoría, etc.

3.8 No contar con un plan de contingencias de TI aprobado por la Junta Directiva, o teniéndolo, no cumpla con los aspectos mínimos señalados en el artículo 15 de la presente norma.

3.9 Cualesquiera otras infracciones de igual o similar gravedad que se cometan a las disposiciones establecidas en la presente norma y/o a las instrucciones del Presidente Ejecutivo.

Articulo 22. Relación de sanciones y multas.- Las sanciones y multas aplicables a cada categoría de infracciones son las que se indican a continuación:

1. Por la comisión ¡le infracciones leves corresponde aplicar una o más de las siguientes sanciones:

1.1 Amonestación al ejecutivo principal, al auditor interno y miembros de la Junta Directiva,

Fuente: http://www.leybook.com/doc/16935

1.2 Multa a la IMF no menor de quinientas (500) unidades de multa ni mayor de cinco mil (5,000) unidades de multa.

1.3 Multa personal a quienes resulten responsables entre los directores y principal ejecutivo no menor de quinientas (500) unidades de multa ni mayor de tres mil (5,000) unidades de multa

2. Por lo comisión de infracciones moderadas corresponde aplicar una o más de las siguientes sanciones:

2.1 Multa a la IMF no menor de cinco mil (5,000) unidades de multa ni mayor de ocho mil (8,000) unidades de multa.

2.2 Multa personal a quienes resulten responsables entre los directores y principal ejecutivo no menor de cinco mil (5,000) unidades de multa ni mayor de ocho mil (8, 000) unidades de multa.

2.3 Suspensión temporal del programa de fomento o de incentivos concedidos conforme a la Ley, por un período no mayor de seis (6) meses.

2.4 Remoción del cargo de director, miembro de Junta Directiva, principal ejecutivo o auditor interno en caso de reincidencia en la comisión de infracciones graves.

3. Por la comisión de infracciones graves corresponde aplicar una o más de las siguientes sanciones:

3.1 Multa a la IMF no menor de ocho mil (8,000) unidades de multa ni mayor de diez mil (10,000) unidades de multa.

3.2 Multa personal a quienes resulten responsables entre los directores y principal ejecutivo no menor de ocho mil (8,000) unidades de multa ni mayor de diez (10,000) unidades de multa.

3.3 Suspensión temporal del programa de fomento o de incentivos concedidos conforme a la Ley, por un período mayor a seis (6) meses y hasta doce (12) meses.

3.4 Cancelación de la inscripción de la IMF en el Registro Nacional de IFIM a cargo de la CONAMI.

3.5 Remoción del cargo de director, miembro de Junta Directiva, principal ejecutivo o auditor interno en caso de reincidencia en la comisión de infracciones muy graves.

Artículo 23. Reincidencia.- En caso de una segunda infracción sobre un hecho ya sancionado, dentro de un periodo de doce meses, de la misma naturaleza de los indicados en el artículo 21 de la presente norma, el Presidente Ejecutivo impondrá una sanción igual al doble de las unidades de multa impuesta en la primera infracción.

Artículo 24. Procedimiento y plazo para el pago de multas – Una vez emitida la correspondiente resolución por el Presidente Ejecutivo, mediante la cual se establezca la infracción a la norma, la IMF tendrá cinco (5) días hábiles para proceder al pago de la multa impuesta de conformidad con la categoría de la infracción.

El monto de la multa será depositado en la cuenta que para tal efecto establezca el Ministerio de Hacienda y Crédito Público, a través de la Tesorería General de la República.

Fuente: http://www.leybook.com/doc/16935

La IMF deberá remitir la minuta de depósito del monto de la multa al Presidente Ejecutivo. Si transcurrido el plazo indicado en el primer párrafo de este artículo, la IMF no remite el respectivo comprobante de pago, el Presidente Ejecutivo procederá a requerir el pago en el término de 24 horas, dando conocimiento a las autoridades del Ministerio de Hacienda y Crédito Público, para que proceda hacer efectivo el cobro.

Los plazos establecidos en el presente artículo son improrrogables, salvo norma expresa en contrario, y se computan a partir del día hábil siguiente de aquél en que se practique la notificación de la infracción

Artículo 25. Responsabilidades de la Junta Directiva.- Las sanciones aplicadas a las IMF por la CONAMI, así como, aquellas aplicadas a sus directores, miembros de la Junta Directiva, ejecutivo principal y auditor interno, deberán ser comunicadas a la Junta Directiva correspondiente, dejándose constancia de dicha comunicación en el acta de la primera sesión de dicho órgano que celebre luego de la recepción de la resolución respectiva o dentro de los treinta (30) días calendarios posteriores a su recepción, lo que ocurra primero. De considerarlo necesario y en atención a la gravedad de los hechos materia de la sanción, el Presidente Ejecutivo puede disponer se convoque a una sesión especial de Junta Directiva, para el cumplimiento de lo previsto en el presente párrafo.

La Junta Directiva, a su vez, es responsable de informar a la junta general de accionistas u órgano equivalente, en la sesión más próxima, las sanciones que la CONAMI imponga a las IMF, a sus directores, miembros de la Junta Directiva, ejecutivo principal y auditor interno por la comisión de infracciones moderadas y graves, dejándose constancia de dicha comunicación en el acta correspondiente a la referida sesión. Asimismo, es responsable de que la IMF cumpla las sanciones que la CONAMI les imponga y de que se cumplan las sanciones que se impongan a sus directores, miembros de la Junta Directiva, ejecutivo principal y auditor interno, según corresponda.

Artículo 26. Impugnación.- El sancionado podrá interponer los recursos administrativos previstos en el artículo 66 de la Ley y conforme la Norma sobre los Procedimientos de los Recursos Administrativos ante la Comisión Nacional de Micro finanzas (CONAMI), publicada en La Gaceta, Diario Oficial No. 244 del veinte de diciembre del dos mil doce.

Artículo 27. Registro y publicidad de sanciones.- Las sanciones que se impongan en virtud de la presente Norma, deben ser notificadas a los infractores y se anotarán en el registro de sanciones de la CONAMI.

El Presidente Ejecutivo, de forma periódica, publicará en la página web de la institución, las sanciones que imponga a las IMF y la razón de dicha sanciones.

CAPÍTULO XI
DISPOSICIONES FINALES

Artículo 28. Información al Presidente Ejecutivo.- La IMF deberá informar al Presidente Ejecutivo, por escrito y de manera inmediata, la ocurrencia de cualquiera de los siguientes eventos, y dentro de las posteriores veinte y cuatro (24) horas, presentar detalle del resultado y las acciones tomadas para corregir el mismo:

1. La ocurrencia de incidentes de seguridad que hubiesen afectado la confidencialidad, integridad o disponibilidad de la información de sus clientes.

2. La activación de planes de contingencia de TI y/o estrategias de recuperación, así como los resultados obtenidos.

Fuente: http://www.leybook.com/doc/16935

2. La interrupción en el funcionamiento normal de los sistemas operativos y software aplicativos principales que afecten la prestación de servicios a sus clientes

Artículo 29. Supervisión de la CONAMI.- La CONAMI, en sus supervisiones in situ y extra situ, verificará el cumplimiento de las disposiciones establecidas en la presente norma.

Artículo 30. Transitorios.- Las IMF deberán adecuarse a los requerimientos establecidos en la presente norma, a más tardar, en los siguientes plazos, contados a partir de la entrada en vigencia de la misma:

CAPÍTULO III	PLAZOS
Artículo 5, Responsabilidades de la Junta Directiva, numeral 1), 3) y Comité de Riesgo de TI	9 meses
Artículo 7. Estructura Organizacional y Procedimientos	1 año
Articulo 8. Planeación de TI	9 meses
CAPITULO IV	
Artículo 10. Requerimientos para la adquisición, desarrollo e implementación de sistemas del año información	1 año
CAPÍTULO V	
Artículo 11. Requerimientos para la gestión de operaciones de TI	1 año
CAPÍTULO VI	
Artículo l2. Requerimientos para la administración de Seguridad de la Información; a) Políticas y procedimientos de seguridad de la Información b) Acuerdos de confidencialidad c) Inventario de activos de información d) Centro de procesamiento de datos (CPD)	9 meses 9 meses 1 año 2 años
CAPÍTULO VII	
Artículo 13. Requerimiento para la administración de servicios y contratos con terceros relacionados con TI	9 meses
CAPÍTULO VIII	
Artículo 15. Plan de contingencias de TI	2 años
CAPÍTULO IX	
Artículos 16, 17 y 18 (Administración Integral de Riesgo Tecnológico)	2 años

El plazo de adecuación para las instituciones cuyo registro sea aprobado con posterioridad a la entrada en vigencia de la presente norma, iniciará a partir de la fecha de registro de las mismas.

Articulo 31. Facultad del Presidente Ejecutivo.- Se faculta al Presidente Ejecutivo a prorrogar de manera individual los plazos establecidos en el artículo precedente, con base en solicitud razonada por

parte de la IMF interesada.

Artículo 32. Vigencia.- La presente norma entrará en vigencia a partir de su publicación en la Gaceta, Diario Oficial. (Ü Jim Madriz López, Presidente Ejecutivo (f) Flavio José Chiong Arauz, Miembro Suplente (f) Rosa Pasos Argüello, Miembro Propietario (f) Freddy José Cruz Cortez, Miembro Propietario (f) Álvaro José Contreras, Secretario. **(f) Álvaro José Contreras. Secretario Consejo Directivo**

Fuente: http://www.leybook.com/doc/16935