EL COMITÉ DE NORMAS DEL BANCO CENTRAL DE RESERVA DE EL SALVADOR,

CONSIDERANDO:

I. Que de conformidad al artículo 2, inciso segundo de la Ley de Supervisión y Regulación del Sistema Financiero, para el buen funcionamiento del Sistema de Supervisión y Regulación Financiera se requiere que los integrantes del sistema financiero y demás supervisados cumplan con las regulaciones vigentes y la adopción de los más altos estándares de conducta en el desarrollo de sus negocios, actos y operaciones, de conformidad a lo establecido en la referida Ley, en las demás leyes aplicables, en los reglamentos y en las normas técnicas que se dicten para tal efecto.

II. Que el artículo 7 de la Ley de Supervisión y Regulación del Sistema Financiero, establece las entidades que están sujetas a la supervisión de la Superintendencia del Sistema Financiero.

III. Que de conformidad al artículo 32, inciso último, de la Ley de Supervisión y Regulación del Sistema Financiero, establece que, para los efectos de dicha Ley, los integrantes del sistema financiero podrán hacer uso de microfilm, de discos ópticos, medios magnéticos, medios electrónicos o de cualquier otro medio que permita archivar documentos e información, con el objeto de guardar eficientemente los registros, documentos e informes que correspondan, inclusive títulos valores.

IV. Que de conformidad al artículo 35, inciso primero y literal d) de la Ley de Supervisión y Regulación del Sistema Financiero los directores, gerentes y demás funcionarios que ostenten cargos de dirección o de administración en los integrantes del sistema financiero deberán conducir sus negocios, actos y operaciones cumpliendo con los más altos estándares éticos de conducta y actuando con la diligencia debida de un buen comerciante en negocio propio, estando obligados a cumplir y a velar porque en la institución que dirigen o laboran se cumpla con la adopción y actualización de políticas y mecanismos para la gestión de riesgos y entre otras acciones deberán incluir las medidas que se adoptarán para prevenir posibles incumplimientos a requerimientos regulatorios y las que adoptarán en el evento de que haya incurrido en ellos.

V. Que de conformidad al artículo 99, literales a) y g) de la Ley de Supervisión y Regulación del Sistema Financiero, el Banco Central de Reserva de El Salvador es la institución responsable de la aprobación de normas técnicas relativas a la gestión de riesgos por parte de los supervisados así como aquellas en las que se definan las condiciones mínimas que deben reunir físicamente los locales, sus medidas de seguridad, lo relativo a la conservación y archivo de documentación de los integrantes del sistema financiero.

VI. Que tomando como referencia estándares internacionales los cuales sugieren, entre otras actividades de buenas prácticas, la implementación de un Gobierno de la Seguridad de la

Información, para que a través de él las entidades se aseguren de gestionar adecuadamente la seguridad de la información que manejan de sus clientes y de la propia entidad.

VII. Que es de suma importancia que las entidades garanticen que la información que recopilan, procesan y almacenan de sus clientes se le aplique la debida confidencialidad; esté siempre disponible para consulta y uso propio de los clientes y de las entidades; y que sea íntegra de acuerdo a la veracidad de los documentos legales de donde fue extraída.

VIII. Que la rapidez con la que evoluciona el entorno de los sistemas de información hace necesario que se emitan disposiciones que contengan las especificaciones necesarias para que las entidades cuenten con la tecnología apropiada para realizar sus funciones de una manera eficiente.

POR TANTO,

en virtud de las facultades normativas que le confiere el artículo 99 de la Ley de Supervisión y Regulación del Sistema Financiero,

ACUERDA, emitir las siguientes:

NORMAS TÉCNICAS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I
OBJETO, SUJETOS Y TÉRMINOS

Objeto

Art. 1.- Las presentes Normas tienen como objeto establecer los criterios mínimos para la gestión de la seguridad de la información y la ciberseguridad de la misma, acordes a las mejores prácticas internacionales, naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones.

Sujetos

Art. 2.- Los sujetos obligados al cumplimiento de las disposiciones establecidas en las presentes Normas son los siguientes:

a) Los bancos constituidos en El Salvador, sus oficinas en el extranjero y sus subsidiarias; las sucursales y oficinas de bancos extranjeros establecidos en el país;
b) Las sociedades que de conformidad con la ley, integran los conglomerados financieros, o que la Superintendencia declare como tales, lo que incluye tanto a sus sociedades controladoras como a sus sociedades miembros;
c) Las instituciones administradoras de fondos de pensiones y los fondos que administran;
d) Las sociedades de seguros, sus sucursales en el extranjero y las sucursales de sociedades de seguros extranjeras establecidas en el país y las Asociaciones Cooperativas de Seguros constituidas en el país, en lo que no contradiga su respectiva Ley;

e) Las bolsas de valores, las casas de corredores de bolsa, las sociedades especializadas en el depósito y custodia de valores, las clasificadoras de riesgo y los agentes especializados en valuación de valores;
f) Los bancos cooperativos, las sociedades de ahorro y crédito y las federaciones reguladas por la Ley de Bancos Cooperativos y Sociedades de Ahorro y Crédito;
g) Las sociedades de garantía recíproca y sus reafianzadoras locales;
h) Las sociedades que ofrecen servicios complementarios a los servicios financieros de los integrantes del sistema financiero, en particular aquellas en los que participen como inversionistas;
i) Las sociedades administradoras u operadoras de sistemas de pagos y de liquidación de valores;
j) El Fondo Social para la Vivienda y el Fondo Nacional de Vivienda Popular, en lo que no contradiga a sus leyes de creación ni a lo dispuesto por la Corte de Cuentas;
k) El Instituto de Previsión Social de la Fuerza Armada;
l) El Instituto Nacional de Pensiones de los Empleados Públicos;
m) El Banco de Fomento Agropecuario, el Banco Hipotecario de El Salvador, S.A., y el Banco de Desarrollo de El Salvador, en lo que no contradiga a sus leyes de creación ni a lo dispuesto por la Corte de Cuentas;
n) Las titularizadoras y los fondos que administran;
o) Las bolsas de productos y servicios;
p) Las Gestoras de fondos de inversión y los fondos que administran;
q) Las Sociedades Proveedoras de Dinero Electrónico;
r) Agencias de Información de Datos;
s) La Unidad de Pensiones del Instituto Salvadoreño del Seguro Social; y
t) El Instituto Salvadoreño del Seguro Social, este último en lo relativo al Sistema de Pensiones Público, al Régimen de Riesgos Profesionales y reservas técnicas de salud.

Términos

Art. 3.- Para efectos de las presentes Normas, los términos que se indican a continuación tienen el significado siguiente:

a) **Activo de información:** componente que sustenta uno o más procesos de negocio y genera valor a la entidad. Los activos de información pueden ser de diversos tipos, entre ellos: datos o información, servicios (procesos), programas informáticos, dispositivos físicos, redes de comunicación, soportes de información, equipamiento auxiliar e instalaciones físicas, e intangibles (marcas);
b) **Alta Gerencia:** el Presidente Ejecutivo, Director Ejecutivo, Gerente General o quien haga sus veces y los cargos ejecutivos que le reportan al mismo, para el caso del Banco de Desarrollo de El Salvador, el Presidente;
c) **Aplicación, programa o sistema informático:** cualquier software utilizado por la entidad para la recopilación, almacenamiento, procesamiento, visualización o transmisión de información relacionada con los productos o servicios financieros que dicha entidad ofrece a sus clientes;
d) **Banco Central:** Banco Central de Reserva de El Salvador;

e) **Centro de datos alterno:** se refiere a una instalación, separada de la infraestructura física de la entidad, con una infraestructura tecnológica que garantice que podrá continuar con las operaciones críticas del negocio cuando el centro de datos principal no esté disponible;
f) **Centro de datos principal:** conjunto de equipos computacionales en los cuales operan los sistemas operativos y aplicaciones que procesan y almacenan información de los productos y servicios financieros que ofrecen las entidades a sus clientes;
g) **Ciberamenaza o amenaza cibernética:** potencial ocurrencia de una situación que pudiera convertirse en un ciberataque;
h) **Ciberataque o ataque cibernético:** acción organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de la materialización de accesos indebidos a la información de la entidad, comprometiendo la seguridad de la información de la misma;
i) **Ciberespacio:** entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física;
j) **Ciberriesgo, riesgo cibernético o de ciberseguridad:** posibles resultados negativos derivados de fallas en la seguridad de la infraestructura tecnológica o asociados a ataques cibernéticos;
k) **Ciberseguridad:** desarrollo de capacidades técnicas para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar la confidencialidad, integridad y disponibilidad de la información en el ciberespacio y que es esencial para la operación de la entidad;
l) **Confidencialidad:** propiedad de la información por la cual se le considera accesible solo a aquellos debidamente autorizados y solo para los fines específicos y expresamente delimitados;
m) **Configuración Segura:** proceso destinado a eliminar un medio de ataque parcheando vulnerabilidades y desactivando servicios no esenciales;
n) **Disponibilidad:** propiedad de la información por la cual permanece organizada y accesible para su uso cuando lo requieran usuarios autorizados;
o) **Entidad:** sujeto obligado al cumplimiento de las disposiciones de las presentes Normas, listado en el artículo 2 de las mismas;
p) **Evento:** suceso o serie de sucesos que pueden ser internos o externos a la entidad, originados por la misma causa, que ocurren durante el mismo período;
q) **Evento de ciberseguridad:** ocurrencia de una situación que podría afectar la protección o el aseguramiento de la información, infraestructura o plataforma tecnológica y aplicaciones de la entidad que son esenciales para el negocio;
r) **Factor de autenticación:** información utilizada para verificar la identidad de un servicio o una persona;
s) **Gestión de la Seguridad de la Información:** procesos mediante los cuales se previene, detecta y se responde a la seguridad de la información, independientemente al formato de ésta, incluyendo documentos en papel, propiedad digital e intelectual, y las comunicaciones verbales o visuales;
t) **Gobierno de la Seguridad de la Información:** conjunto de responsabilidades y prácticas que tienen la finalidad de brindar dirección estratégica y garantizar que se logren los objetivos

corporativos relacionados con la seguridad de la información, gestionándolo conforme a estándares internacionales, de acuerdo con la naturaleza, tamaño, perfil de riesgo de las entidades y volumen de sus operaciones y verificando que los recursos de la empresa se empleen con responsabilidad para estos fines;

u) **Incidente de seguridad de la información o de ciberseguridad:** uno o más eventos en concreto, asociados a un ciberataque, una posible falla en la política de seguridad de la información, en los controles o una situación previamente desconocida relevante para la seguridad de la información, que tiene una probabilidad significativa de comprometer las operaciones del negocio y dañar dicha seguridad;

v) **Información:** conjunto de datos organizados y comprensibles que comunican un mensaje. La información puede estar impresa o digital. En caso de que la información sea digital, esta puede estar en formatos de cualquier tipo, tales como electrónico, óptico o magnético. También se considerará cualquier comunicación (oral, visual o escrita) que podría incluir hechos, datos, u opiniones en cualquier medio o forma;

w) **Infraestructura o plataforma tecnológica:** componentes de hardware y software en los cuales se recopila, procesa, transmite y almacena la información relacionada con productos y servicios financieros que ofrece la entidad;

x) **Integridad:** propiedad por la que se salvaguarda que la información sea completa, exacta y válida;

y) **ISAE (Información de Seguridad para la Administración de Eventos) o SIEM por sus siglas en inglés:** sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red, como por ejemplo sistemas de centralización de registros de eventos del sistema operativo;

z) **Junta Directiva:** órgano colegiado encargado de la administración de la entidad, con funciones de supervisión, dirección y control u órgano equivalente. Para el caso de las Asociaciones Cooperativas será el Consejo de Administración, o según se defina en su Ley de creación;

aa) **Respaldo:** copia de la información original que se realiza con el fin de disponer de un medio para su recuperación en caso de pérdida parcial o total de estos;

bb) **Programa de Seguridad de la Información:** conjunto de planes implementados para preservar y mejorar continuamente la seguridad de la información, sobre la base de los requerimientos del negocio y el análisis de riesgos;

cc) **Resiliencia:** es la capacidad de un mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que pudo estar sometido;

dd) **Seguridad de la Información:** conjunto de medidas que permiten resguardar y proteger la información cumpliendo con las propiedades de confidencialidad, integridad y disponibilidad de la misma, con el fin que las amenazas no se materialicen;

ee) **Seguridad física:** aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los activos de información e información de la entidad;

ff) **Seguridad lógica:** aplicación de barreras y procedimientos que resguarden el acceso a la información y solo se permita acceder a ellos a las personas o servicios autorizadas para hacerlo, quedando evidencia de ello;

gg) **Servicios críticos:** son los servicios y actividades definidas como prioritarios cuya no disponibilidad compromete la existencia de la entidad;

hh) **Sistema de Gestión de la Seguridad de la Información (SGSI)**: se refiere al diseño, implementación y mantenimiento continuo de un conjunto de políticas y procesos para gestionar eficazmente la seguridad de la información y de la ciberseguridad;

ii) **Superintendencia:** Superintendencia del Sistema Financiero;

jj) **Tercerización de actividades, operaciones o procesos de tecnologías de la información:** se produce cuando la entidad encarga la realización de actividades, operaciones o procesos de tecnologías de la información, relacionados a servicios o productos financieros de la entidad, a un tercero, es decir, a una persona natural o jurídica distinta a la entidad;

kk) **Unidad de Ciberseguridad (UCIB):** unidad encargada de monitorear, evaluar y defender los sistemas de información de la entidad como por ejemplo sitios web, aplicaciones, bases de datos, centros de datos principales o alternos, servidores, redes, escritorios, dispositivos, entre otros; y

ll) **Vulnerabilidad**: debilidad de un activo o control que puede ser explotado o utilizado por una amenaza. Se tienen en cuenta todas aquellas amenazas que surgen por la interacción de los sistemas en el ciberespacio.

CAPÍTULO II
ROLES Y RESPONSABILIDADES

Función de seguridad de la información y de ciberseguridad

Art. 4.- Las entidades deberán contar con una estructura organizacional acorde a sus productos, servicios, operaciones, tamaño, perfil de riesgos y modelo de negocio, de tal forma que delimite claramente las funciones, roles, responsabilidades y facultades asociadas a la seguridad de la información y la ciberseguridad, así como los niveles de dependencia e interrelación que corresponde con cada una de las demás áreas de la entidad.

Asimismo, las entidades deberán asegurarse que todo su personal reconozca a la seguridad de la información y ciberseguridad como una de sus responsabilidades, aplicando las medidas de confidencialidad que fueran necesarias. La información cuya seguridad deberá preservarse, será la que de acuerdo a la clasificación de los activos de información que realice la entidad, requiera un tratamiento de aseguramiento o protección.

Responsabilidades de la Junta Directiva

Art. 5.- La Junta Directiva u órgano equivalente será la responsable de establecer un adecuado gobierno y gestión de la seguridad de la información por lo que deberá realizar como mínimo lo siguiente:

a) Aprobar los recursos necesarios para el establecimiento, implementación, monitoreo y mantenimiento de la gestión de la seguridad de la información, a fin de contar con la infraestructura, metodología, tácticas y personal apropiados. Asimismo, deberá nombrar a una persona responsable de gestionar la seguridad de la información, el cual tendrá una

comunicación permanente y directa con la Alta Gerencia, quien a su vez informará directamente a la Junta Directiva. La Junta Directiva hará constar en Punto de Acta su nombramiento, el cual deberá ser remitido a la Superintendencia a más tardar diez días hábiles después de dicho nombramiento;

b) Aprobar el programa de seguridad de la información y la estructura del SGSI; y
c) Requerir a Auditoría Interna que verifique la existencia y el cumplimiento de la estructura del SGSI.

Responsabilidades de la Alta Gerencia

Art. 6.- Para implementar la gestión de la seguridad de la información conforme a las disposiciones de la Junta Directiva, la Alta Gerencia de las entidades deberá realizar al menos lo siguiente:

a) Apoyar el programa de seguridad de la información;
b) Promover la mejora continua del SGSI y velar por su vigencia permanente; y
c) Apoyar al responsable de la seguridad de la información en la ejecución de estrategias y tácticas de seguridad de la información requeridas, ante un incidente de seguridad de la información o de ciberseguridad no previsto. La Alta Gerencia deberá comunicarlo directamente a la Junta Directiva.

Responsabilidades del Comité de Riesgos

Art. 7.- Las entidades deberán contar con un Comité de Riesgos el cual observará lo establecido en las presentes Normas y en las Normas Técnicas de Gobierno Corporativo" (NRP-17) aprobadas por el Banco Central, por medio de su Comité de Normas.

En materia de gestión de riesgos de la seguridad de la información, el Comité de Riesgos, o quien haga sus veces, será el responsable de llevar a cabo como mínimo, lo siguiente:

a) Proponer a la Junta Directiva la estructura del SGSI;
b) Revisar, evaluar y proponer para aprobación de la Junta Directiva el programa y recursos de seguridad de la información, dichos recursos deberán estar separados de los presupuestos destinados a cualquier otra área de la entidad; y
c) Efectuar el seguimiento de la gestión de la seguridad de la información.

Responsabilidad de la Unidad de Riesgos

Art. 8.- En cuanto a la gestión de la seguridad de la información, la Unidad de Riesgos, o quien haga sus veces, deberá realizar lo siguiente:

a) Proponer al Comité de Riesgos o quien haga sus veces, la creación de Comités, áreas o cargos especializados para el cumplimiento de las responsabilidades relacionadas con la gestión de la seguridad de la información; y
b) Velar que la gestión de la seguridad de la información sea consistente con las políticas y metodologías aplicadas para la gestión de riesgos.

Debido a su posición jerárquica y funciones, la persona designada o la unidad organizacional deberá asegurarse de que sus informes se hagan del conocimiento de la Junta Directiva o de la instancia que ésta delegue.

Unidad o área especializada en seguridad de la información

Art. 9.- En función a su tamaño, naturaleza y complejidad de productos, servicios y operaciones, la función de la seguridad de la información será desempeñada por una unidad o área especializada de la entidad. La unidad o área especializada debe ser independiente respecto de las áreas de negocio o de apoyo.

La Junta Directiva, u órgano equivalente de la entidad debe definir la unidad o área especializada en seguridad de la información que será la responsable de diseñar, implementar y mantener un SGSI. Dicha unidad deberá realizar como mínimo lo siguiente:

a) Elaborar y proponer al Comité de Riesgos o quien haga sus veces, las políticas y metodologías para la gestión de la seguridad de la información;
b) Coordinar entre las diversas áreas relevantes de la entidad la administración del SGSI;
c) Velar por una gestión eficaz de la seguridad de la información;
d) Proponer un manual de controles específicos de seguridad de la información, al Comité de Riesgos para su evaluación y validación y posteriormente someterlo a aprobación de la Junta Directiva;
e) Coordinar con las áreas correspondientes la implementación de los controles de seguridad de la información en toda la entidad y en las operaciones o procesos tercerizados, relacionados con activos de información de acuerdo a la clasificación de la entidad;
f) Diseñar y proponer, al Comité de Riesgos para su evaluación y validación, las métricas que permitan revisar y monitorear la seguridad de la información;
g) Desarrollar actividades de concientización a todo el personal en seguridad de la información;
h) Elaborar el programa de seguridad de la información y proponerlo al Comité de Riesgos o quien haga sus veces, para su revisión y evaluación;
i) Evaluar los incidentes de seguridad de la información y de ciberseguridad y recomendar, a las instancias correspondientes, acciones preventivas y correctivas, de acuerdo a procedimientos internos que establezca la entidad; y
j) Informar al Comité de Riesgos los aspectos relevantes de la gestión de la seguridad de la información para una oportuna toma de decisiones.

Para el caso que la estructura organizativa o el tamaño de la entidad no permita la creación de esta unidad, las funciones correspondientes podrán ser desarrolladas por una unidad administrativa que la Junta Directiva designe, procurando cumplir con lo dispuesto en las presentes Normas y se garantice la objetividad, el adecuado manejo de conflictos de interés, independencia de criterio, confidencialidad y acceso a la información. En estos casos, la entidad será responsable de contar con la documentación de respaldo de los temas revisados y la Junta Directiva de la entidad mantendrá la responsabilidad sobre la ejecución de las funciones definidas en las presentes Normas.

CAPÍTULO III
DE LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Sistema de Gestión de la Seguridad de la Información (SGSI) y controles de seguridad de la información

Art. 10.- Las entidades deben establecer, mantener y documentar un SGSI que guarde consistencia con el Sistema de Gestión de la Continuidad del Negocio y con la gestión de los riesgos operacionales. Las actividades mínimas que las entidades deberán realizar para desarrollar un SGSI serán las siguientes:

a) Establecimiento de un SGSI:

   i. Especificar el alcance del SGSI de acuerdo a las características del negocio de la entidad, sus activos, tecnología, entre otros;
   ii. Instaurar una política de seguridad de la información y ciberseguridad en relación a la naturaleza, tamaño o volumen de operaciones del negocio de la entidad;
   iii. Identificar, analizar, evaluar y mitigar los riesgos asociados a los activos, procesos, personas, proyectos y servicios de tecnología de la información, a través de la metodología aprobada por la Junta Directiva, considerando las amenazas y las vulnerabilidades a los que están expuestos, identificando los impactos; y
   iv. Definir controles de seguridad de la información, debidamente documentados.

b) Operación de un SGSI:

   i. Elaborar e implementar un plan mediante el cual se dará tratamiento a los riesgos identificados con sus respectivos controles;
   ii. Especificar cómo medirá la efectividad de dichos controles;
   iii. Establecer programas de capacitación y concientización para todo el personal de la entidad, al menos, una vez al año;
   iv. Administrar los recursos que componen el SGSI; y
   v. Aplicar las instrucciones y controles que sean efectivos para la inmediata detección y respuesta a incidentes de seguridad de la información.

c) Monitoreo y Revisión del SGSI:

   i. Ejecutar revisiones periódicas de la efectividad del SGSI;
   ii. Evaluar los controles definidos; y
   iii. Revisar al menos una vez al año el programa de seguridad de la información y, de ser pertinente, actualizar dicho plan.

d) Mantenimiento y Mejora del SGSI:

   i. Aplicar las mejoras encontradas al SGSI;
   ii. Ejecutar acciones correctivas y preventivas a fin de eliminar o mitigar fallos en la seguridad de la información y ciberseguridad; y
   iii. Informar de forma oportuna a las partes interesadas todas las acciones y resultados de la gestión de seguridad de la información.

En función a su tamaño, naturaleza y complejidad de productos, servicios y operaciones, las entidades podrán someter sus procesos a certificaciones reconocidas internacionalmente en relación a la seguridad de la información.

Seguridad lógica

Art. 11.- Para la gestión de la seguridad lógica de la información que se administre, las entidades deben considerar como mínimo lo siguiente:

a) Procedimientos formales para la concesión, administración de derechos, perfiles y roles de cuentas privilegiadas y cuentas de usuarios finales, así como la desactivación de las mismas en los casos que sea requerido;
b) Establecer una adecuada segregación de funciones, de tal manera que una misma persona no tenga varios roles o privilegios que puedan poner en peligro la seguridad de la información;
c) Revisiones periódicas sobre los derechos concedidos a los usuarios y el uso real de los derechos;
d) Los usuarios deben contar con factores de autenticación de uso personal, de tal manera que las responsabilidades asignadas puedan ser seguidas e identificadas. Asimismo, las entidades deben aplicar factores de autenticación para sus activos de información;
e) Controles permanentes sobre aplicaciones informáticas;
f) Mantenimiento, monitoreo y análisis de registros de auditoría;
g) Seguimiento sobre pistas de auditoría y el acceso y uso de los sistemas para detectar actividades no autorizadas;
h) Controles sobre accesos remotos y dispositivos móviles que interactúen con la infraestructura de tecnología de la entidad; y
i) Controles sobre configuración segura de hardware, software, equipo de comunicación, dispositivos móviles; limitando servicios, protocolos, puertos y usuarios.

Función de Ciberseguridad

Art. 12.- Para una gestión efectiva del riesgo de ciberseguridad, considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados, la entidad debe implementar una función de ciberseguridad, la cual, deberá cumplir como mínimo, con lo siguiente:

a) Reportar a la Junta Directiva, al Comité de Riesgos y a la Alta Gerencia, los resultados de su gestión, especialmente en la identificación de ciberamenazas, resultados de la evaluación de efectividad de los programas de ciberseguridad, propuestas de mejora en materia de ciberseguridad y resumen de los incidentes de ciberseguridad que afectaron la entidad. La periodicidad de los reportes debe ser, al menos, semestralmente;
b) Actualizarse permanentemente y de manera especializada para que esté al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad;

c) Proponer capacitaciones que deben recibir regularmente los miembros de la Junta Directiva, Comité de Riesgos, Alta Gerencia y otros que designe la Junta Directiva de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas;
d) Monitorear y verificar el cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna;
e) Asesorar a la Alta Gerencia y la Junta Directiva en temas que considere necesarios sobre ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia;
f) Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de una UCIB, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán; considerando lo establecido en el Anexo No. 1 de las presentes Normas; y
g) Proponer, a las instancias correspondientes, los presupuestos de ciberseguridad.

Sin perjuicio de las actividades que debe realizar la función de ciberseguridad de la que trata el presente Capítulo, las funciones de gestión de respuesta a incidentes podrán ser desagregadas en diferentes líneas de defensa que establezca la entidad.

Comunicación de incidentes de seguridad de la información o ciberseguridad

Art. 13.- La entidad deberá establecer procedimientos de notificación y comunicación que contemple, como mínimo, lo siguiente:

a) Información que reportará a la Alta Gerencia y a la Superintendencia, sobre incidentes de seguridad de la información y ciberseguridad, en el momento que tenga conocimiento sobre el incidente materializado, por el medio que tenga disponible y que de acuerdo a su análisis de riesgos, exceda los límites de riesgos que la Junta Directiva ha aprobado, haciendo una breve descripción del incidente, que incluya la información general que tenga a su disposición sobre la posible causa e impacto y acciones ejecutadas. Posteriormente la entidad, diez días calendario después de haber reportado el referido incidente, deberá remitir completa la documentación siguiente:

    i. Fecha y hora de inicio de ocurrencia;
    ii. Fecha y hora de fin de ocurrencia, si hubiere terminado el incidente;
    iii. Descripción del incidente;
    iv. Causas de las fallas;
    v. Diagnóstico técnico;
    vi. Canales afectados;
    vii. Tiempo fuera de servicio;
    viii. Impacto ocasionado; y
    ix. Acciones correctivas ejecutadas y/o plan de acción a implementar por esa entidad para solventar las causas que originaron el o los incidentes, así como para prevenirlos en el futuro; y

b) Información que reportará, de acuerdo a sus políticas y de manera oportuna, a sus clientes y usuarios de productos y servicios financieros afectados, sobre incidentes de ciberseguridad que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para mitigar el incidente.

Cobertura de riesgos

Art. 14.- Las entidades deberán incluir en los contratos de tercerizaciones de servicios críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de ciberseguridad y seguridad de la información. Asimismo, verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas en dichos contratos, para lo cual debe implementar los mecanismos adecuados para tales efectos.

Para el caso de las entidades que se rigen conforme a lo dispuesto en la Ley de Adquisiciones y Contrataciones de la Administración Pública, realizarán esta actividad sin contravención a dicha Ley.

En ningún caso la seguridad del tercero debe ser inferior que la del cliente. Por tanto, los contratos deberán especificar los requerimientos mínimos de seguridad de la información aceptados por las entidades.

Art. 15.- La entidad podrá evaluar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos, debiendo establecer la periodicidad con la cual efectuará la evaluación.

Etapas del proceso de gestión de riesgos de ciberseguridad

Art. 16.- Las entidades deberán contar con un proceso continúo documentado y revisado periódicamente, para la gestión de los riesgos de ciberseguridad, para lo cual deberá contemplar, al menos, las etapas siguientes:

a) **Prevención:** Las entidades deben desarrollar e implementar los controles adecuados para velar por la seguridad de la información y la gestión de la ciberseguridad. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad. En esta etapa, las entidades deben realizar, al menos, lo siguiente:

   i. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales) y gestión de identidades bajo la premisa que las personas solo pueden disponer de los recursos que demande su trabajo, durante el tiempo que ello sea necesario;
   ii. Adoptar políticas, procedimientos, mecanismos y herramientas manuales o automatizadas para la protección de la información;
   iii. Identificar y medir las amenazas cibernéticas que puedan llegar a afectar a la entidad y establecer controles para su mitigación;
   iv. Contar con herramientas o servicios que permitan identificar, registrar bitácoras y correlacionar eventos que alerten sobre anomalías e incidentes de seguridad que hayan

afectado activos de información, para implementar controles adecuados tal como un sistema ISAE;

v. Monitorear diferentes fuentes de información tales como sitios web, blogs, redes sociales, proveedores y comunidades de interés, con el propósito de identificar posibles ataques cibernéticos contra la entidad;
vi. Informar a los clientes y usuarios de servicios financieros de la entidad sobre recomendaciones que deberán adoptar para la gestión de la ciberseguridad; y
vii. Identificación de los activos de información críticos que estén expuestos al ciberespacio.

b) **Protección y detección:** En esta etapa, las entidades deben desarrollar e implementar actividades apropiadas para identificar, analizar y controlar eventos de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos, para lo cual, las entidades deberán aplicar como mínimo, lo siguiente:

i. Adoptar procedimientos y mecanismos para identificar, analizar y mitigar las amenazas y los incidentes de ciberseguridad que se presenten;
ii. Gestionar las vulnerabilidades informáticas de las plataformas tecnológicas que soporten activos de información y que estén expuestos a ciberataques o riesgos tecnológicos internos, fortaleciendo los eslabones de seguridad en los servicios informáticos relacionados a productos o servicios financieros brindados por la entidad; y
iii. Realizar un monitoreo continuo de la infraestructura tecnológica de la entidad, haciendo uso de herramientas automatizadas y una estructura organizativa, con el propósito de identificar y mitigar comportamientos inusuales que puedan evidenciar ciberataques o incidentes de ciberseguridad contra la entidad.

c) **Respuesta:** Aún con las medidas de seguridad adoptadas, las entidades deben desarrollar e implementar actividades para mitigar los incidentes relacionados con ciberseguridad. Para hacerle frente a esta situación, las entidades deberán realizar, al menos, las actividades siguientes:

i. Establecer procedimientos de respuesta a incidentes de ciberseguridad tales como: desconexión automática de equipos, cambios de contraseñas, actualizar la base de firmas del antivirus, bloqueo de direcciones IP o cualquier otro que determine la entidad;
ii. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados;
iii. Adoptar los mecanismos necesarios para que los sistemas de información o cualquier otro elemento de la infraestructura tecnológica de la entidad, se le aplique la debida resiliencia posterior a un ataque cibernético;
iv. Preservar, las evidencias digitales, si existieren, para que las áreas de seguridad o las autoridades pertinentes puedan realizar las investigaciones correspondientes; y

d) **Recuperación y aprendizaje:** Para llevar a cabo esta etapa, las entidades deberán desarrollar e implementar actividades apropiadas para mantener los planes de resiliencia y restaurar cualquier capacidad o servicio que se haya deteriorado debido a un incidente de ciberseguridad. Por lo que, dichas entidades, deberán como mínimo, realizar lo siguiente:

i. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes;
ii. Considerar dentro del plan de continuidad del negocio la recuperación y reanudación de la operación;
iii. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos; y
iv. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la misma y con las entidades de su sector financiero.

Art. 17.- Seguridad de personal

Las entidades, en lo aplicable, para la gestión de la información por parte de los empleados y personal subcontratados que en ella laboran, deben considerar como mínimo lo siguiente:

a) Procesos de selección del personal que incluyan la verificación de los antecedentes, de conformidad con la legislación laboral vigente;
b) Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad; y
c) Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución formal de activos.

Art. 18.- Seguridad física y ambiental de los activos de información

Las entidades deben asegurarse de que se acceda apropiadamente a todos los activos de información y que se encuentren en los lugares y condiciones óptimas, para tales efectos se considerará al menos lo siguiente:

a) Controles para evitar daños o interferencias al personal y a los activos de información de la entidad y evitar acceso físico no autorizado; y
b) Controles para prevenir pérdidas, daños o robos de los activos de información, incluyendo la protección de los equipos y del personal frente a amenazas físicas y ambientales que permitan combatir amenazas latentes como fuego, agua, temperaturas inusuales, terremotos, entre otros.

Inventario de activos de información y clasificación de la información

Art. 19.- Para el inventario de activos de información y clasificación de la información, la entidad debe realizar al menos lo siguiente:

a) Realizar y mantener un inventario de activos de información y asignar responsabilidades respecto a la protección de dichos activos; y
b) Clasificar la información, en términos de los requerimientos legalmente establecidos, que fueren aplicables, y grado crítico de la información para la entidad, así como las medidas apropiadas de control que deberán asociarse a las clasificaciones.

Administración de las operaciones y comunicaciones

Art. 20.- Las entidades deben implementar una administración de las operaciones y comunicaciones de servicios o productos financieros que se ofrecen a los clientes o usuarios, de tal

forma que les permita contar con políticas y planes de renovación de infraestructura tecnológica, y así poder mitigar los riesgos de seguridad asociados a la obsolescencia de dicha infraestructura, para la cual establecerá como mínimo, lo siguiente:

a) Procedimientos aprobados y documentados para la operación de los sistemas informáticos;
b) Controles y pruebas sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, la infraestructura tecnológica y los procedimientos;
c) Separación de los ambientes de desarrollo, pruebas y producción de sistemas informáticos;
d) Monitoreo y supervisión de los servicios de tecnología de información dado por terceras partes;
e) Administración de la capacidad de procesamiento, almacenamiento y transmisión de información, realizándose análisis periódicos de estas capacidades;
f) Controles preventivos y de detección sobre el uso de programas informáticos de procedencia dudosa, virus, malware, denegación de servicios, phishing y otros similares;
g) Seguridad sobre protocolos, puertos de redes y redes inalámbricas, navegadores, medios de almacenamiento, perímetro y documentación de sistemas, intercambio de la información a nivel interno y externo, incluido el correo electrónico brindado por la entidad como el de uso personal, tanto a nivel local como remoto, y sobre los canales electrónicos;
h) Resguardo de registros de auditoría y monitoreo del uso de los sistemas; y
i) Pruebas o evaluaciones de vulnerabilidad e intrusión sobre los componentes de infraestructura de tecnología y mitigar las brechas de seguridad identificadas. Estas deberán realizarse al menos una vez al año y cuando existan cambios en la infraestructura referida. Dichas actividades podrán ser realizadas por proveedores de este tipo de servicios y serán documentadas de acuerdo a lo dispuesto en el artículo 29 de las presentes Normas.

Adquisición, desarrollo y mantenimiento de sistemas informáticos

Art. 21.- Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, las entidades en lo aplicable, deben tomar en cuenta como mínimo lo siguiente:

a) Incluir controles al ingreso, acceso, transmisión, procesamiento y salida de información;
b) Aplicar las técnicas de cifrado que garanticen efectivamente la protección del almacenamiento y transporte de la información crítica de acuerdo a la clasificación de la entidad;
c) Definir controles sobre la implementación de aplicaciones antes del ingreso a producción;
d) Controlar el acceso al código fuente de los sistemas informáticos que son propiedad de la entidad;
e) Mantener un estricto y formal control de cambios y versiones, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios;
f) Contar con mecanismos de desarrollo seguro que permita analizar y corregir las vulnerabilidades de seguridad existentes en las aplicaciones informáticas de la entidad. Deberá efectuarse este tipo de análisis en el ciclo de vida del desarrollo de dichas aplicaciones y establecer los procedimientos de corrección adecuados; asimismo, cuando dichos sistemas se encuentren en producción; y
g) Establecer un procedimiento de instalación de actualización de software, de forma segura y

controlada, con el objeto de prevenir vulnerabilidades y sin afectar el desempeño de la infraestructura.

Art. 22.- La Junta Directiva, resolverá sobre la necesidad de realizar reemplazos, sustituciones o adquisiciones dejando constancia de su decisión en el Acta de Sesión correspondiente.

Para el caso de las entidades que se rigen conforme a lo dispuesto en la Ley de Adquisiciones y Contrataciones de la Administración Pública, realizarán esta actividad sin contravención a dicha Ley.

Si derivado de las actividades establecidas en el artículo 10 de las presentes Normas, las entidades determinan la necesidad de efectuar sustituciones o reemplazos de sistemas informáticos principales, sean estos sistemas gestores de bases de datos o aplicaciones, o la adquisición de sistemas informáticos para nuevas operaciones, productos o servicios financieros que la entidad ofrece a sus clientes; la unidad o área correspondiente deberá presentar a la Junta Directiva o quien haga sus veces, la información siguiente:

a) Estudio de factibilidad técnica y financiera;
b) Estudio de las características de la plataforma actual;
c) Potenciales riesgos asociados a la sustitución o reemplazo del sistema informático principal;
d) Mecanismos de mitigación y contingencia en caso de materializarse los riesgos a que se refiere el literal anterior;
e) Ventajas y desventajas asociadas a la sustitución, reemplazo o adquisición del sistema informático;
f) Justificación de la actividad a realizar; y
g) Análisis y conclusiones de las ofertas de los proveedores.

Procesamiento, procedimientos de respaldo y restauración de la información

Art. 23.- Las entidades deben contar con procedimientos de respaldo regular y periódicamente validados. Estos procedimientos deberán incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada, en forma oportuna y eficiente, en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad del negocio de la entidad.

Las entidades conservarán la información de respaldo y los procedimientos de restauración en una ubicación a suficiente distancia, que evite exponerlos ante posibles eventos que comprometan la operación del centro de datos principal de procesamiento de la información, de tal forma que se mitiguen amenazas de índole geográfica, física y ambiental. La distancia se determinará de acuerdo a la evaluación de riesgos que realice la entidad.

Las entidades deben almacenar sus respaldos de información, debiendo notificar a la Superintendencia el lugar específico donde se almacena o procesa la información de sus clientes. Dicha notificación deberá realizarla 10 días hábiles posteriores al haberse iniciado operaciones o cuando ocurra un cambio de ubicación de los mismos.

Gestión de incidentes de seguridad de la información

Art. 24.- Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las entidades deben considerar al menos los aspectos siguientes:

a) Procedimientos para la comunicación interna y debida documentación de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información; y
b) Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

Ubicación y traslado del centro de datos principal y centro de datos alterno de la información

Art. 25.- Las entidades deben informar a la Superintendencia, con 30 días hábiles de anticipación de inicio de operaciones, el traslado y ubicación específica de su centro de datos principal y centro de datos alterno de operaciones, donde se almacena y procesa la información correspondiente a los productos y servicios financieros que ofrecen a sus clientes.

Cuando una entidad desee ubicar fuera de las fronteras del país el centro de datos principal o el centro de datos alterno de la información, por medio de la tercerización de actividades u operaciones de tecnología de la información, deberá demostrar a la Superintendencia el cumplimiento de las condiciones establecidas en el Anexo No. 1 de las presentes Normas.

Tercerización de actividades u operaciones de tecnología de la información

Art. 26.- Las entidades son las responsables de preservar la seguridad de su información, la de sus clientes y toda información a la que accedan, empleen, procesen o almacenen para el desarrollo de sus operaciones, por lo que, en caso decidan tercerizar actividades u operaciones de tecnología de la información, deberán constatar que la prestación del servicio cumpla las condiciones contenidas en las Secciones A, B y C del Anexo No. 1, de las presentes Normas.

Las condiciones establecidas en el Anexo No. 1, deberán ser documentadas en un informe que las entidades remitirán a la Superintendencia, según lo establecido en el artículo 31 de las presentes Normas.

Las condiciones descritas en la Sección B, del Anexo No. 1 de las presentes Normas, bajo las cuales se tercerizarán las actividades u operaciones de tecnología de la información, podrán establecerse en un contrato de adhesión o en un contrato negociable. En el citado contrato debe constar explícitamente todo lo concerniente al servicio brindado, a la confidencialidad, seguridad de la información, procesos, sistemas, tecnologías que las albergan, entre otros. Además, que el procesamiento o almacenamiento de la información tercerizada se encuentran efectivamente aislados en todo momento, de tal forma que no exista comunicación o conectividad con la información de otros clientes del proveedor.

Las entidades que deseen tercerizar actividades u operaciones de tecnología de la información relacionados con productos y servicios financieros que estas ofrecen, serán siempre las

responsables en última instancia de la integridad, disponibilidad y confidencialidad de la información que se acceda, procese, trasmita y almacene en dichas tercerizaciones.

Asimismo, las entidades deberán elaborar un cronograma de actividades que incluya plazos, responsables, principales hitos de control de implementación del proyecto.

CAPÍTULO IV
INFORMACIÓN Y CONTROL

Conglomerados financieros

Art. 27.- En el caso de los conglomerados financieros a los que se refiere el Capítulo I del Título Quinto de la Ley de Bancos, la unidad de seguridad de la información podrá ser la misma que tenga el banco controlador para las entidades con giro similar o complementario; las Instituciones Administradoras de Fondos de Pensiones, tendrán su propia unidad de seguridad de la información.

Previa consulta con la Junta Directiva, el jefe de la unidad de seguridad de la información de la controladora o del banco controlador deben definir el programa de seguridad de la información a emplear en las sociedades que conforman los conglomerados financieros y determinar la organización interna de la seguridad de la información, tanto a nivel de controladora como de las sociedades que la integran, con el objeto de asegurar la calidad y metodologías a emplear en el programa de seguridad de la información.

La unidad de seguridad de la información del banco controlador o de la controladora debe disponer de sistemas de control efectivos para verificar que todas las empresas que sean controladas por un banco o una controladora de finalidad exclusiva, cumplan con las políticas establecidas por la Junta Directiva y las regulaciones locales.

Privacidad de la información

Art. 28.- Las entidades deben adoptar medidas que aseguren la protección y confidencialidad de la información bajo su responsabilidad, como datos personales, e información que reciben de sus clientes, usuarios de servicios, proveedores, entre otros; sin perjuicio de lo establecido en el marco legal vigente.

Documentación

Art. 29.- Las entidades deben presentar a la Superintendencia, dentro de los primeros ciento veinte días calendario siguientes al cierre de cada ejercicio anual, como parte del "Informe de Evaluación Técnica de la Gestión Integral de Riesgos", un informe relativo a nivel de cumplimiento de los requisitos del SGSI.

El informe deberá contener como mínimo lo siguiente:

a) Las estrategias y principales políticas utilizadas para la gestión de la seguridad de información y de la ciberseguridad;

b) Principales requisitos logrados del SGSI; y
c) El programa de seguridad de la información.

Para el caso del Programa de Seguridad de la Información, las entidades deberán remitirlo a la Superintendencia, anualmente y cuando se modifique.

Auditoría Interna
Art. 30.- La Unidad de Auditoría Interna debe considerar en su plan anual de trabajo, la evaluación del cumplimiento de las disposiciones de las presentes Normas.

Detalles técnicos del envío de información
Art. 31.- La Superintendencia remitirá a las entidades, en un plazo máximo de noventa días posteriores a la fecha de entrada en vigencia de las presentes Normas, con copia al Banco Central, los detalles técnicos relacionados con el envío de la información requerida. Los requerimientos de información se circunscribirán a la recopilación de información conforme lo regulado en las presentes Normas.

CAPÍTULO V
OTRAS DISPOSICIONES Y VIGENCIA

Sanciones
Art. 32.- Los incumplimientos a las disposiciones contenidas en las presentes Normas, serán sancionados de conformidad con lo previsto en la Ley de Supervisión y Regulación del Sistema Financiero.

Trámites en Proceso
Art. 33.- Los procedimientos y recursos administrativos que estuvieran pendientes a la fecha de la vigencia de las presentes Normas, se continuarán realizando de acuerdo con la normativa con que se hayan iniciado.

Contrataciones posteriores a la entrada en vigencia
Art. 34.- Las entidades que después de la fecha de entrada en vigencia de las presentes Normas deseen adquirir sistemas informáticos o encomendar en un tercero el desarrollo de los mismos y que estén relacionados con productos o servicios financieros de dicha entidad, deberán cumplir con lo dispuesto en el artículo 22, literal c) de las presentes Normas.

Plan de Adecuación
Art. 35.- Las entidades, para cumplir las disposiciones establecidas en las presentes Normas, deberán presentar a la Superintendencia un plan de adecuación, dentro de los ciento ochenta días siguientes a la vigencia de las presentes Normas. Una vez presentado el plan, las entidades deberán implementarlo en un plazo máximo de veinticuatro meses contados a partir de su presentación.

Aspectos no previstos

Art. 36.- Los aspectos no previstos en materia de regulación en las presentes Normas, serán resueltos por el Banco Central por medio de su Comité de Normas.

Vigencia

Art. 37.- Las presentes Normas entrarán en vigencia a partir del día uno de julio del dos mil veinte.

Anexo No.1

CONDICIONES PARA TERCERIZAR ACTIVIDADES U OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN RELACIONADAS A PRODUCTOS Y SERVICIOS FINANCIEROS QUE OFRECE LA ENTIDAD

La entidad que desee tercerizar actividades u operaciones de tecnología de la información, deberá constatar que la prestación del servicio cumpla las condiciones siguientes:

Sección A

1. Previo a la tercerización se deberá realizar una evaluación de riesgos a efecto de identificar aquellos riesgos derivados de los servicios a contratar (o del outsourcing de actividades o servicios) y establecer los mecanismos de mitigación apropiados. La entidad deberá, además, considerar en las evaluaciones aquellos riesgos que se generan como consecuencia de la concentración de entidades financieras en un proveedor, debiendo establecer los mecanismos de mitigación y las acciones a realizar si dicho proveedor falla, considerando, en la medida de lo posible contratar otros proveedores o contar con otras garantías para mitigar este tipo de riesgos, a fin de garantizar los derechos de los clientes.
2. La evaluación a que se refiere el numeral anterior deberá considerar los riesgos operacionales (incluyendo los tecnológicos y legales), riesgos reputacionales y riesgos financieros.
3. Debida identificación del proveedor:
    a. Sobre el proveedor: Denominación o Razón social y giro del negocio, experiencia, servicios, clientes (personas jurídicas), periodos de servicio, entre otros.
    b. Para el caso de un proveedor local, nómina de accionistas y principales funcionarios y en los casos previstos por la Ley, Declaración Jurada suscrita por la entidad en la que se confirma la no existencia de conflicto de interés entre la entidad y el proveedor.
    c. La entidad deberá realizar la debida diligencia de dicho proveedor sobre su solidez financiera, experiencia en la prestación del servicio, reputación, capacidades administrativas, técnicas y operativas en relación con los servicios a ser tercerizados. La debida diligencia realizada durante el proceso de selección debe ser documentada y revisada anualmente; utilizando la información más reciente, como parte de los procesos de monitoreo y control de la tercerización de la actividad u operación.
    d. Ubicación (país y ciudad) de las instalaciones del proveedor en donde se encuentran tercerizadas las actividades u operaciones de tecnología de la información.
    e. Descripción de las fortalezas o razones para la selección del proveedor.

Anexo No.1

4. La entidad debe identificar todos los proveedores de servicios en la cadena de suministro y garantizar que las responsabilidades del proveedor se pueden cumplir a lo largo de la cadena.

5. La entidad debe garantizar a la Superintendencia, cuando ésta lo estime pertinente, el acceso y disposición de los datos o información relacionada con el servicio tercerizado sin restricciones; manteniendo en el territorio nacional los mecanismos apropiados y el personal idóneo y necesario para tales efectos, así mismo, garantizar las condiciones del acceso para la auditoría interna y las firmas de auditoría externa que deben efectuar sus evaluaciones en cumplimiento al marco regulatorio vigente.
6. La entidad debe requerir al proveedor de servicios prestados una declaración jurada o certificación vigente, que indique que cuentan con un programa o gestión de la seguridad de la información, planes de continuidad del negocio, pruebas desarrolladas y resultados de las pruebas, así mismo, verificar la capacidad para recuperar y reanudar el servicio ante interrupciones.
7. La entidad debe verificar que puede requerir al proveedor del servicio, informes de auditoría vigentes y asociados a los servicios prestados. Dicha información deberá ser provista, a requerimiento de la Superintendencia.

Sección B

1. Indicar claramente que la entidad es la que tiene la propiedad exclusiva sobre todos sus datos o información relacionada con la actividad o proceso a tercerizar; que el proveedor no adquiere ningún tipo de derechos o licencias a través del contrato para utilizar los datos o información que la entidad le proporcione para sus propios fines; y que el proveedor no adquiere y no puede reclamar ningún interés en los datos o información debido a la confidencialidad y seguridad que se debe guardar sobre los mismos, sin perjuicio de lo establecido en el artículo 133 de la Ley de Bancos.
2. Descripción de los servicios u operaciones de tecnología de información que planean tercerizar y el tipo de información a ser procesada.
3. Descripción de las aplicaciones que planean estar a cargo del proveedor.
4. Establecer claramente el alcance del servicio, las responsabilidades de la entidad y las de su (s) proveedor (es) de servicios, sobre cada servicio que se proporcione.
5. Establecer los niveles de servicios en condiciones normales y de contingencia tras una interrupción, para esto último se deberá garantizar el establecimiento de planes de contingencia y de continuidad del servicio, de tal forma que el proveedor, y subcontratistas si hubieren, garanticen el cumplimiento de la actividad u operación tercerizada y que el

riesgo de tercerización está dentro del nivel determinado como aceptable para la entidad contratante.

Anexo No.1

6. Procedimiento planeado de comunicación entre los proveedores y la entidad.
7. Condiciones referentes a la capacidad, disponibilidad, tiempos de recuperación, resolución de incidentes y horarios de atención del proveedor del servicio.
8. La obligación del proveedor del servicio de informar, en cuanto le sea posible, a la entidad sobre cualquier evento o situación que pudiera afectar significativamente la prestación del servicio.
9. Que el proveedor corregirá oportunamente las vulnerabilidades informáticas detectadas.
10. Definición de mecanismos de control, por parte de la entidad, en la revisión y monitoreo de los servicios prestados, así como el procedimiento de escalamiento.
11. Obligación de establecer acuerdos de no revelación, de ser el caso, por el personal subcontratado por el proveedor relacionados con el manejo de la información de la entidad.
12. Disposiciones sobre la propiedad intelectual y derechos de autor.
13. Confidencialidad y protección de la información durante la vigencia del contrato y posteriormente, en caso de terminación del mismo.
14. Establecer canales de comunicación con el proveedor de servicios cifrados de extremo a extremo.
15. Acuerdos de indemnizaciones para mitigar los impactos ocasionados por posibles deficiencias en la prestación del servicio por parte del proveedor, de acuerdo a lo establecido en relación al nivel de servicio acordado.
16. Para el caso de que el proveedor realice subcontrataciones en los servicios que está ofreciendo a la entidad, deberá considerar los riesgos operacionales (incluyendo los tecnológicos y legales), riesgos reputacionales y riesgos financieros.
17. Cuando sea aplicable, el proveedor debe hacer constar que la información y el procesamiento o almacenamiento objeto de la contratación se encuentran efectivamente aislados en todo momento, de tal forma que no exista comunicación o conectividad con la información de otros clientes del proveedor subcontratado.
18. El proveedor deberá indicar claramente, al subcontratista que la entidad es la que tiene la propiedad exclusiva sobre todos sus datos o información relacionada con la actividad o proceso a tercerizar; que el proveedor subcontratado no adquiere ningún tipo de derechos o licencias a través del contrato para utilizar los datos o información que el proveedor le proporcione para sus propios fines; y que el proveedor subcontratado no adquiere y no puede reclamar ningún interés en los datos o información debido a la confidencialidad y seguridad que se debe guardar sobre los mismos.

19. Garantizar la devolución y destrucción o borrado seguro de la información involucrada en la prestación del servicio en caso de que lo solicite la entidad o ante la terminación del contrato, y tratamiento de la misma, a fin, de proteger los derechos de los clientes.

Anexo No.1

Sección C

1. La entidad deberá establecer procedimientos de respuesta, los cuales deben ser transparentes, para compartir información a la Superintendencia, setenta y dos horas después de ocurrido un incidente de seguridad de la información.
2. La entidad debe asegurarse que puede dar por finalizado el servicio contratado sin interrupción indebida a su servicios u operaciones, o su cumplimiento con el marco regulatorio por lo que deberán contar con planes de salida y arreglos de terminación, todo debidamente documentado y probado.
3. Que la entidad cuenta con políticas y procedimientos apropiados para evaluar, administrar y monitorear los servicios brindados por terceros y verificar periódicamente su cumplimiento.
4. La entidad deberá establecer los procesos a ser aplicados en caso de resolución, intervención o liquidación para garantizar que la Superintendencia tenga acceso a los datos o información en caso de materializarse dichos casos.