Tegucigalpa, MDC
19 de diciembre de 2022

INSTITUCIONES SUPERVISADAS
Toda la República

CIRCULAR CNBS No.025/2022

Señores:

La infrascrita Secretaria General de la Comisión Nacional de Bancos y Seguros CERTIFICA la parte conducente del Acta de la Sesión No.1689 celebrada en Tegucigalpa, Municipio del Distrito Central el dieciséis de diciembre de dos mil veintidós, con la asistencia de los Comisionados MARCIO GIOVANNY SIERRA DISCUA, Presidente; ESDRAS JOSIEL SÁNCHEZ BARAHONA, Comisionado Propietario; ALEX ROBERTO LARA ENAMORADO, Superintendente de Seguros, designado por el Presidente para integrar la Comisión en calidad de Comisionado Suplente por disposición del Artículo 2 de la Ley de la Comisión Nacional de Bancos y Seguros; ANA GABRIELA AGUILAR PINEDA, Secretaria General; que dice:

"… **2. Asuntos de la Gerencia de Regulación, Investigación y Desarrollo:** … literal **a)** … **RESOLUCIÓN GRD No.793/16-12-2022.-** La Comisión Nacional de Bancos y Seguros,

CONSIDERANDO (1): Que de conformidad con lo dispuesto en el Artículo 13, numerales 1) y 2) de la Ley de la Comisión Nacional de Bancos y Seguros, corresponde a este Ente Supervisor dictar las normas prudenciales que se requieran para la revisión, verificación, control, vigilancia y fiscalización de las Instituciones Supervisadas, para lo cual se basará en la legislación vigente, en acuerdos y prácticas internacionales.

CONSIDERANDO (2): Que la Comisión Nacional de Bancos y Seguros (CNBS), mediante Resolución No.1301/22-11-2005, aprobó las "NORMAS PARA REGULAR LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO", las cuales tienen por objeto regular la administración de las tecnologías de información y comunicaciones utilizadas por las instituciones del sistema financiero; asimismo, regular los servicios financieros y operaciones realizadas por medio de redes electrónicas de uso externo e interno. La Junta Directiva o Consejo de Administración de las instituciones del sistema financiero, deben prestar la debida importancia a la administración del riesgo derivado de los sistemas de información, tomando en cuenta que su continuidad, desarrollo y funcionamiento constituyen el elemento central para su operatividad y su manejo administrativo y financiero.

CONSIDERANDO (3): Que la Comisión Nacional de Bancos y Seguros mediante Resolución GES No.662/29-12-2020, aprobó el Marco Integral de Supervisión Basada en Riesgos (MISBR) para el Sector Financiero, Asegurador y Previsional Público, con el objetivo de establecer un enfoque de

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

Supervisión dinámico y prospectivo que permita identificar oportunamente los eventos actuales y potenciales, que puedan afectar el perfil de riesgos de las Instituciones Supervisados.

CONSIDERANDO (4): Que los estándares y mejores prácticas internacionales relacionados con las Tecnologías de Información (TI), están en constante actualización brindando mecanismos de control robustos para la gestión de las TI.

CONSIDERANDO (5): Que conforme con lo descrito en los Considerandos (3) y (4) precedentes, la Comisión Nacional de Bancos y Seguros (CNBS) considera procedente reformar las disposiciones contenidas en las "NORMAS PARA REGULAR LA ADMINISTRACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LAS INSTITUCIONES DEL SISTEMA FINANCIERO", relacionadas con la gestión de tecnologías de información, la continuidad del negocio, seguridad de la información y ciberseguridad en las Instituciones Supervisadas, dada la rápida evolución de las tecnologías de la información en las últimas décadas y el aumento considerable en su uso por parte de las Instituciones Supervisadas y los usuarios financieros, adaptándolas a mejores estándares y prácticas internacionales.

CONSIDERANDO (6): Que en cumplimiento a lo dispuesto en el Artículo 39 de la Ley de la Comisión Nacional de Bancos y Seguros, del 9 al 24 de mayo de 2022, este Ente Supervisor publicó en su página de web, en la sección de "Proyectos de Normativa", el Proyecto de reformas de las "NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO", con el propósito de recibir comentarios y observaciones del público en general, de las Instituciones Supervisadas.

POR TANTO: Con fundamento en lo establecido en los Artículos 1, 6, 13 numerales 1) y 2) y 39 de la Ley de la Comisión Nacional de Bancos y Seguros; Normas para Regular la Administración de las Tecnologías de Información y Comunicaciones en las Instituciones del Sistema Financiero, aprobadas mediante Resolución No.1301/22-11-2005;

RESUELVE:

1. Reformar las "Normas para Regular la Administración de las Tecnologías de Información y Comunicaciones en las Instituciones del Sistema Financiero", aprobadas por la Comisión Nacional de Bancos y Seguros mediante Resolución No.1301/22-11-2005, cuyo contenido íntegramente se leerá así:

"NORMAS PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, CIBERSEGURIDAD Y CONTINUIDAD DEL NEGOCIO"

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- OBJETO
Las presentes Normas tiene por objeto regular la gestión de tecnologías de información, continuidad del negocio, seguridad de la información y ciberseguridad en las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros (CNBS), así como a los Grupos

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

Financieros de los cuales éstas formen parte, en función de su tamaño, naturaleza, complejidad de operaciones y perfil de riesgos.

ARTÍCULO 2.- ALCANCE
Las presentes Normas son aplicables a las Instituciones Supervisadas por la Comisión, así como a los Grupos Financieros conformados por estas.

ARTÍCULO 3.- DEFINICIONES
Para efectos de las presentes Normas, se entenderá por:

1. **Acuerdos de Nivel de Servicio (SLA, por sus siglas en inglés):** Convenio entre el área de Tecnologías de Información 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, tales como exactitud, integridad, puntualidad, disponibilidad y seguridad;

2. **Alta Gerencia:** Grupo de personas responsables de la gestión diaria, sólida y prudente de la Institución Supervisada ante la Junta Directiva, Consejo de Administración u órgano equivalente;

3. **Análisis de Impacto del Negocio (BIA, por sus siglas en inglés):** Etapa de la planeación de continuidad de negocio en la que se identifican los sucesos que podrían tener un impacto sobre la continuidad de las operaciones y su impacto financiero, humano y de reputación sobre la Institución Supervisada;

4. **Apetito de Riesgo:** Nivel agregado y los tipos de riesgo que una Institución Supervisada está dispuesta a asumir dentro de su capacidad de riesgo para lograr sus objetivos estratégicos y plan de negocios. También puede entenderse, como la cantidad de riesgo que una Institución Supervisada decide tomar dentro de su capacidad de riesgo;

5. **Capacidad de Riesgo:** Nivel máximo de riesgo que una Institución Supervisada puede asumir dado su nivel actual de recursos antes de exceder las restricciones determinadas por el capital reglamentario y las necesidades de liquidez, el ambiente operativo como ser la infraestructura técnica, capacidad para la gestión de riesgo y su conocimiento experto;

6. **Ciberamenaza:** Circunstancia que podría explotar una o más vulnerabilidades y afectar la ciberseguridad;

7. **Ciberespacio:** Es el ambiente complejo que resulta de la interacción de personas, software, y servicios en internet por medio de dispositivos y redes conectadas. No posee existencia física, sino que es un dominio virtual que engloba todos los sistemas;

8. **Ciberresiliencia:** Capacidad de la Institución Supervisada de continuar llevando a cabo su misión, anticipándose, adaptándose a ciberamenazas y otros cambios relevantes en el entorno; y, resistiendo, conteniendo y recuperándose rápidamente de incidentes de ciberseguridad;

9. **Ciberseguridad:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas de información a través del ciberespacio;

10. **Comisión o CNBS:** Comisión Nacional de Bancos y Seguros;

11. **Confidencialidad:** Característica que consiste en que la información sea accesible para quienes están autorizados;

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

13. **Funciones de Vigilancia:** Son las encargadas de brindar vigilancia integral e independiente a nivel institucional, así como el control y monitoreo, de la gestión operativa, como ser: Auditoría Interna, Gestión de Riesgo, Análisis Actuarial, Análisis Financiero, Cumplimiento Regulatorio, Alta Gerencia, Consejo de Administración, Junta Directiva o su equivalente, entre otras según la naturaleza, tamaño, alcance, complejidad y perfil de riesgo de la Institución Supervisada;

14. **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;

15. **Grupos de Interés:** Involucra todos los ámbitos y personas sobre los cuales tiene influencia la Institución Supervisada o Grupo Financiero, tales como: accionistas, funcionarios o ejecutivos y empleados, usuarios, competidores, órganos reguladores de control y fiscalización, comunidad y los proveedores de bienes y servicios según corresponda;

16. **Grupo Financiero:** El constituido por una o más instituciones del sistema financiero. Además podrá estar integrado por una o más de las instituciones siguientes: casas de cambio, almacenes generales de depósito, instituciones de seguros, de reaseguros, emisoras y/o administradoras de tarjetas de crédito, arrendadoras, casas de bolsa, depósitos centralizados de custodia, mecanismos de compensación y liquidación de valores, sociedades administradoras de fondos, remesadoras, sociedades administradoras de fondos mutuos, sociedades dedicadas al descuento de documentos y otras con propósitos y actividades financieras similares;

17. **Incidente:** Es la ocurrencia de un suceso que afecta adversamente el desarrollo normal de las operaciones de la Institución Supervisada;

18. **Incidente de Seguridad de la Información:** Ocurrencia de un suceso que constituye una violación o amenaza de las políticas y los procedimientos de seguridad de la Institución Supervisada, y afecta adversamente la confidencialidad, integridad y/o disponibilidad de la información independientemente de su formato y contenedor;

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

19. **Infraestructura de TI:** Conjunto de hardware, software, redes, instalaciones y otros elementos que se requieren para desarrollar, probar, entregar, monitorear, controlar o dar soporte a los servicios de TI. La infraestructura de TI excluye al recurso humano, los procesos y la documentación;

20. **Integridad:** Característica que consiste en que la información esté exacta y completa, y que solo puede ser creada, modificada o eliminada por quien esté autorizado para hacerlo;

21. **Líneas de Defensa:** Áreas o funciones organizacionales que contribuyen a la gestión y control de los riesgos de las Instituciones Supervisadas. Estas se dividen en tres: **a) Primera Línea de Defensa:** Es responsable de la gestión diaria de los riesgos, enfocada en identificar, evaluar y reportar cada exposición, en consideración del apetito de riesgo aprobado y sus políticas, procedimientos y controles. Generalmente se asocia a las líneas de negocio o a las actividades significativas de la Institución Supervisada. Las líneas de negocios o gestión operativa tienen la propiedad sobre el riesgo asumido, por lo que debe reconocerlo y gestionarlo en el ejercicio de sus actividades; **b) Segunda Línea de Defensa:** Complementa a la primera línea de defensa a través del seguimiento y reporte a las autoridades respectivas. Generalmente incluye la función de gestión de riesgo, la función de cumplimiento regulatorio, incluyendo lo referente a la prevención de lavado de activos y financiamiento del terrorismo u otras funciones de vigilancia de acuerdo con lo establecido por la Comisión; y, **c) Tercera Línea de Defensa:** consiste en la función de una Auditoría Interna independiente y efectiva, que proporcione a la Junta Directiva, Consejo de Administración o su equivalente, información sobre la calidad del proceso de gestión del riesgo. Además, es la encargada de efectuar revisiones generales y basadas en el riesgo para garantizar a estos, que el Marco de Gobierno Corporativo;

22. **Marco de Gobierno de Riesgo:** Componente del marco de gobierno corporativo, a través del cual la Junta Directiva, Consejo de Administración o su equivalente, la Alta Gerencia establecen, toman decisiones sobre la estrategia, la metodología de riesgo, articulan, monitorean la observancia del apetito, límites de riesgo según su estrategia, así como su identificación, medición, gestión y control de los riesgos;

23. **Órgano de Administración:** Se refiere a la Junta Directiva, Consejo de Administración Asamblea de Participantes o Aportantes, o su órgano equivalente;

24. **Perfil de Riesgos:** Evaluación de las exposiciones de riesgo de la Institución Supervisada, después de tomar en cuenta los mitigantes;

25. **Procesamiento de Datos**: Es el proceso de almacenamiento y transformación de datos con el objetivo de obtener información para la Institución Supervisada;

26. **Procesamiento de Datos Significativo:** Es el proceso de almacenamiento y transformación de datos de carácter vital, con el objetivo de obtener información; y que en caso de ser afectado provocarían un impacto significativo en la continuidad del negocio o reputación de la institución;

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

27. **Proveedor de Servicios de TI:** Persona natural o jurídica que provee o presta un servicio relacionado con la tecnología de información, operando en territorio nacional o fuera de él sea independiente o que pertenezca al mismo Grupo o Conglomerado Financiero, incluyendo las casas matrices;

28. **Punto Objetivo de Recuperación (RPO, por sus siglas en inglés):** Volumen de datos en riesgo de pérdida que la Institución Supervisada considera tolerable en caso de una interrupción en sus operaciones, de acuerdo con al apetito de riesgo definido por la Institución Supervisada;

29. **Resiliencia**: Capacidad del personal, los sistemas, redes, actividades o procesos de una Institución para resistir, absorber y recuperarse o adaptarse rápidamente de un incidente;

30. **Riesgo Tecnológico (RT):** Es una subdivisión del Riesgo Operativo y se evalúa en dicha categoría de riesgo. Surge de la potencial pérdida por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal digital de distribución de información;

31. **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, servicios, entre otros) que pueden ser suministrados y liberados rápidamente por el proveedor de servicios;

32. **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;

33. **Tercerización:** Subcontratar los trabajos o servicios con terceros;

34. **Tercerización Significativa:** Tercerización de servicios que son de carácter vital para una Institución Supervisada, ya que si fallan provocarían un impacto en la continuidad del negocio; y,

35. **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 suceso de interrupción de operaciones. Es menor al periodo de tiempo luego del cual la viabilidad de la Institución Supervisada sería afectada seriamente, si un producto o servicio en particular no es reanudado.

CAPÍTULO II
DE LA GESTIÓN DE LOS RIESGOS ASOCIADOS CON TECNOLOGÍAS DE INFORMACIÓN

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

ARTÍCULO 4.- GESTIÓN DE LOS RIESGOS ASOCIADOS CON TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas deben garantizar que su Marco de Gobierno de Riesgo, contemplen lo relacionado con las TI como un proceso institucional, transversal, coherente con los objetivos estratégicos y el plan de negocios de la Institución o del Grupo Financiero.

La gestión de riesgos asociados con TI debe incluir al menos lo siguiente:

a. Declaración de apetito de riesgo;

b. Estrategia de gestión de riesgo;

c. Políticas, procedimientos, controles y herramientas para la gestión de riesgo tecnológico; que soporten los roles, responsabilidades y estructura formal de reporte, conforme a las operaciones de la institución;

d. Función de gestión de riesgos tecnológicos; y,

e. Procesos de revisión para asegurar que el Marco de Gobierno de Riesgo continúa siendo eficaz; de manera que se identifiquen y pongan en práctica modificaciones o mejoras de forma oportuna.

CAPÍTULO III
DEL GOBIERNO Y LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ARTÍCULO 5.- GOBIERNO DE TI
El Gobierno de TI como parte integral del Gobierno Corporativo, debe establecer la estructura, políticas y procesos garantizando que las TI soportan las estrategias y objetivos de la Institución, y el cual debe considerar al menos los siguientes aspectos:

a. **Alineación Estratégica:** Elaborar e implementar un Plan Estratégico de TI, aprobado por el Órgano de Administración, en el que se defina la estrategia de TI y sus objetivos estratégicos, alineados con la estrategia institucional, 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 TI asegurándose que genere los beneficios financieros y no financieros esperados y proyectados en el Plan Estratégico Institucional, mediante servicios y soluciones efectivas;

c. **Administración de Recursos:** Administrar de forma óptima y efectiva los recursos para ejecutar el Plan Estratégico de TI, tales como el recurso humano, financiero, infraestructura de TI e información, asegurando el desarrollo y monitoreo para la administración de dichos recursos;

d. **Gestión de Riesgos Asociados con TI:** Identificar, evaluar, mitigar, monitorear y

comunicar los riesgos asociados con TI, alineado al Marco de Gobierno de Riesgo definido por la Institución Supervisada; y,

e. **Medición del Desempeño de TI**: Dar seguimiento permanente y efectivo, por parte de la Gerencia General o su equivalente y el Órgano de Administración a través de la unidad que éste defina, a la implementación de la estrategia de TI mediante la revisión continua y reportes del desempeño de los procesos y el logro de sus objetivos y metas, así como a la terminación de sus proyectos, uso de los recursos y entrega del servicio.

ARTICULO 6.- GOBIERNO DE TI EN GRUPOS FINANCIEROS
Cuando la Institución Supervisada que forme parte de un Grupo Financiero, puede establecer las funciones o comités para la gestión operativa y las funciones de vigilancia relacionadas con TI a nivel de grupo. Asimismo, las funciones o comités que opten por esta opción deben asegurar que se realice de forma efectiva en cada una de las Instituciones que formen parte del Grupo Financiero.

Los comités deben estar integrados por ejecutivos de cada una de las Instituciones que forman parte del Grupo Financiero; lo que debe establecerse en los reglamentos aprobados por el Órgano de Administración.

ARTÍCULO 7.- GESTIÓN DE TI
Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar el Marco de Gestión de TI, el cual debe estar conformado por políticas, procesos y procedimientos relacionados con la adquisición, mantenimiento e implementación de los sistemas, bases de datos e infraestructura de TI, así como la administración de recursos, garantizando que toda tarea o proceso interno de TI esté debidamente documentado, con el objetivo de lograr un entorno operativo que tenga un nivel adecuado de madurez. De igual forma, definir los roles, funciones y responsabilidades de la Alta Gerencia y las Funciones de Vigilancia con respecto a dicha gestión.

El Marco de Gestión de TI debe revisarse y/o actualizarse de acuerdo con la periodicidad definida por la Institución o Grupo Financiero o ante el surgimiento de cambios significativos, de manera tal que asegure su actualización, vigencia y efectividad.

ARTÍCULO 8.- ORGANIZACIÓN DEL ÁREA DE TI
El área de TI, debe gestionar los riesgos materiales a las tecnologías de la información como primera línea de defensa; además, dicha área debe contar con la estructura organizacional alineada con el Plan Estratégico de TI, con adecuada separación de funciones, delegación de autoridad, definición de roles y asignación de responsabilidades; asegurándose que el recurso humano tenga las capacidades necesarias mediante programas de entrenamiento y capacitación, así como, estrategias de promoción y transferencia de conocimiento entre los mismos.

Asimismo, el área de TI debe estar a cargo de un ejecutivo especializado con formación académica y experiencia comprobada sobre la administración de TI.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

ARTÍCULO 9.- CAMBIO O ACTUALIZACIÓN DEL SISTEMA DE INFORMACIÓN PRINCIPAL
Las Instituciones Supervisadas deben notificar a la Comisión, con al menos treinta (30) días calendario de anticipación, la realización del pase a producción del sistema de información principal derivado de un cambio o actualización de este, remitiendo al menos la siguiente información:

a. Nombre y versión del sistema de información vigente;

b. Nombre y versión del sistema de información nuevo; y,

c. Cronograma de las fases de salida a producción, detallando las tareas que lo conforman. Las modificaciones al cronograma antes mencionado deben ser notificadas a la Comisión diez (10) días hábiles posteriores a su aprobación por parte del Órgano de Administración.

Lo anterior, sin perjuicio de la facultad que tiene la Comisión de solicitar la información adicional en el momento que lo estime conveniente.

Esta disposición también es aplicable para el cambio o actualización de sistemas de información relacionados con el procesamiento de tarjetas de crédito.

CAPÍTULO IV
DE LA TERCERIZACIÓN DE SERVICIOS DE TI

ARTÍCULO 10.- GESTIÓN DE PROVEEDORES DE TI
Las Instituciones Supervisadas deben realizar la gestión con los proveedores de servicios de TI en función de la criticidad y los riesgos asociados. La gestión de proveedores debe tomar en consideración si el servicio tercerizado se ejecutará en el sitio, fuera del sitio o países extranjeros, incluyendo la medición de desempeño, requisitos fiscales, legales, regulatorios, continuidad de operaciones, recurso humano y gestión de incidentes de seguridad, así como el cumplimiento de la confidencialidad, integridad y disponibilidad de la información en los casos que aplique.

ARTÍCULO 11.- RESPONSABILIDAD DE TERCERIZACIÓN DE SERVICIOS
Las Instituciones Supervisadas son responsables de establecer y velar por las medidas de control y seguimiento de los servicios tercerizados relacionados con el uso y monitoreo de las TI, de manera que se ejecuten con base en las mejores prácticas, requisitos legales y regulatorios, minimizando riesgos objeto de la tercerización de servicios de TI; además, se debe asegurar que el procesamiento y la información derivado de la tercerización en todo momento se encuentre aislada lógicamente del resto de las operaciones del proveedor de servicios de TI.

ARTÍCULO 12.- DILIGENCIA SOBRE EL PROVEEDOR DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas deben establecer acciones de diligencia para la selección, evaluación de rendimiento, gestión de contratos y riesgos de los proveedores de servicios de

TI, analizando al menos la viabilidad técnica, financiera y legal del proveedor, de modo que ninguno de los aspectos anteriores afecte la prestación del servicio en el futuro.

ARTÍCULO 13.- TERCERIZACIÓN SIGNIFICATIVA DE TI
Se considera tercerización significativa la función de auditoría de sistemas, gestión de seguridad de la información, gestión de riesgo tecnológico, la infraestructura de TI, y las identificadas por la Comisión o la propia Institución.

La tercerización significativa de TI debe ser notificada a esta Comisión, treinta (30) días calendario previos a la suscripción del contrato. La Comisión podrá requerir información adicional necesaria para su análisis.

ARTÍCULO 14.- TERCERIZACIÓN SIGNIFICATIVA DE PROCESAMIENTO DE DATOS
Los servicios de procesamientos de datos objeto de tercerización significativa deben ser sometidos periódicamente a un examen de auditoría independiente del proveedor, realizada por entes especializados y de conformidad con las mejores prácticas internacionales; asimismo, el resultado debe ser comunicado a las funciones de vigilancia que la Institución Supervisada establezca.

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

La tercerización significativa de procesamiento de datos debe ser notificada a la Comisión, treinta (30) días calendario previos a la suscripción del contrato. Asimismo, una vez contratado este servicio, la Institución Supervisada debe contar con la información requerida en el Anexo No.1 de las presentes Normas, misma que debe estar a disposición de la Comisión cuando sea requerida.

ARTÍCULO 15.- SERVICIOS BASADOS EN LA NUBE
Las Instituciones Supervisadas podrán optar por tercerizar sus servicios con un esquema en la nube, considerando las condiciones contractuales que les permitan gestionar efectivamente los riesgos asociados, y contemplando, entre otros factores, el tipo de nube contratada, el proveedor de servicios, los sitios de procesamiento, los servicios contratados, el tipo de información a procesar, los controles de seguridad para la protección de los datos en ambientes virtualizados y la protección de las aplicaciones de la Institución.

ARTÍCULO 16.- CONTRATOS DE TERCERIZACIÓN DE SERVICIOS TECNOLÓGICOS
Las Instituciones Supervisadas deben establecer una efectiva gestión de sus contratos, considerando al menos los aspectos siguientes:

a. Facultades suficientes para que la actividad del proveedor de servicios para la institución

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

pueda ser auditada por la institución contratante y por la Comisión respecto de los servicios tercerizados;

b. Facultades para que la Institución Supervisada pueda obtener la base de datos, los programas fuentes, manuales y documentación técnica de los sistemas de información, ante cualquier situación adversa que pudiera sufrir el proveedor, en el cual afecte la prestación de servicios. La Comisión en el uso de sus facultades puede solicitar cualquier información relacionada con dichos contratos y la tercerización de servicios tecnológicos;

c. Determinación de SLA según las necesidades de la Institución;

d. Obligatoriedad para el proveedor de servicios, en cuanto al establecimiento de controles de seguridad de la información y los riesgos asociados con relación a la tercerización del servicio; y,

e. Obligatoriedad para el proveedor de servicios, en el cual, se establezcan disposiciones relacionadas con la continuidad de negocio y recuperación de desastre.

Sin perjuicio de lo anterior, la Institución debe incluir los aspectos que consideren pertinentes para la gestión efectiva de contratos y proveedores que permitan el desarrollo y cumplimiento apropiado de la tercerización de servicios contratados.

CAPÍTULO V
DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

ARTÍCULO 17.- GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD
El gobierno de seguridad de la información y ciberseguridad, ejercido por el Órgano de Administración y la Alta Gerencia, debe comprender transversalmente la estructura organizacional y los procesos de la Institución, garantizando que la información cumpla con la confidencialidad, integridad y disponibilidad, independientemente de su formato y contenedor; para ello, deben considerar al menos los siguientes aspectos:

a. **Alineación Estratégica:** Elaborar e implementar un plan de seguridad de la información y ciberseguridad, en donde se definan las estrategias e iniciativas de seguridad alineadas con las metas del negocio, planes y operaciones, para lo cual debe identificar los objetivos a corto, mediano y largo plazo de las actividades y proyectos a ejecutar;

b. **Administración de Recursos:** Optimizar las inversiones en seguridad utilizando la infraestructura y recursos con eficiencia para el logro de los objetivos del negocio;

c. **Gestión de los Riesgos:** Administrar efectivamente los riesgos de seguridad de la información y ciberseguridad, para mitigar o reducir su impacto de acuerdo con el

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

apetito y tolerancia al riesgo definido; y,

d. **Medición del Desempeño:** Implementar métricas o indicadores de desempeño que le permitan monitorear, reportar y garantizar la efectividad de este.

ARTÍCULO 18.- MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar el Marco de Gestión de la Seguridad de la Información y Ciberseguridad, el cual debe incluir al menos los siguientes aspectos:

a. La definición de las políticas, procedimientos y controles de seguridad de la información y ciberseguridad;

b. La implementación de una metodología de gestión de riesgos de seguridad de la información y ciberseguridad alineada con el Marco de Gobierno de Riesgo de la Institución;

c. La designación de una función (área o responsable) encargada de la gestión de seguridad de la información y ciberseguridad; y,

d. Un proceso de revisión y actualización para asegurar que la gestión de seguridad de la información y ciberseguridad continúa siendo eficaz, de manera que se identifiquen y pongan en práctica modificaciones o mejoras de forma oportuna. Además, debe considerar los activos de información de la Institución Supervisada, así como los vinculados con sus grupos de interés.

ARTÍCULO 19.- GESTIÓN DE LA CIBERSEGURIDAD

Como parte del Marco de Gestión de la Seguridad de la Información y Ciberseguridad, las Instituciones Supervisadas deben gestionar la ciberseguridad basado en las mejores prácticas y estándares internacionales que les permita:

a. **Identificar:** Tener plenamente identificados los sistemas de información, los activos y los datos expuestos en el ciberespacio, así como su contexto de negocio y los recursos que soportan las funciones críticas y los riesgos de ciberseguridad que afectan su entorno;

b. **Proteger:** Desarrollar e implementar los controles necesarios para limitar o contener el impacto de eventos potenciales de ciberseguridad;

c. **Detectar:** Desarrollar e implementar actividades apropiadas para identificar la ocurrencia de eventos de ciberseguridad a través del monitoreo continuo;

d. **Responder:** Contar con procesos y procedimientos para garantizar respuestas oportunas, durante y después de un incidente de ciberseguridad; y,

e. **Recuperar y Aprender:** Desarrollar e implementar actividades para la gestión de

ciberresiliencia y el retorno a la operación normal después de un incidente. Asimismo, ajustar su Marco de Gobierno de Riesgo en lo relacionado al Marco de Gestión de TI y el Marco de Gestión de la Seguridad de la Información, como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.

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

Las Instituciones Supervisadas deben tener una función encargada de la gestión de la seguridad de la información y ciberseguridad, la cual debe contar con independencia funcional y operativa respecto al área encargada de TI y del resto de las áreas usuarias. Asimismo, debe gestionar el diseño, implementación, monitoreo y actualización del Marco de Gestión Seguridad de la Información y Ciberseguridad establecido por el Órgano de Administración.

La función de gestión de la seguridad de la información y ciberseguridad debe estar a cargo de un ejecutivo especializado con formación académica y experiencia comprobada sobre la administración de TI, Seguridad de la Información y/o Ciberseguridad.

Sin perjuicio de lo anterior, las Instituciones Supervisadas podrán optar por tercerizar la función de gestión de seguridad de la información y ciberseguridad, cumpliendo con las disposiciones establecidas en las presentes Normas relacionadas con la tercerización de servicios.

ARTÍCULO 21.- GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Instituciones Supervisadas deben gestionar efectivamente los incidentes de seguridad de la información y ciberseguridad, de forma tal, que sean identificados, detectados, analizados, para proteger efectivamente los activos de información afectados e implementar las medidas correctivas necesarias que les permita continuar o restablecer sus operaciones de manera oportuna.

Asimismo, las Instituciones Supervisadas deben notificar a la Comisión, los incidentes de seguridad de la información y ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la institución. Este proceso de notificación se realizará en las tres (3) etapas siguientes:

a. **Primera Comunicación:** Debe realizarse en un plazo máximo de dos (2) horas luego de identificado el incidente y contendrá datos generales, orientados a proporcionar una descripción global del incidente e identificar el contacto dentro de la Institución Supervisada para posteriores comunicaciones;

b. **Reporte Preliminar:** Debe remitirse en un plazo máximo de dos (2) días hábiles luego de identificado el incidente y contendrá datos detallados, incluyendo la naturaleza del incidente como su impacto preliminar, y las medidas adoptadas para gestionarlo. Este informe debe actualizase cada cinco (5) días hábiles mientras el incidente no sea resuelto; y,

c. **Reporte Final:** Debe remitirse en un plazo máximo de quince (15) días hábiles posteriores a la resolución final del incidente. Este reporte debe contener al menos datos detallados del incidente, causa raíz, vulnerabilidades explotadas (en los casos que aplique), plan de acción ejecutado, controles preventivos que se implementarán para evitar una reincidencia, impacto económico, legal y reputacional; participaciones y comunicaciones con terceros, utilización de pólizas de seguros, entre otros.

ARTÍCULO 22.- POLÍTICAS, PROCEDIMIENTOS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Instituciones Supervisadas deben establecer, implementar y actualizar políticas, procedimientos y controles específicos de seguridad de la información y ciberseguridad que permitan proteger los activos de información y mantener la confidencialidad, integridad y disponibilidad de la información, de acuerdo con las operaciones realizadas por grupos de interés, de forma que les permita apoyar la gestión efectiva de la seguridad de la información y ciberseguridad. Asimismo, el incumplimiento de estas políticas debe estar contemplado en el Reglamento de Sanciones correspondiente.

ARTÍCULO 23.- CAPACITACIÓN, CONCIENTIZACIÓN Y CULTURIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Instituciones Supervisadas deben establecer un programa de capacitación, concientización y culturización sobre seguridad de la información y ciberseguridad para sus colaboradores, integrantes del Órgano de Administración, y cuando sea relevante, al resto de los grupos de interés, a fin de asegurarse de que cuentan con la formación necesaria para cumplir con sus funciones y responsabilidades conforme a las políticas, procedimientos y el cumplimiento del Marco de Gestión de Seguridad de la Información y Ciberseguridad. Asimismo, deben promover campañas de concientización de seguridad de la información en el uso de sus canales digitales dirigidas a sus Usuarios Financieros.

ARTÍCULO 24.- EVALUACIONES DE SEGURIDAD Y PRUEBAS DE INTRUSIÓN POR TERCEROS

Las Instituciones Supervisadas deben realizar evaluaciones de seguridad y pruebas de intrusión a su plataforma tecnológica, ejecutadas por terceros. La periodicidad y el alcance de estas evaluaciones debe definirse con base en un análisis y considerando el perfil de riesgo de los procesos a revisar.

CAPÍTULO VI
DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

ARTÍCULO 25.- GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Las Instituciones Supervisadas deben implementar un Marco de Gestión de la Continuidad del Negocio con base en las mejores prácticas y estándares internacionales, aprobado por el Órgano de Administración, que brinde respuestas efectivas para que la operatividad del negocio continúe y responda de una manera razonable, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la Institución. Este marco debe contar con una estructura organizacional o funcional, responsabilidades y funciones claras, recursos, políticas, procesos, planes, entre otros.

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

ARTÍCULO 26.- ORGANIZACIÓN DE LA CONTINUIDAD DE NEGOCIO
Las Instituciones Supervisadas deben establecer, dentro de su estructura organizacional, una Unidad o función responsable de la gestión efectiva de la continuidad del negocio; la cual debe contar con la autoridad suficiente y capacidad de reportar al Órgano de Administración, Alta Gerencia y sus respectivos Comités. Asimismo, el Órgano de Administración y la Alta Gerencia deben garantizar la aplicación del Marco de Gestión de Continuidad del Negocio definiendo funciones y responsabilidades claras de los involucrados, rendición de cuentas, y asignando los recursos necesarios para la continuidad del negocio.

El personal que lidera la gestión de la continuidad de negocio debe contar con conocimientos, habilidades, competencias y experiencia sobre la gestión de continuidad de negocios, resiliencia operativa, y/o gestión de riesgos.

ARTÍCULO 27.- FASES DE LA CONTINUIDAD DEL NEGOCIO
Las Instituciones Supervisadas deben desarrollar al menos las siguientes fases como parte de la gestión de continuidad del negocio:

1. Evaluación y análisis de riesgos;

2. BIA;

3. Desarrollo de estrategias de continuidad;

4. Desarrollo de planes de continuidad;

5. Ejecución de pruebas y ejercicios;

6. Capacitación y concientización; y,

7. Mantenimiento y actualización de plan de continuidad.

ARTÍCULO 28.- EVALUACIÓN Y ANÁLISIS DE RIESGOS
Las Instituciones Supervisadas deben identificar y evaluar los riesgos que podrían causar una interrupción del negocio, aplicando una metodología consistente con la utilizada para la evaluación de los riesgos operativos.

Los resultados de la evaluación mencionada y sus actualizaciones periódicas deben ser reportados a la Alta Gerencia, que es el responsable de gestionar los niveles de riesgo aceptables. Estos resultados deben ser de conocimiento del Órgano de Administración.

ARTÍCULO 29.- ANÁLISIS DE IMPACTO DEL NEGOCIO (BIA)
Las Instituciones Supervisadas deben determinar el impacto que tendría una interrupción de los procesos que soportan sus principales líneas de negocios. Para ello, deben considerarse aspectos como: a) Daños a la viabilidad financiera de la Institución; b) Daños a su reputación; c) Incumplimiento de requerimientos regulatorios; y, d) Daños al personal o al público en general.

Para cada proceso debe establecerse el RTO y RPO para determinar el impacto, así como los recursos necesarios para su implementación. Adicionalmente, deben definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos.

ARTÍCULO 30.- DESARROLLO DE ESTRATEGIAS DE CONTINUIDAD
Las Instituciones Supervisadas deben determinar e implementar 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:

a) Acciones diferidas;

b) Procedimientos manuales;

c) Soluciones internas;

d) Degradación de servicios; y,

e) Acuerdos recíprocos y servicios comerciales de recuperación. Las estrategias de continuidad deben ser aprobadas por el Órgano de Administración, basadas en un análisis costo/beneficio de las estrategias identificadas y el cumplimiento del RTO y el RPO definido para cada proceso.

ARTÍCULO 31.- DESARROLLO DEL PLAN DE CONTINUIDAD
Las Instituciones Supervisadas deben implementar un Plan de Continuidad de Negocio, consistente en establecer un plan documentado que permita a la Institución la capacidad de mantener, o recuperar los principales procesos de negocio dentro de los parámetros previamente establecidos. El Plan de Continuidad de Negocio debe considerar mecanismos que tengan como objetivo principal, salvaguardar la integridad física del personal.

Además, debe contener un plan de continuidad de operaciones de tecnología, también conocido como Plan de Recuperación de Desastres (DRP, por sus siglas en inglés), 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 32.- EJECUCIÓN DE PRUEBAS Y EJERCICIOS
Las pruebas al Plan de Continuidad del Negocio deben realizarse de forma periódica, cuando existan cambios significativos en la Institución Supervisada o en el ambiente en el que opera; asimismo, deben estar basadas en escenarios adecuados y planificados que permitan a la Institución tener certeza de la efectividad de la estrategia de continuidad. Las pruebas deben documentarse, de forma tal, que contenga los resultados alcanzados, recomendaciones y acciones para implementar las mejoras de forma oportuna.

ARTÍCULO 33.- CONCIENTIZACIÓN Y CAPACITACIÓN
Las Instituciones Supervisadas deben implementar programas de concientización y capacitación para sus colaboradores, integrantes del Órgano de Administración y cuando

sea relevante al resto de los grupos de interés, con el propósito de crear, ampliar y actualizar los conocimientos sobre resiliencia, objetivos, políticas, roles y responsabilidades de la administración de la continuidad del negocio y sus procesos de soporte.

ARTÍCULO 34.- MANTENIMIENTO Y ACTUALIZACIÓN
Las Instituciones Supervisadas deben desarrollar procedimientos de mantenimiento y actualización del Marco de Gestión de Continuidad del Negocio, para la ejecución del mismo por un evento que afecte la continuidad de las operaciones de la institución.

ARTÍCULO 35.- PROCEDIMIENTOS DE RESPALDO Y RECUPERACIÓN
Las Instituciones Supervisadas deben establecer con base en un análisis de riesgos, y considerando el RTO y RPO definidos, procedimientos de respaldo y recuperación que incluyan aspectos como:

a) Rutinas de respaldo;

b) Duración;

c) Frecuencia;

d) Medio;

e) Controles de acceso;

f) Transporte;

g) Resguardo; y,

h) Destrucción.

Estos procedimientos deben ser probados periódicamente para garantizar que se reanude 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.

Sin perjuicio de lo anterior, las Instituciones Supervisadas obligatoriamente deben realizar al menos, respaldos al cierre contable mensual y al cierre contable anual.

ARTÍCULO 36.- PROCESAMIENTO DE DATOS SIGNIFICATIVO FUERA DEL 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 asumir la responsabilidad del conocimiento pleno sobre la arquitectura de las bases de datos y la estructura de procesamiento, a través del personal radicado en territorio nacional, atendiendo cualquier requerimiento de información que realice la Comisión. Asimismo, deben establecer las medidas necesarias para garantizar que la Comisión pueda acceder a la información en cualquier momento que lo requiera.

ARTÍCULO 37.- INCIDENTES QUE AFECTAN LA CONTINUIDAD DEL NEGOCIO
Las Instituciones Supervisadas deben notificar a la Comisión, los incidentes que afectan de manera significativa la continuidad del negocio. Esta notificación será dentro de los dos (2) días hábiles posteriores a la identificación del incidente y debe incluir entre otros la descripción de este y las medidas adoptadas para gestionarlo.

ARTÍCULO 38.- 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 digital y/o física actualizada del Plan en una ubicación que garantice la confidencialidad, integridad y disponibilidad del mismo, de modo que, en caso de cualquier interrupción o contingencia, se tenga acceso.

CAPÍTULO VII
DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

ARTÍCULO 39.- ORGANIZACIÓN DE LA UNIDAD DE AUDITORÍA INTERNA EN RELACIÓN CON TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas, dentro de sus Unidades de Auditoría Interna deben contar con un área o responsable especializado en auditorías de los sistemas de información, contando con un mandato claro, autoridad, libre acceso a la información, independencia de las funciones operativas, y con capacidad de reportar al Órgano de Administración y al Comité de Auditoría, ya sea directamente o a través del Auditor Interno. Asimismo, el área o responsable de las auditorías de sistemas de información debe contar con planes, metodologías, políticas, y procesos operativos para la vigilancia efectiva de las operaciones procurando la consecución de los objetivos institucionales.

El área o responsable de auditoría de los sistemas de información debe estar a cargo de un ejecutivo con formación académica, experiencia y competencias suficientes que le permitan el adecuado cumplimiento de sus funciones.

Sin perjuicio de lo anterior, las Instituciones Supervisadas podrán optar por tercerizar la auditoría de sistemas de información.

ARTÍCULO 40.- AUDITORÍA BASADA EN RIESGOS
La planificación de auditoría de sistemas, de conformidad con la metodología de auditoría, debe ser con base en los riesgos asociados a las TI, y así, garantizar una correcta asignación de recursos en las revisiones que, de acuerdo con el análisis de riesgos, presentan una mayor exposición. Sin perjuicio de lo anterior, la auditoría de sistemas de información debe evaluar la integridad y confiabilidad de la información administrada en los sistemas de información.

El Órgano de Administración debe proveer a la Auditoría Interna los recursos suficientes para el desarrollo de sus funciones, esto incluye la asignación de recursos necesarios del área o responsable especializada en auditoría de sistemas, para sus evaluaciones al ambiente de control relacionado a las TI.

En el caso de Instituciones miembros de Grupos Financieros cuya casa matriz radique fuera del territorio nacional y la auditoría de sistemas este a cargo de la casa matriz, el plan de auditoría de sistemas debe considerar los riesgos particulares de la Institución domiciliada en el país.

ARTÍCULO 41.- AUDITORÍA EXTERNA DE SISTEMAS
Sin perjuicio de lo establecido en los Artículos 39 y 40 de las presentes Normas, las Instituciones Supervisadas podrán contratar auditorías de sistemas de información realizadas por entes externos especializados. El alcance de estas revisiones debe definirse por parte de la Institución respecto de los procesos a auditar.

CAPITULO VIII
DEL HISTORIAL Y MONITOREO

ARTÍCULO 42.- RESGUARDO Y MONITOREO DE BITÁCORAS
Las Instituciones Supervisadas deben resguardar las bitácoras de auditorías de los sistemas, de forma automatizada, registrando los accesos, transacciones y consultas realizadas tanto a los sistemas de información como a los dispositivos de comunicaciones y seguridad. Estos registros deben al menos identificar la persona, lugar, tiempo y las acciones relacionadas con el aplicativo utilizado; y deben ser monitoreados por las funciones de vigilancia correspondientes. Los mismos deben estar a disposición de la Comisión cuando esta lo requiera.

ARTÍCULO 43.- PERÍODO DE RESGUARDO
Las Instituciones Supervisadas deben resguardar por un periodo de cinco (5) años las transacciones y seis (6) meses las consultas realizadas de conformidad con el Artículo anterior.

CAPITULO IX
DE LAS DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 44.- SANCIONES
La determinación y aplicación de sanciones por incumplimiento a las disposiciones establecidas en las presentes Normas serán realizadas de conformidad a lo establecido en la normativa aplicable.

ARTÍCULO 45.- CASOS NO PREVISTOS
La Comisión resolverá los casos no previstos, conforme a lo establecido en la legislación aplicable, mejores prácticas y estándares internacionales.

ARTÍCULO 46.- PLAZO DE ADECUACIÓN
Para efectos de la implementación de las disposiciones contenidas en las presentes Normas, las Instituciones Supervisadas contarán con el plan de adecuación siguiente:

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán

Programa	Tipo de Instituciones	Plazo	Observaciones
1.1 Plan de acción para adecuarse a las modificaciones de las presentes Normas, con su respectiva aprobación por el Órgano de Administración.	Instituciones del Sistema Financiero.	Noventa (90) días calendarios contados a partir de la entrada en vigencia de estas Normas.	El plan de acción debe tener un plazo máximo de doce (12) meses a partir de los noventa (90) días calendarios de entrada en vigencia de las presentes Normas, para adecuar los procesos de gestión de TI, la continuidad del negocio, seguridad de la información y ciberseguridad con lo dispuesto en estas Normas. Asimismo, dicho proceso de adecuación no exime de responsabilidad al Órgano de Administración en velar porque se gestionen los riesgos a los que se expone la Institución. Este plan de acción debe incluir al menos: a) Fecha de inicio y finalización de las actividades; b) Responsables de la ejecución; c) Descripción de las actividades a realizar, entre otros.
1.2 Plan de acción para adecuarse a las modificaciones de las presentes Normas, con su respectiva aprobación por el Órgano de Administración.	Resto de Instituciones Supervisadas.	Noventa (90) días calendarios contados a partir de la entrada en vigencia de estas Normas.	El plan de acción debe tener un plazo máximo de dieciocho (18) meses a partir de los noventa (90) días calendarios de entrada en vigencia de las presentes Normas, para adecuar los procesos de gestión de TI, la continuidad del negocio, seguridad de la información y ciberseguridad con lo dispuesto en estas Normas. Asimismo, dicho proceso de adecuación no exime de responsabilidad al Órgano de Administración en velar porque se gestionen los riesgos a los que se expone la Institución. Este plan de acción debe incluir al menos: a) Fecha de inicio y finalización de las actividades; b) Responsables de ejecución; y c) Descripción de las actividades a realizar, entre otros.
2.1 Informe semestral sobre los avances en la implementación de las presentes Normas para Gestión De Tecnologías De Información, Ciberseguridad y Continuidad del Negocio.	Instituciones Supervisadas	Diez (10) días hábiles después del cierre de cada semestre del plan implementado por la Institución.	

ARTÍCULO 47.- 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 la Resolución No.496/08-12-98, Resolución No.566/24-07-2001 y Resolución GE No. 266/21-02-2012, y cualquier otra disposición que contravenga las presentes Normas.

ARTÍCULO 48.- VIGENCIA
Las presentes Normas entrarán en vigencia a partir de la fecha de su publicación en el Diario Oficial "La Gaceta".

2. Comunicar la presente Resolución a las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros (CNBS), para los efectos legales correspondientes, así como a la Superintendencia de Bancos y Otras Instituciones Financieras, Superintendencia de Seguros, Superintendencia de Pensiones y Valores y Gerencia de Riesgos para su conocimiento.

3. Instruir a la Secretaría General de esta Comisión, que remita la presente Resolución, a la Gerencia Administrativa para que esta la envíe al Diario Oficial La Gaceta, para efectos de su publicación.

4. La presente Resolución entrará en vigencia a partir de su publicación en el Diario Oficial "La Gaceta". … Queda aprobado por unanimidad. … F) **MARCIO GIOVANNY SIERRA DISCUA**, Presidente; **ESDRAS JOSIEL SÁNCHEZ BARAHONA**, Comisionado Propietario; **ALEX ROBERTO LARA ENAMORADO**, Comisionado Suplente; **ANA GABRIELA AGUILAR PINEDA**, Secretaria General".

ANA GABRIELA AGUILAR PINEDA
Secretaria General

CNBS Honduras
https://www.cnbs.gob.hn/
Comisión Nacional de Bancos y Seguros
+504 2290-4500
Tegucigalpa, Honduras.
Francisco Morazán