PROYECTO DE REFROMAS A LAS NORMAS PARA LA GESTIÓN DEL RIESGO TECNOLÓGICO Y CONTINUIDAD DE LAS OPERACIONES DE TECNOLOGIA

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- OBJETO
Las presentes Normas tienen por objeto regular la gestión del riesgo tecnológico y la continuidad de las operaciones de tecnología en las instituciones supervisadas por la Comisión Nacional de Bancos y Seguros.

ARTÍCULO 2.- ALCANCE
Las disposiciones contenidas en las presentes Normas serán aplicables a todas las instituciones supervisadas por la Comisión Nacional de Bancos y Seguros, en función del tamaño, naturaleza y complejidad de sus operaciones.

ARTÍCULO 3.- NORMAS RELACIONADAS
Las disposiciones contenidas en las presentes Normas deberán aplicarse en adición a las contenidas en la Norma sobre Gestión Integral de Riesgos y en la Norma de Gestión de Riesgo Operativo.

ARTÍCULO 4.- DEFINICIONES
Adicionalmente a las definiciones establecidas en la Norma Sobre Gestión Integral de Riesgos, serán aplicables en las presentes Normas las siguientes definiciones:

a) **Acuerdos de Nivel de Servicio (SLA):** Convenio entre el área de Tecnologías de Información (TI) y los usuarios finales; o entre la institución supervisada y un proveedor de tecnologías de información, en el cual se detallen los servicios prestados y las características esperadas de éstos, entre ellas exactitud, integridad, puntualidad y seguridad.

b) **Análisis de Impacto del Negocio (BIA):** Etapa de la planeación de continuidad de negocio en la que se identifican los eventos que podrían tener un impacto sobre la continuidad de operaciones y su impacto financiero, humano y de reputación sobre la institución supervisada.

c) **Comisión o CNBS:** Comisión Nacional de Bancos y Seguros.

d) **Confidencialidad:** Característica que consiste en que la información sea accesible solo para quienes están autorizados.

e) **Disponibilidad:** Característica que consiste en que la información debe estar disponible en el momento que se requiera.

f) **Gobierno de TI:** Conjunto de principios, prácticas y normas cuyo objetivo es dirigir y controlar la organización de TI, para asegurar que su rendimiento logre un alineamiento con los objetivos institucionales, a través de la generación de valor al negocio y de una gestión efectiva de los riesgos asociados.

g) **Infraestructura como Servicio (IaaS, por sus siglas en inglés):** Capacidad de un proveedor para configurar procesamiento, almacenamiento, redes y otros

recursos de TI, ofreciendo al cliente que lo contrata, la posibilidad de implementar y ejecutar software arbitrario, el cual puede incluir sistemas operativos y aplicaciones.

h) **Integridad:** Característica que consiste en que la información solo puede ser creada y modificada por quien esté autorizado para hacerlo.

i) **Mejores Prácticas:** Marcos de referencia de control, estándares internaciones, u otros estudios que ayuden a la gestión, control, monitoreo y mejora de las actividades de TI, y que aumenten el valor del negocio y reduzcan los riesgos.

j) **Plataforma como Servicio (PaaS, por sus siglas en inglés):** Capacidad para implementar en la infraestructura de la nube aplicaciones creadas o adquiridas por el cliente que se hayan creado utilizando lenguajes y herramientas de programación que estén respaldados por el proveedor.

k) **Productos y/o Servicios Críticos:** Aquellos procesos que soportan la prestación de productos y/o servicios, cuya interrupción o degradación puede poner en riesgo las operaciones normales del negocio, afectando sus ingresos, solvencia, continuidad operativa o reputación de forma significativa. Estos procesos tienen la característica que no pueden ejecutarse a menos que se reemplacen por capacidades idénticas, y no se pueden reemplazar por métodos manuales. Su tolerancia a interrupciones es muy baja y el costo de interrupción es muy alto.

l) **Proveedor de Servicios de TI:** Persona natural o jurídica que provee o presta un servicio relacionado con la tecnología de información, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices.

m) **Punto Objetivo de Recuperación (RPO):** Volumen de datos en riesgo de pérdida que la institución considera tolerable en caso de una interrupción en sus operaciones, de acuerdo al apetito de riesgo definido por la Institución.

n) **Riesgo Tecnológico:** Posibilidad de pérdidas derivadas de un evento o incidente relacionado con la infraestructura tecnológica, el uso de la tecnología que afecta el desarrollo de los procesos de negocio o de la gestión de riesgos de la institución, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad, cumplimiento o uso oportuno de la información. Las instituciones supervisadas deberán gestionar el riesgo tecnológico, de acuerdo a la estrategia, metodología, manuales, políticas y procedimientos empleados para la gestión del riesgo operativo, de acuerdo a lo establecido en la respectiva norma.

o) **Servicios basados en la Nube:** Modelo que permite el acceso bajo demanda a la red a un conjunto compartido de recursos informáticos configurables (redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y liberados rápidamente por el proveedor de servicios.

p) **Software como Servicio (SaaS, por sus siglas en inglés):** Capacidad para utilizar las aplicaciones del proveedor que se ejecutan en la infraestructura de la nube, a las cuales se puede acceder desde diferentes dispositivos a través de una interfaz de cliente.

q) **Tecnologías de Información (TI):** Conjunto de recursos tecnológicos que permiten la captura, almacenamiento, transformación, transmisión y presentación

de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

r) **Tiempo Objetivo de Recuperación (RTO, por sus siglas en inglés)**: Es el tiempo establecido por la institución supervisada para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo de tiempo luego del cual la viabilidad de la institución sería afectada seriamente, si un producto o servicio en particular no es reanudado.

CAPÍTULO II
DE LAS RESPONSABILIDADES DEL DIRECTORIO Y DEL COMITÉ DE RIESGOS

ARTÍCULO 5.- DE LA GESTIÓN DEL RIESGO TECNOLÓGICO

El Consejo de Administración, Junta Directiva u Órgano que haga sus veces en las instituciones supervisadas, debe gestionar adecuadamente el riesgo derivado de los sistemas de información, tomando en cuenta que su seguridad, continuidad, desarrollo y funcionamiento constituyen un elemento primordial en su operatividad y manejo administrativo y financiero.

ARTÍCULO 6.- RESPONSABILIDAD DEL DIRECTORIO

Adicionalmente a las responsabilidades establecidas en la Norma de Gestión de Riesgo Operativo y en la Norma de Gestión Integral de Riesgos, en materia de gestión del riesgo tecnológico, el Directorio tiene las siguientes responsabilidades:

a) Velar por la existencia e implementación de un Gobierno de TI.
b) Aprobar el Marco de Gestión de TI y el Marco de Gestión de Seguridad de la Información, los cuales contendrán las políticas y procedimientos para administrar de manera adecuada y prudente la entrega de productos y servicios de TI en la institución, la seguridad y los riesgos de tecnología de la información, incidiendo positivamente en los procesos críticos asociados a dicho riesgo.
c) Aprobar el Plan Estratégico de TI.
d) Aprobar las prioridades de inversión de TI de conformidad con los objetivos definidos en el Plan Estratégico de la institución.
e) Velar porque se defina y se mantenga una estructura organizacional, las políticas y los procedimientos que permitan gestionar las tecnologías de información y sus riesgos asociados, acorde a su tamaño, naturaleza y complejidad de las operaciones que realiza.
f) Proveer a través de la Alta Gerencia, los recursos necesarios para lograr el cumplimiento del Marco de Gestión de TI, el Marco de Gestión de Seguridad de la Información y de Continuidad de las Operaciones Tecnológicas, así como las disposiciones contenidas en las presentes Normas.
g) Procurar la disponibilidad, capacidad y el desempeño de los sistemas de información requeridos para la continuidad de procesos críticos del negocio.
h) Conocer los reportes sobre el nivel de cumplimiento del Marco de Gestión de las Tecnologías de Información y el Marco de Gestión de Seguridad de la Información

aprobados, así como las propuestas sobre acciones correctivas a adoptar para corregir con relación a los incumplimientos. Lo anterior, sin perjuicio de las sanciones legales que el caso amerite.

i) Velar por la administración adecuada de los riesgos asociados a TI.

ARTÍCULO 7.- RESPONSABILIDAD DEL COMITÉ DE RIESGOS EN MATERIA DE TI

El Comité de Riesgos o éste a través de un sub comité de TI, será responsable de coordinar los temas de Tecnologías de Información con el fin de garantizar el alineamiento estratégico y la adecuada gestión del riesgo de TI, cumpliendo entre otras, las siguientes funciones:

a) Proponer al Directorio el Marco de Gestión de las Tecnologías de la Información y Comunicaciones;
b) Brindar asesoría en la formulación del Plan Estratégico de TI para asegurar el alineamiento con la estrategia institucional;
c) Vigilar el funcionamiento del entorno de TI;
d) Asegurar que se mantiene un proceso de gestión de riesgo tecnológico adecuado y mantener informado al Directorio sobre su efectividad;
e) Supervisar que el riesgo tecnológico sea identificado, evaluado, mitigado, monitoreado y comunicado a los diferentes niveles de la institución en forma efectiva;
f) Dar seguimiento a los planes operativos y proyectos de TI;
g) Revisar el marco de Gestión de TI de acuerdo al comportamiento de los indicadores del mismo marco o a raíz de observaciones de los entes de control interno, auditoria interna, auditoria externa y de la Comisión; y,
h) Proponer los planes de acción derivados de los hallazgos sobre la Gestión de TI formulados por los entes de control interno, auditoria interna, auditoria externa y de la Comisión.

CAPÍTULO III
DE LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ARTÍCULO 8.- GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

El gobierno de TI debe contemplar la implementación de políticas, planes estratégicos y procedimientos, así como la asignación de recursos necesarios para la gestión de TI, que serán revisadas de manera permanente y continua, enfocándose como mínimo en los siguientes aspectos:

a) Alineación Estratégica: Contar con un Plan Estratégico de TI en el que se definan las iniciativas de TI alineadas con las metas del negocio, sus planes y operaciones, para lo cual debe contar con la identificación de los objetivos a corto, mediano y largo plazo de las actividades y proyectos de TI.

b) Entrega de Valor: Gestionar las tecnologías de información asegurándose que genere los beneficios proyectados en el plan estratégico.

c) Administración de Recursos: Administrar de forma óptima y adecuada los recursos de TI, tales como el recurso humano y la infraestructura tecnológica, asegurando el desarrollo y monitoreo de un presupuesto para la administración de dichos recursos.

d) **Gestión de Riesgos de TI**: Identificar, evaluar, mitigar, monitorear y comunicar los riesgos a los que se encuentra expuesta la institución, así como determinar su tolerancia al riesgo. Para ello debe contar con una metodología de gestión de riesgos de TI, la cual debe estar alineada a la metodología institucional de gestión de riesgo operativo, que incluya el diseño de una matriz de riesgos y que garantice la seguridad de los sistemas, en donde se indique, como mínimo, las medidas de control de la seguridad lógica, de seguridad física y de seguridad de las redes.
e) **Medición del Desempeño**: Dar seguimiento permanente a la implementación de la estrategia de TI mediante la revisión continua del desempeño de los procesos y el logro de los objetivos y metas de TI, así como a la terminación de sus proyectos, uso de los recursos y entrega del servicio.

ARTÍCULO 9.- PLANEACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

Las instituciones, como parte de su Plan Estratégico Institucional, deben tener un Plan Estratégico de TI alineado con la estrategia de negocios, para gestionar la infraestructura de TI, los sistemas de información, la base de datos y al recurso humano de TI. La periodicidad de formulación y/o actualización de dicho plan debe alinearse con la periodicidad con que se formule y/o actualice el Plan Estratégico Institucional.

El Plan Estratégico de TI debe incluir, como mínimo los aspectos siguientes:

a) Objetivos de TI, los cuales deben estar alineados con la estrategia de negocios en función del análisis e impacto de factores internos y externos en esta materia, tales como oportunidades, limitaciones y desempeño de la infraestructura de TI, los sistemas de información, la base de datos y el recurso humano relacionado;
b) Estrategias de TI para la consecución de los objetivos;
c) Proyectos y actividades específicas; y,
d) El presupuesto financiero para su ejecución.

Las instituciones deben poner a disposición de la Comisión el Plan Estratégico de TI y sus modificaciones, cuando ésta lo requiera.

ARTÍCULO 10.- ORGANIZACIÓN DEL ÁREA ENCARGADA DE TECNOLOGÍAS DE INFORMACIÓN

El área encargada de tecnología de información debe contar con una estructura organizacional que se encuentre alineada con el Plan Estratégico de TI, así como contar con una adecuada separación de funciones, delegación de autoridad, definición de roles y asignación de responsabilidades; asegurándose que el recurso humano de TI tenga las capacidades necesarias mediante programas de entrenamiento y capacitación. Todo esto soportado con un marco de trabajo estructurado en procesos, los cuales deben estar debidamente identificados y documentados.

Esta área debe contar con independencia funcional y operativa de áreas usuarias de su gestión. Asimismo, debe estar a cargo de un ejecutivo especializado con formación académica y experiencia comprobada sobre la administración de Tecnologías de Información y Comunicaciones.

ARTÍCULO 11.- MARCO DE GESTIÓN DE TI

La institución supervisada debe diseñar, implementar, documentar, monitorear y actualizar un Marco de Gestión de TI, el cual está conformado por una serie de políticas, procesos y procedimientos relacionados a la adquisición, mantenimiento e implementación de los sistemas, bases de datos e infraestructura de TI, garantizando que toda tarea o proceso interno de TI esté debidamente documentado, esto con el objetivo de lograr un entorno operativo que tenga un nivel adecuado de madurez.

Este Marco de TI debe revisarse y actualizarse en un periodo no mayor a dos (2) años o al momento de presentarse cambios significativos en el ambiente operacional o del negocio.

El Marco de Gestión de TI debe elaborarse considerando los siguientes aspectos:

a) Plan Estratégico de TI;
b) Infraestructura de tecnología;
c) Cumplimiento de requerimientos legales y regulatorios;
d) Administración de proyectos de sistemas;
e) Administración de la calidad;
f) Adquisición, instalación y mantenimiento de software y hardware;
g) Administración de cambios;
h) Administración de servicios con terceros;
i) Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica;
j) Continuidad del negocio;
k) Seguridad de los sistemas;
l) Educación y entrenamiento de usuarios;
m) Administración de los datos;
n) Administración de instalaciones; y,
o) Planes de sucesión del personal clave de TI.

CAPÍTULO IV
TERCERIZACIÓN DE SERVICIOS DE TI

ARTÍCULO 12.- RESPONSABILIDAD

Las instituciones supervisadas son responsables ante la Comisión de las funciones o procesos que puedan ser objeto de una tercerización y deben verificar que se mantengan las disposiciones contempladas en la norma de Gestión de Riesgo Operativo y en las presentes Normas. Asimismo, deben asegurarse que el procesamiento y la información objeto de la tercerización en todo momento se encuentre aislada lógicamente del resto de las operaciones del proveedor de servicios de TI.

ARTÍCULO 13.- DEBIDA DILIGENCIA SOBRE EL PROVEEDOR DE SERVICIOS DE TI

Las instituciones supervisadas deben ejecutar acciones de debida diligencia para seleccionar el proveedor de servicios de TI, analizando al menos la viabilidad técnica, financiera y legal del proveedor, de modo que alguno de estos aspectos no afecten la prestación del servicio en el futuro.

ARTÍCULO 14.- TERCERIZACIÓN SIGNIFICATIVA DE TI

Para efectos de las presentes Normas se considera tercerización significativa, además de las identificadas por la propia institución, la de auditoria de sistemas y del procesamiento de datos.

Las instituciones supervisadas deben asegurarse que en los casos de tercerización significativa de TI, los contratos suscritos con los proveedores correspondientes incluyan los aspectos mínimos establecidos en la Norma de Gestión de Riesgo Operativo.

En caso que el objeto de tercerización sea un sistema de información, la institución supervisada debe requerir al proveedor la entrega de la documentación técnica actualizada relacionada a la arquitectura de información del sistema, la cual debe contener como mínimo un diccionario de datos de las tablas del sistema y diagramas entidad - relación de la base de datos.

La tercerización significativa de TI debe ser hecha del conocimiento de la Comisión, treinta (30) días calendario previo a la suscripción del acuerdo. La Comisión podrá formular observaciones a dicho acuerdo y requerir la información adicional necesaria para su análisis.

ARTÍCULO 15.- TERCERIZACIÓN SIGNIFICATIVA DE PROCESAMIENTO DE DATOS

En caso que las instituciones supervisadas opten por realizar una tercerización significativa de su procesamiento de datos, requerirán de la autorización previa y expresa de la Comisión.

En caso que el procesamiento de datos sea realizado fuera del país, la Comisión requerirá que el proveedor del servicio en el exterior se encuentre bajo la supervisión de una autoridad supervisora, similar a la Comisión, en el país en el cual se brindará dicho servicio.

La autorización concedida por la Comisión, de ser el caso, es específica al proveedor del servicio y el país desde el que se recibe, así como a las condiciones generales que fueron objeto de la autorización, por lo que de existir modificaciones en ellas, se requiere de un nuevo procedimiento de autorización ante la Comisión.

Las instituciones deben adjuntar a la solicitud de autorización referida en este Artículo, la información requerida en el Anexo No. 1 de las presentes Normas.

Una vez recibida la documentación completa, dentro de un plazo que no excede de sesenta (60) días hábiles, la Comisión emitirá la Resolución autorizando o denegando la solicitud presentada por la institución supervisada.

Los servicios objeto de subcontratación en el exterior deberán ser sometidos anualmente a un examen de auditoría independiente, realizada por una empresa auditora de prestigio, de conformidad a las mejores prácticas internacionales, debiendo cada entidad remitir a esta Comisión los respectivos informes, a más tardar diez (10) días hábiles posteriores al cierre del primer trimestre de cada año.

ARTÍCULO 16.- SERVICIOS BASADOS EN LA NUBE

Las instituciones supervisadas podrán optar por tercerizar sus servicios bajo el esquema de “en la nube” en cualquiera de sus modalidades: Infraestructura como servicio (IaaS), Plataforma como un servicio (PaaS) y Software como un servicio (SaaS). Estas solicitudes

deberán ser aprobadas por la Comisión, para lo cual las instituciones deberán remitir la información requerida en el Anexo 1 de las presentes Normas.

ARTÍCULO 17.- PROCESAMIENTO DE INFORMACIÓN FUERA DE TERRITORIO NACIONAL

Las instituciones supervisadas cuya plataforma de procesamiento de información se encuentre fuera del territorio nacional, o aquellas que en un determinado momento opten por ello, deben mantener en el país una réplica en línea del ambiente de procesamiento de los sistemas de información y de las bases de datos del ambiente de producción, así como copias de los respaldos de información del sistema principal. La Comisión en todo momento podrá acceder de forma irrestricta desde el territorio nacional, a la información y a los sistemas tanto en la plataforma de procesamiento de información como en la réplica en territorio nacional. Asimismo, las instituciones supervisadas deberán realizar al menos una vez al año, pruebas de funcionamiento de la réplica del ambiente de procesamiento de sus sistemas y sus base de datos.

Las instituciones deberán asumir la responsabilidad del conocimiento pleno sobre la arquitectura de las bases de datos y la estructura de procesamiento, a través de personal radicado en territorio nacional, con la finalidad de atender diligentemente cualquier requerimiento de información que realice la Comisión, de conformidad con las disposiciones legales vigentes.

Las instituciones deberán habilitar credenciales de acceso irrestricto a todas las aplicaciones y objetos de sus sistemas, con derechos de lectura, en los ambientes de producción y desarrollo, al personal de la Comisión debidamente acreditado para ejecutar las labores de supervisión, en cualquier momento que ésta lo requiera. Estos accesos también serán extensivos a los archivos maestros, transaccionales e históricos que la Comisión requiera.

CAPÍTULO V
GESTION DE SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 18.- GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN

El gobierno de seguridad de la información ejercido por el Directorio y los principales ejecutivos de la institución debe abarcar la estructura organizacional y los procesos requeridos con los siguientes objetivos: a) proporcionar dirección estratégica; b) asegurar que se logren los objetivos de negocio; c) determinar que el riesgo se gestione adecuadamente; y, d) garantizar que la información independientemente de su formato y contenedor cumpla con las tres (3) características principales de seguridad que son confidencialidad, integridad y disponibilidad.

ARTÍCULO 19.- ALINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON EL PLAN ESTRATÉGICO INSTITUCIONAL

La institución debe elaborar un Plan de Seguridad de la Información, en el que se definan las iniciativas de seguridad alineadas con las metas del negocio, sus planes y operaciones,

para lo cual debe contar con la identificación de los objetivos a corto, mediano y largo plazo de las actividades y proyectos a ejecutar.

ARTÍCULO 20.- ORGANIZACIÓN DEL ÁREA ENCARGADA DE LA SEGURIDAD DE LA INFORMACIÓN

Dentro de la estructura organizacional de las instituciones supervisadas debe existir un área encargada de la gestión de la seguridad de la información. La ubicación jerárquica del área debe garantizar independencia funcional y operativa del área de TI, del resto de las áreas usuarias y de la función de auditoría.

Asimismo, el área debe estar a cargo de un ejecutivo especializado, quien debe gestionar el diseño, implementación, monitoreo y actualización del Marco de Seguridad de la Información establecido por el Directorio. Este ejecutivo debe contar con formación académica y experiencia comprobada sobre la administración de Tecnologías de Información y Comunicaciones.

ARTÍCULO 21.- FUNCIONES Y RESPONSABILIDADES DEL ÁREA ENCARGADA DE LA SEGURIDAD DE LA INFORMACIÓN

El área encargada de la gestión de la seguridad de la información tendrá al menos las siguientes funciones:

a) Diseñar, implementar, documentar, monitorear y actualizar las políticas, normas y procedimientos según los estándares internacionales y las mejores prácticas en materia de seguridad de la información, aprobadas por el Directorio;
b) Velar por la seguridad de la información, en cualquiera de sus formatos o contenedores, realizando análisis de riesgo de los diferentes procesos de la Institución, así como de los recursos tecnológicos y humanos que intervienen en los mismos;
c) Identificar e implementar controles de seguridad que garanticen que la información y la infraestructura tecnológica de la institución no sean utilizadas en perjuicio de la misma institución, instituciones externas y los usuarios;
d) Velar por la protección de los sistemas de información ante nuevas amenazas y vulnerabilidades existentes, garantizando la confidencialidad, integridad y disponibilidad de la información, y la continuidad de las operaciones;
e) Desarrollar actividades de concientización y entrenamiento en seguridad de la información;
f) Desarrollar al menos una vez al año, evaluaciones de seguridad de la información a los procesos, tecnológicos y operativos, que soporta la institución. Los resultados de estas revisiones deberán ser de conocimiento del Comité de Riesgos;
g) Mantener comunicación con los miembros de seguridad de la información de otras instituciones supervisadas con la finalidad de trabajar en conjunto para fortalecer la seguridad del Sistema Supervisado;
h) Coordinar y ejecutar la realización de análisis y de pruebas de intrusión y vulnerabilidad en el entorno tecnológico de la institución;
i) Establecer los lineamientos y estándares para controlar el acceso a los sistemas de información y la modificación de privilegios o perfiles de los usuarios;

j) Participar en el mantenimiento y actualización de los planes de contingencia, planes de continuidad del negocio y planes de recuperación de desastre para mantener el nivel de seguridad durante las actividades de recuperación;
k) Monitorear y evaluar los incidentes de seguridad de la información y recomendar acciones apropiadas; y,
l) Notificar a la Comisión en caso de incidentes o problemas de seguridad de la información en la institución supervisada.

ARTÍCULO 22.- MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La institución supervisada debe diseñar, implementar, documentar, monitorear y actualizar un Marco de Gestión de la Seguridad de la Información, el cual incluir la definición de una política de seguridad de la información y la implementación de una metodología de gestión de riesgos de TI consistente con la gestión de riesgo operativo. Además, deben considerar los activos de información de la institución supervisada, sus grupos de interés, proveedores, operadores de telecomunicaciones, entes de supervisión y vigilancia, y otras entidades vinculadas directa o indirectamente. Lo anterior, debe estar alineado con el perfil de riesgo institucional.

ARTÍCULO 23.- POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

La institución debe establecer y mantener políticas y procedimientos de seguridad de la información, cuyo contenido incluya al menos:

1. Política Institucional de Seguridad de la Información.
2. Políticas específicas sobre:
   a. Clasificación de la Información.
   b. Control de acceso a los activos de información.
   c. Uso seguro y adecuado de los activos de información.
   d. Manejo de contraseñas.
   e. Desarrollo de aplicaciones seguras.
   f. Seguridad física y ambiental.
   g. Respaldo y recuperación de información.
   h. Proceso antimalware.
   i. Relación con proveedores o terceros.
   j. Gestión de incidentes.
   k. Prestación de productos y servicios financieros a sus clientes.
   l. Uso de dispositivos móviles.
3. Procedimientos de implementación de las políticas de seguridad específicas.
4. Manual de sanciones por incumplimiento.

ARTÍCULO 24.- CONTROLES MÍNIMOS A IMPLEMENTAR PARA LA SEGURIDAD DE LA INFORMACIÓN

Como parte de la gestión de la seguridad de la información, las instituciones supervisadas basadas en un análisis de riesgos, deben implementar controles para la seguridad de la

información considerando al menos las áreas generales contenidas en el Anexo No. 2 de las presentes Normas.

ARTÍCULO 25.- EDUCACIÓN Y CONCIENTIZACIÓN EN TEMAS DE SEGURIDAD DE LA INFORMACIÓN

Todos los empleados de la institución supervisada, y cuando sea relevante los usuarios de terceras partes, deben recibir un entrenamiento apropiado y actualizaciones periódicas sobre la importancia de la seguridad de la información y del cumplimiento del Marco de Gestión de Seguridad de la Información. Esto incluye requerimientos de seguridad, responsabilidades legales y controles del negocio, así como también entrenamiento en el uso correcto de los activos para el procesamiento de información.

ARTÍCULO 26.- REVISIONES DE TERCEROS

Las instituciones supervisadas deben realizar al menos una vez al año, o cuando ocurran cambios significativos en el ambiente operativo/tecnológico, evaluaciones de seguridad a la plataforma tecnológica y pruebas de intrusión, por entes externos. El alcance de estas evaluaciones debe definirse en base a un análisis de riesgos y considerando el perfil de riesgo de los procesos a revisar.

CAPÍTULO VI
DE LA AUDITORIA INTERNA DE SISTEMAS Y REVISIONES EXTERNAS

ARTÍCULO 27.- ORGANIZACIÓN DEL ÁREA O FUNCIÓN ENCARGADA DE AUDITORIA DE SISTEMAS

Dentro de la estructura organizacional de las instituciones supervisadas debe existir la función encargada de la gestión de las auditorias de sistemas, la cual debe estar adscrita al área de auditoría interna de la institución supervisada. Sin embargo, de acuerdo al tamaño y complejidad de la institución supervisada, la Comisión podrá requerir la creación de una unidad especializada en auditoría de sistemas en las instituciones que a su criterio resulten complejas, y cuando se observe en el ejercicio de las acciones de supervisión que no se cumple con los criterios previstos en la normativa vigente.

Asimismo, esta área debe contar con planes operativos para la vigilancia de las operaciones que procuren la consecución de los objetivos organizacionales.

No obstante lo anterior, las instituciones supervisadas podrán optar por tercerizar la función de auditoria de sistemas. En ese caso, la firma auditora contratada deberá cumplir con lo establecido en el Artículo 28 de las presentes Normas.

ARTICULO 28.- AUDITORIA EN BASE A RIESGOS

La institución supervisada es responsable de desarrollar e implementar una estrategia de auditoría de TI basada en riesgos, de conformidad con el manual interno de auditoria y estándares de auditoría de TI, para garantizar una correcta asignación de recursos en las revisiones a los aspectos que de acuerdo a un análisis de riesgos, presentan una mayor exposición.

La planificación anual de auditoria de sistemas, debe incluir los riesgos potenciales en la administración de las Tecnologías de Información y Comunicaciones, incluyendo al menos los factores siguientes:

a) Los usuarios externos e internos del sistema de información.
b) El ambiente del sistema, la operatividad del sistema y sus implicaciones sobre el negocio.
c) Los niveles de acceso y la sensibilidad de la información.
d) La calidad de la información administrada por los sistemas de información, así como la calidad de la información remitida a la Comisión.
e) La Tercerización (outsourcing).
f) El ambiente de control de los procesos críticos definidos por la institución.
g) Planes de contingencia y recuperación ante desastres.
h) La efectividad del proceso de gestión de riesgo tecnológico implementado por la Institución.

La institución debe proveerle a la función de auditoria de sistemas las herramientas necesarias para la realización de las revisiones al ambiente de control relacionado a las tecnologías de información y comunicaciones.

En el caso de instituciones miembros de Grupos Financieros internacionales y cuya función de auditoria de sistemas este a cargo de la casa matriz, el plan de auditoria de sistemas debe considerar los riesgos particulares del país.

ARTÍCULO 29.- REVISIONES DE TERCEROS

Sin perjuicio de lo establecido en los Artículos 27 y 28 de las presentes Normas, las instituciones supervisadas deben realizar al menos una vez al año, auditorias de sistemas por entes externos. El alcance de estas revisiones debe definirse en base a un análisis de riesgos y considerando el perfil de riesgo de los procesos a auditar.

CAPÍTULO VII
GESTION DE CONTINUIDAD DE LAS OPERACIONES DE TECNOLOGIA

ARTÍCULO 30.- GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Tal como se establece en la Norma de Gestión de Riesgo Operativo, las instituciones supervisadas deben realizar una gestión de la continuidad de las operaciones de tecnología adecuada a su tamaño y la complejidad de sus operaciones y servicios.

ARTÍCULO 31.- FASES DE LA CONTINUIDAD DE LAS OPERACIONES DE TECNOLOGÍA

La institución supervisada debe desarrollar al menos las siguientes fases como parte de la gestión de continuidad de las operaciones de tecnología:

1. Evaluación y análisis de riesgos.
2. Análisis de impacto del negocio (BIA).
3. Desarrollo de estrategias de recuperación.
4. Desarrollo de planes.
5. Pruebas y ejercicios.
6. Concientización y capacitación.

7. Mantenimiento y actualización.

La ejecución de cada una de estas fases debe ser documentada y aprobada por el Directorio de la institución supervisada.

ARTÍCULO 32.- EVALUACIÓN Y ANÁLISIS DE RIESGOS

La institución supervisada debe identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deber aplicar una metodología consistente con aquella utilizada para la evaluación de los riesgos operativos que enfrenta la institución.

Los resultados de la evaluación mencionada y sus actualizaciones periódicas deben ser formalmente reportados a la Alta Gerencia, que es el responsable de gestionar que las debilidades que expongan a la institución supervisada a niveles de riesgo alto o inaceptable sean corregidas a niveles aceptables. Estos resultados deberán ser de conocimiento del Directorio.

ARTÍCULO 33.- ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)

La institución supervisada debe determinar el impacto que tendría una interrupción de los procesos que soportan sus principales productos y servicios. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera de la institución, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según el impacto determinado debe establecerse el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO) para cada proceso de negocio, así como los recursos necesarios para su cumplimiento.

ARTÍCULO 34.- DESARROLLO DE ESTRATEGIAS DE RECUPERACIÓN

La institución supervisada debe determinar las estrategias de continuidad que permitirán mantener las actividades y procesos de negocio luego de ocurrida una interrupción en las operaciones, considerando entre otras opciones: acciones diferidas, procedimientos manuales, soluciones internas, degradación de servicios, acuerdos recíprocos y servicios comerciales de recuperación. Las estrategias de recuperación deben ser aprobadas por el Directorio y deben estar basadas en un análisis costo/beneficio de las estrategias identificadas y el cumplimiento del tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO) definido para cada proceso.

ARTÍCULO 35.- DESARROLLO DEL PLAN DE CONTINUIDAD

El plan de continuidad de negocio como lo establece la Norma de Riesgo Operativo, además de los planes de respuesta de emergencia y comunicación de crisis, debe contener un plan de continuidad de operaciones de tecnología, o también conocido como Plan de Recuperación de Desastres (DRP), cuyo objetivo es restaurar los servicios de TI dentro de los parámetros establecidos, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.

ARTÍCULO 36.- ESTRATEGIAS DE CONTINUIDAD RESPECTO AL PROCESAMIENTO DE DATOS

Las instituciones supervisadas deben implementar estrategias de continuidad respecto al procesamiento de datos en caso de contingencia, mediante la cual puedan dar continuidad a las operaciones y los procesos críticos de negocio.

En caso que las instituciones supervisadas opten por un centro de procesamiento de datos alterno ubicado fuera del territorio hondureño, las instituciones deberán permitir a la Comisión el libre acceso a su infraestructura de TI, sistemas de información y bases de datos, y proporcionar a ésta la información que les requiera. Asimismo, deberán observar lo estipulado en el Artículo 15 de las presentes Normas.

ARTÍCULO 37.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN

Las instituciones supervisadas deben establecer en base a su análisis de riesgos, procedimientos de respaldo y recuperación que incluyan aspectos como: las rutinas de respaldo, duración, frecuencia, medio y, controles de acceso, transporte, resguardo y destrucción.

Estos procedimientos deben ser probados periódicamente para garantizar que se reasuma el procesamiento normal de la información en caso de una interrupción a corto plazo o si hay necesidad de procesar o de reiniciar un proceso.

Las instituciones obligatoriamente deben realizar respaldos al cierre contable mensual y al cierre contable anual.

ARTÍCULO 38.- MANEJO DE INCIDENCIAS DE CONTINUIDAD

Las instituciones supervisadas deben establecer mecanismos y procedimientos formalmente documentados para la gestión, registro, accionar y comunicación de incidencias de continuidad en las operaciones de TI. Estos mecanismos deben permitir la identificación, análisis, resolución y documentación de errores. Estos eventos deberán ser incluidos como incidentes de riesgos operacionales y reportados a la Comisión, de acuerdo a lo establecido en la Norma de Riesgo Operativo emitida por la Comisión.

ARTÍCULO 39.- PÓLIZAS DE SEGUROS

Las instituciones supervisadas deben contar con cobertura de seguros para los principales equipos de su plataforma tecnológica para mitigar al menos los riesgos provocados por incendio y las líneas aliadas, las propias para proteger el equipo electrónico, no siendo excluyente de cualquier otra cobertura que la institución desee adicionar al seguro.

En el caso de las instituciones de seguros, dichas pólizas deberán ser contratadas con otra institución de seguros.

ARTÍCULO 40.- CUSTODIA Y UBICACIÓN DE LOS PLANES DE CONTINUIDAD FUERA DE SITIO.

La custodia del plan de continuidad de negocio debe estar a cargo del área respectiva, quien debe conservar una copia actualizada del Plan en una ubicación fuera de sitio, de modo que en caso de cualquier interrupción o contingencia en las instalaciones donde se encuentre almacenado el Plan, se tenga acceso al mismo.

CAPITULO VIII
DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 41.- SANCIONES
En caso de incumplimiento de las disposiciones contenidas en las presentes Normas, la Comisión aplicará las sanciones correspondientes, de conformidad con lo establecido en el marco legal aplicable y en el Reglamento de Sanciones vigente.

ARTÍCULO 42.- CASOS NO PREVISTOS
Los casos no previstos en la presente norma serán resueltos por la Comisión, de conformidad al marco legal y normativo vigente.

ARTÍCULO 43.- PLAZO DE ADECUACIÓN
Para efectos de adecuación a las disposiciones contenidas en la presente Norma, las instituciones deberán sujetarse a los siguientes plazos:

Programa	Plazo	Observaciones
1. Plan de acción para adecuarse a las modificaciones de la presente Norma, con su respectiva aprobación por el Directorio	Treinta (30) días hábiles contados a partir de la entrada en vigencia de la Norma.	Se deberá acompañar un plan de acción con plazo límite máximo de diez y ocho (18) meses a partir de la entrada en vigencia de la Norma, para adecuar su proceso de gestión de riesgo tecnológico a las modificaciones de la misma. El proceso de adecuación de esta norma, no exime de responsabilidad al Directorio en velar porque se gestionen los riesgos a que se expone la institución. Este plan de acción deberá incluir al menos: Fechas de inicio y finalización de las actividades, responsables de ejecución, descripción de las actividades a realizar, entre otros.
2. Informe trimestral sobre los avances en la implementación de la Norma de Gestión de Riesgo Operativo.	Diez (10) días hábiles después del cierre del trimestre.	Según Anexo No. 3, a partir del cierre del segundo trimestre del año 2019.
3. Capitulo II. Adecuación de las responsabilidades y funciones para la gestión del riesgo tecnológico.	Tres (3) meses contados a partir de la entrada en	

Programa	Plazo	Observaciones
	vigencia de la Norma.	
4. Capitulo III. Adecuación de aspectos de Gestión de las Tecnologías de Información.	Seis (6) meses contados a partir de la entrada en vigencia de la Norma.	
5. Capitulo V. Adecuación de aspectos de Gestión de la Seguridad de la Información.	Seis (6) meses contados a partir de la entrada en vigencia de la Norma.	
6. Capitulo IV. Adecuación de contratos de servicios tercerizados.	Un (1) año a partir de la entrada en vigencia de la Norma.	
7. Capítulo VI. Adecuación de aspectos de auditoria interna.	De Inmediato.	
8. Capitulo VII. Adecuación de aspectos de continuidad de operaciones.	Diez y ocho (18) meses a partir de la entrada en vigencia de la Norma.	

ARTÍCULO 44.- DEROGATORIA

A partir de la entrada en vigencia de las presentes Normas, queda sin valor y efecto la Resolución No. 1301/22-11-2005, contentiva de las “Normas para Regular la Administración de las Tecnologías de Información y Comunicaciones en las Instituciones del Sistema Financiero”, así como las Resoluciones Nos. 566/24-07-2001 y GE No. 266/21-02-2012, y cualquier otra disposición que se oponga a las presentes Normas.

ARTÍCULO 45.- VIGENCIA

Las presentes Normas entrarán en vigencia a partir de la fecha de su publicación en el Diario Oficial “La Gaceta”.