PROYECTO DE NORMA PARA LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y CIBERSEGURIDAD

CAPÍTULO I
DISPOSICIONES GENERALES

ARTÍCULO 1.- OBJETO
La presente Norma tiene por objeto regular la gestión de tecnologías de información, la continuidad de las operaciones de tecnología, seguridad de la información y ciberseguridad en las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros.

ARTÍCULO 2.- ALCANCE
La presente Norma es aplicable a las Instituciones Supervisadas por la Comisión Nacional de Bancos y Seguros, así como a los Grupos Financieros de los cuales estas formen parte.

ARTÍCULO 3.- PRINCIPIO DE PROPORCIONALIDAD
La presente Norma y su contenido, es aplicable a las Instituciones Supervisadas, en función de su tamaño, naturaleza, complejidad de operaciones y perfil de riesgos. La Comisión Nacional de Bancos y Seguros realizará las supervisiones pertinentes en el momento que lo considere, así como, también podrá requerir las medidas o los ajustes que estime convenientes para su cumplimiento.

ARTÍCULO 4.- DEFINICIONES
Para los efectos de la presente Norma, serán aplicables las siguientes definiciones:

a. **Acuerdos de Nivel de Servicio (SLA, Service Level Agreement):** 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 de éstos, entre ellas exactitud, integridad, puntualidad y seguridad.

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

c. **Análisis de Impacto del Negocio (BIA, Business Impact Analysis):** 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.

d. **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.

e. **Capacidad o Tolerancia 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.

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

g. **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.

h. **Ciberincidente:** Ocurrencia de un evento que afecta adversamente la confidencialidad, integridad y disponibilidad de un sistema de información, red y/o la información que reside en ellos.

i. **Ciberresiliencia:** Capacidad de una organización de continuar llevando a cabo su misión, anticipando y adaptándose a ciberamenazas y otros cambios relevantes en el entorno; y, resistiendo, conteniendo y recuperándose rápidamente de incidentes de ciberseguridad.

j. **Ciberseguridad:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas de información a través del medio cibernético.

k. **Comisión:** Comisión Nacional de Bancos y Seguros.

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

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

n. **Funciones de vigilancia:** Son las encargadas de brindar vigilancia integral e independiente a nivel institucional, de la gestión operativa.

o. **Gestión Integral de Riesgos:** Proceso mediante el cual la Institución Supervisada, tanto a nivel individual como de Grupo Financiero, a través de sus líneas de defensa, realiza la identificación, medición, evaluación, mitigación o control, monitoreo y comunicación oportuna, de todos los riesgos materiales que puedan afectar su capacidad de cumplir con las obligaciones para sus clientes. Esto incluye los riesgos actuales (internos y externos) y los emergentes, a nivel de actividades significativas, institución en su conjunto o Grupo Financiero, cuando corresponda.

p. **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.

q. **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, clientes o afiliados, competidores, órganos reguladores de control y fiscalización, comunidad y los proveedores de bienes y servicios.

r. **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 que apruebe la Comisión.

s. **Incidente de seguridad de la información:** Ocurrencia de un evento que constituye una violación o amenaza inminente de las políticas y los procedimientos de seguridad de la Institución Supervisada, y pone en peligro real o potencialmente la confidencialidad, integridad y/o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite.

t. **Infraestructura de Tecnología de la Información o 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 tecnología de la información. La infraestructura de TI excluye al recurso humano, los procesos y la documentación.

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

v. **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, por lo que debe reconocer y gestionar el riesgo que asume en el ejercicio de sus actividades; **b) Segunda Línea de Defensa:** Complementa a la primera a través del seguimiento y reporte a las autoridades respectivas. Generalmente incluye la función de gestión de riesgo, la función de ética y cumplimiento, incluyendo lo referente a la prevención de lavado de activos y financiamiento del terrorismo u otras funciones de vigilancia de acuerdo a lo que la Comisión establezca; y, **c) Tercera Línea de Defensa:** consiste en la función de una Auditoría Interna independiente y efectiva, que proporcione al Consejo de Administración, Junta Directiva 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 al Consejo de Administración, Junta Directiva o su equivalente, que el Marco de Gobierno Corporativo, incluido el Marco de Gobierno de Riesgo sea eficaz y que existen y aplican consistentemente las políticas y procesos.

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

x. **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.

y. **Órgano de Administración:** Se refiere al Consejo de Administración, Junta Directiva, Asamblea de Participantes o Aportantes, o su equivalente.

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

aa. **Procesos 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. Su tolerancia a interrupciones es muy baja y el costo de interrupción es muy alto.

bb. **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.

cc. **Punto Objetivo de Recuperación (RPO, Recovery Point Objective):** Volumen de datos en riesgo de pérdida que la Institución Supervisada considera tolerable en caso

de una interrupción en sus operaciones, de acuerdo al apetito de riesgo definido por la Institución.

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

ee. 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.

ff. 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.

gg. 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.

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

ii. Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective): 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 LA GESTIÓN DE LOS RIESGOS ASOCIADOS CON TECNOLOGÍAS DE INFORMACIÓN

ARTÍCULO 5.- GESTIÓN DE LOS RIESGOS ASOCIADOS CON TECNOLOGÍAS DE INFORMACIÓN

Las Instituciones Supervisadas deben garantizar que su Marco de Gobierno de Riesgo, contemple lo relacionado con las tecnologías de información como un proceso institucional, transversal, y 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) La Declaración de Apetito de Riesgo;

b) Una 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) Una función de gestión de riesgos tecnológicos;

e) Un proceso 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 6.- GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN
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, la infraestructura de TI y la 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.

e) **Medición del Desempeño de TI**: Dar seguimiento permanente y efectivo, por parte de la Gerencia General o su equivalente, el Órgano de Administración y/o la instancia que estos definan, 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.

ARTÍCULO 7.- GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar un Marco de Gestión de TI, el cual debe estar conformado por un conjunto de 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 a una periodicidad definida por la Institución o ante el surgimiento de cambios significativos, de manera tal que asegure su actualización, vigencia y efectividad.

ARTÍCULO 8.- ORGANIZACIÓN DEL ÁREA ENCARGADA DE TECNOLOGÍAS DE INFORMACIÓN
El responsable de la gestión de TI y su área correspondiente, deben gestionar los riesgos materiales a las tecnologías de la información como primera línea de defensa; además, el área debe contar con una estructura organizacional alineada con el Plan Estratégico de TI, con una 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 el personal.

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

CAPÍTULO IV
DE LA TERCERIZACIÓN DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN

ARTÍCULO 9.- GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN
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 10.- RESPONSABILIDAD DE TERCERIZACIÓN DE SERVICIOS
Las Instituciones Supervisadas son las 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 11.- DEBIDA DILIGENCIA SOBRE EL PROVEEDOR DE SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas deben establecer acciones de debida 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 12.- TERCERIZACIÓN SIGNIFICATIVA DE TECNOLOGÍAS DE INFORMACIÓN
Para efectos de la presente Norma, se considera tercerización significativa la función de auditoría de sistemas, la función de gestión de seguridad de la información, la infraestructura tecnológica, procesamiento de datos, servicios en la nube y las identificadas por la propia institución.

La tercerización significativa de TI debe ser notificada a esta Comisión, treinta (30) días calendario previo a la suscripción del contrato. La Comisión podrá formular observaciones a dicho acuerdo conforme a lo establecido en el Artículo 15 de la presente Norma, y requerir la información adicional necesaria para su análisis.

ARTÍCULO 13.- TERCERIZACIÓN SIGNIFICATIVA DE PROCESAMIENTO DE DATOS
Los servicios de procesamientos de datos objeto de tercerización deben ser sometidos anualmente a un examen de auditoría independiente, esta debe ser realizada por entes especializados y de conformidad con las mejores prácticas internacionales.

Adicionalmente, las instituciones deben 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 son extensivos a los archivos maestros, transaccionales e históricos que la Comisión requiera.

Para la tercerización significativa de procesamiento de datos, la Institución Supervisada debe contar con la información requerida en el Anexo No.1 de la presente Norma, misma que debe estar a disposición de la Comisión cuando sea requerido.

ARTÍCULO 14.- 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.

ARTÍCULO 15.- GESTIÓN DE CONTRATOS POR 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 pueda ser auditada por la institución contratante y por la Comisión respecto de los servicios tercerizados.

b) Facultades para que el contratante y la Comisión 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.

c) Determinación de acuerdos de niveles de servicio (SLA) según las necesidades del contratante.

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

e) Obligatoriedad para el contratante, 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. Asimismo, la Institución debe tener la facultad de suspender contratos cuando el ente regulador lo requiera, por aspectos que puedan poner en riesgo la continuidad de sus operaciones.

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

ARTÍCULO 16.- 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 abarcar transversalmente la estructura organizacional y los procesos de la institución, garantizando que la información cumpla con las tres (3) características principales de seguridad que son 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, 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.

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 mitigarlos o reducir el impacto de acuerdo con el apetito y tolerancia al riesgo definido.

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

ARTÍCULO 17.- MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

Las Instituciones Supervisadas deben diseñar, implementar, documentar, monitorear y actualizar un Marco de Gestión de la Seguridad de la Información y Ciberseguridad, el cual debe incluir al menos: **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 y empresas relacionadas.

ARTÍCULO 18.- 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**: Las instituciones deben 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**: Las instituciones deben desarrollar e implementar los controles necesarios para limitar o contener el impacto de un evento potencial de ciberseguridad.

c) **Detectar**: Las instituciones deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través del monitoreo continuo.

d) **Responder**: Las instituciones deben contar con procesos y procedimientos para garantizar una respuesta oportuna, durante y después de un incidente de ciberseguridad.

e) **Recuperar y aprender**: Las instituciones deben 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 19.- 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.

ARTÍCULO 20.- 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, así como proteger 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 o problemas 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 tres (3) etapas, de la siguiente manera:

a) Primera comunicación: Deberá realizarse en un plazo máximo de dos (2) horas luego de ocurrido el evento 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: Deberá remitirse en un plazo máximo de dos (2) días hábiles luego de ocurrido el evento y contendrá datos detallados, incluyendo la naturaleza del incidente como su impacto preliminar, y las medidas adoptadas para gestionarlo. Este informe deberá actualizase cada cinco (5) días hábiles mientras el incidente no sea resuelto.

c) Reporte final: Deberá remitirse en un plazo máximo de diez (10) días hábiles posteriores a la resolución final del incidente. Este reporte deberá 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.

Sin perjuicio de lo anterior, las Instituciones Supervisadas deben notificar por medio del Capturador de Riesgo Operacional con la periodicidad que el Manual de Reporte de Datos establezca.

ARTÍCULO 21.- 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 sus 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 22.- 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. Esto incluye requerimientos de seguridad, responsabilidades legales y controles, así como entrenamiento en el uso correcto de los sistemas de información.

Asimismo, las Instituciones Supervisadas deben promover campañas de concientización de seguridad de la información en el uso de sus canales digitales dirigidas a sus Usuarios Financieros.

ARTÍCULO 23.- REVISIONES DE TERCEROS
Las Instituciones Supervisadas deben realizar evaluaciones de seguridad y pruebas de intrusión a su plataforma tecnológica, ejecutadas por entes externos. 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.

ARTÍCULO 24.- PÓLIZAS DE SEGUROS
Las Instituciones Supervisadas, conforme al principio de proporcionalidad respecto a su tamaño, naturaleza, complejidad de operaciones y perfil de riesgos, deben contar con cobertura de seguros que permita mitigar los riesgos provocados por ciberincidentes, así como los riesgos relacionados con eventos que afecten la integridad y disponibilidad de la infraestructura de TI, no siendo excluyente de cualquier otra cobertura que la institución pueda adicionar al seguro.

CAPÍTULO VI
DE LA GESTIÓN DE CONTINUIDAD DE LAS OPERACIONES DE TECNOLOGÍA

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, funciones y responsabilidades claras, recursos, políticas, procesos, planes, entre otros.

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 de las operaciones de tecnología:

1. Evaluación y análisis de riesgos.

2. Análisis de impacto del negocio (BIA).

3. Desarrollo de estrategias de continuidad.

4. Desarrollo de planes de continuidad.

5. Ejecución de pruebas y ejercicios.

6. Capacitación y concientización.

7. Mantenimiento y actualización de plan de continuidad.

La ejecución de cada una de estas fases debe ser documentada y aprobada por el Órgano de Administración de las Instituciones Supervisadas.

ARTÍCULO 28.- EVALUACIÓN Y ANÁLISIS DE RIESGOS
Las Instituciones Supervisadas deben identificar y evaluar los riesgos que podrían causar una interrupción del negocio. Para ello, deben aplicar 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 formalmente reportados a la Alta Gerencia, que es el responsable de gestionar las debilidades a 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: daños a la viabilidad financiera de la institución, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público

en general. Para cada proceso debe establecerse el tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (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: acciones diferidas, procedimientos manuales, soluciones internas, degradación de servicios, 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 tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (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 dotar a la institución de la capacidad de mantener, o de ser el caso, 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), 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 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 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 que este se encuentre siempre vigente en caso de requerir 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: las rutinas de respaldo, duración, frecuencia, medio, controles de acceso, transporte, resguardo y 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 obligatoriamente deben realizar al menos, respaldos al cierre contable mensual y al cierre contable anual.

ARTÍCULO 36.- 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 de las bases de datos. La Comisión en todo momento podrá acceder de forma irrestricta desde el territorio nacional, a la réplica de la base de datos antes mencionada y al ambiente de producción tanto del sistema de información como de su base de datos. Asimismo, las Instituciones Supervisadas deben realizar al menos una vez al año, pruebas de funcionamiento de la réplica de la base de datos, el resultado de estas pruebas debe ser documentado.

Las instituciones deben 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.

ARTÍCULO 37.- INCIDENTES DE CONTINUIDAD
Las Instituciones Supervisadas deben notificar a la Comisión, los incidentes de continuidad que afecten de manera significativa la operatividad del negocio. Esta notificación será dentro de los siguientes dos (2) días hábiles luego de ocurrido el evento y contendrá una breve descripción del incidente y las medidas adoptadas para gestionarlo.

Sin perjuicio de lo anterior, las Instituciones Supervisadas deben notificar por medio del Capturador de Riesgo Operacional con la periodicidad que el Manual de Reporte de Datos establezca.

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 A TECNOLOGÍAS DE INFORMACIÓN
Las Instituciones Supervisadas, dentro de sus Unidades de Auditoría Interna deben contar con un área o responsable especializada en auditorías de los sistemas de información, la cual debe contar con un mandato claro, autoridad, libre acceso a todo tipo de información, independencia de las funciones operativas, y 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 anual 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 a un análisis de riesgos, presentan una mayor exposición. Sin perjuicio de lo anterior, la auditoría de sistemas de información deberá evaluar la integridad y confiabilidad de la información administrada en los sistemas de información, así como la remitida a la Comisión por los diferentes medios que se han dispuesto para tal fin.

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.- AUDITORÍAS EXTERNAS DE SISTEMAS
Sin perjuicio de lo establecido en los Artículos 39 y 40 de la presente Norma, 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
HISTORIAL Y MONITOREO

ARTÍCULO 42.- MANTENIMIENTO Y MONITOREO DE REGISTROS
Las Instituciones Supervisadas deben mantener 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 los registros previstos en el Artículo anterior. El periodo de resguardo será de 5 años para las transacciones y 6 meses para la consulta.

CAPITULO IX
DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 44.- SANCIONES
La determinación y aplicación de sanciones por incumplimiento a las disposiciones establecidas en la presente Norma serán realizadas de conformidad a lo establecido en el reglamento de sanciones y las leyes y normativa vigente 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. Lo anterior, sin perjuicio de la

discrecionalidad que tendrán las instituciones de elevar a la Comisión los casos que estimen pertinentes.

ARTÍCULO 46.- PLAZO DE ADECUACIÓN

Para efectos de adecuación a las disposiciones contenidas en la presente Norma, las instituciones deben 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 Órgano de Administración	Sesenta (60) días calendarios contados a partir de la entrada en vigencia de la Norma.	Se deberá acompañar un plan de acción con plazo límite máximo de seis (6) meses a partir de los sesenta (60) días calendarios de entrada en vigencia de la Norma, para adecuar los procesos de gestión de TI, la continuidad de las operaciones de tecnología, seguridad de la información y ciberseguridad a esta Norma. El proceso de adecuación de esta Norma, 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 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 Tecnologías de la Información y Ciberseguridad.	Diez (10) días hábiles después del cierre del trimestre.	Según Anexo No. 2 a partir del segundo trimestre posterior a la entrada en vigencia de la presente Norma.

ARTÍCULO 47.- DEROGATORIA

A partir de la entrada en vigencia de la presente Norma, 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.

ARTÍCULO 48.- VIGENCIA

La presente Norma entrarán en vigencia a partir de la fecha de su publicación en el Diario Oficial “La Gaceta”.

Anexo No. 1

DOCUMENTACIÓN REQUERIDA PARA LA TERCERIZACIÓN SIGNIFICATIVA DE PROCESAMIENTO DE DATOS

Documento	Contenido mínimo requerido
1. Información general del proveedor y del servicio	• Razón social del proveedor. • Giro del negocio y años de experiencia, indicando a qué empresas brinda servicios actualmente, tanto fuera como dentro del país. • Estados financieros auditados del proveedor correspondiente a los tres (3) últimos años. • Relación de accionistas del proveedor y funcionarios principales. • Relación con la institución supervisada (indicar si pertenecen al mismo grupo económico). • Servicios que serán provistos por el proveedor y el tipo de información a ser procesada. • Ubicación (país y ciudad) del centro de procesamiento principal. • Informe del análisis de riesgos para la selección del proveedor.
2. Informe de la Plataforma Tecnológica	Aspectos a considerar: (Señalar qué equipos y aplicaciones estarán a cargo del proveedor) • Inventario de equipos de cómputo. • Inventario de software base. • Herramientas y/o manejadores de base de datos. • Aplicaciones críticas. • Esquema de comunicaciones a ser implementado entre el proveedor y la institución supervisada.
3. Informe de Evaluación de Riesgos	• Evaluación de los riesgos de operación asociados con el esquema propuesto por la institución supervisada, realizada por la Unidad de Riesgos.
4. Gestión de la seguridad de información	• Política de seguridad de información del proveedor. • Estructura organizativa para la gestión de la seguridad de información. • Asignación de responsabilidades asociadas con la seguridad de información en la institución supervisada y el proveedor. • Forma en que se aislará lógica y físicamente el procesamiento y la información objeto de la subcontratación. • Procedimientos y controles a implementar en los siguientes aspectos: - Seguridad lógica. - Seguridad de personal. - Seguridad física y ambiental.

	- Administración de las operaciones y comunicaciones. - Desarrollo y mantenimiento de los sistemas informáticos. - Administración de las copias de respaldo.
5. Gestión de continuidad de negocios	• Plan de Contingencia del proveedor, para asegurar la continuidad del servicio de procesamiento tecnológico. • Señalar la prioridad asignada al procesamiento de la información de la Institución Supervisada respecto al resto de clientes del proveedor, en caso que hubieren. • Señalar la forma en que se dará aviso a la institución supervisada, y las acciones que se deberán desarrollar en caso de una contingencia en el proveedor. • Frecuencia y alcance de las pruebas al Plan de Contingencia del proveedor.
6. Plan de Auditoría de Sistemas	• Señalar el alcance, forma y periodicidad de las revisiones de auditoría interna de sistemas, considerando el nuevo esquema de procesamiento principal de la institución supervisada.
7. Gestión del proyecto	• Cronograma de actividades, incluyendo plazos, responsables y principales hitos de control. • Costo estimado de implementación del proyecto.