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

**CONSIDERANDO:**

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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 cuenten a las entidades 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**

1. Las presentes Normas tienen como objeto establecer los criterios mínimos para la adopción de políticas y procedimientos relacionados con el desarrollo de metodologías 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**

1. Los sujetos obligados al cumplimiento de las disposiciones establecidas en las presentes Normas son:
2. 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;
3. 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;
4. Las instituciones administradoras de fondos de pensiones;
5. Las sociedades de seguros, sus sucursales en el extranjero y las sucursales de sociedades de seguros extranjeras establecidas en el país;
6. Las bolsas de valores, las casas de corredores de bolsa, las sociedades especializadas en el depósito y custodia de valores, las clasificadoras de riesgo, los agentes especializados en valuación de valores y los almacenes generales de depósito;
7. 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;
8. Las sociedades de garantía recíproca y sus reafianzadoras locales;
9. 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;
10. Las sociedades administradoras u operadoras de sistemas de pagos y de liquidación de valores;
11. El Fondo Social para la Vivienda y el Fondo Nacional de Vivienda Popular;
12. El Instituto de Previsión Social de la Fuerza Armada;
13. El Instituto Nacional de Pensiones de los Empleados Públicos;
14. 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;
15. Las titularizadoras y los fondos que administran;
16. Las bolsas de productos y servicios;
17. Las Gestoras de fondos de inversión y los fondos que administran;
18. Las Empresas de Transferencia de Dinero y los Agentes cuyo país de origen sea El Salvador de acuerdo a lo establecido en las “Normas Técnicas para el Registro, Obligaciones y Funcionamiento de Entidades que Realizan Operaciones de Envío o Recepción de Dinero” (NRP-12); y
19. Las Sociedades Proveedoras de Dinero Electrónico.

**Términos**

1. Para efectos de las presentes Normas, los términos que se indican a continuación tienen el significado siguiente:
2. **Activo de información:** componente que sustenta uno o más procesos de negocio de una entidad y genera alto 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);
3. **Alta Gerencia:** el Presidente Ejecutivo, Gerente General o quien haga sus veces y los ejecutivos que le reportan directamente;
4. **Autenticidad:** condición bajo la cual la información es originada por quien dice ser el autor o propietario y recibida por quien es el destinatario; y que no ha sido alterado en ningún momento;
5. **Centro de datos principal:** conjunto de equipos computacionales en los cuales la mayor parte del tiempo operan los sistemas operativos y aplicaciones que procesan y almacenan un alto volumen de información de los productos y servicios financieros que ofrecen las entidades a sus clientes;
6. **Ciberamenaza o amenaza cibernética:** potencial ocurrencia de una situación que pudiera convertirse en un ciberataque;
7. **Ciberataque o ataque cibernético:** acción criminal 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 un crimen y mediante la cual, dichos agentes comprometen la seguridad de la información de la entidad;
8. **Ciberespacio: e**ntorno 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;
9. **Ciberiesgo o riesgo cibernético:** posibles resultados negativos derivados de fallas en la seguridad de la infraestructura tecnológica o asociados a ataques cibernéticos;
10. **Ciberseguridad:** desarrollo de capacidades técnicas para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar la información, infraestructura o plataforma tecnológica y aplicaciones en el ciberespacio y que son esenciales para la operación de la entidad;
11. **Computación en la nube:** modelo informático que permite obtener, desde cualquier lugar y bajo demanda, acceso a través de una red a un conjunto compartido de recursos informáticos configurables, el cual se puede conformar y suministrar rápidamente con un esfuerzo de gestión mínimo o con una interacción mínima con el proveedor de los servicios;
12. **Confidencialidad:** propiedad de la información por la cual se le considera accesible solo a aquellos debidamente autorizados y solo para los fines clara y expresamente delimitados;
13. **Disponibilidad:** propiedad de la información por la cual permanece organizada y accesible para su uso cuando lo requieran usuarios autorizados;
14. **Entidad(es):** sujeto obligado al cumplimiento de las disposiciones de las presentes Normas, listado en el artículo 2 de las mismas;
15. **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;
16. **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;
17. **Factor de autenticación:** información utilizada para verificar la identidad de una persona;
18. **Gestión de la Seguridad de la Información:** procesos mediante los cuales se previene, detecta y se responde a incidentes de seguridad de la información implicando un mantenimiento continuo, revisión y auditoría a dichos procesos;
19. **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 y verificando que los recursos de la empresa se empleen con responsabilidad para estos fines;
20. **Factor de autenticación:** información utilizada para verificar la identidad de una persona;
21. **Incidente de ciberseguridad:** ocurrencia de una situación que afecta la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio;
22. **Incidente de Seguridad de la Información:** uno o más eventos en concreto, asociados a 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;
23. **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;
24. **Información en tránsito:** información que fluye a través de la red pública, como internet, y los datos que viajan en una red privada, como una red de área local (LAN) corporativa o empresarial;
25. **Información sensible: i**nformación de los clientes que no puede ser expuesta o compartida al público de acuerdo a la legislación;
26. **Infraestructura o plataforma tecnológica:** componentes de hardware y software en los cuales se recolecta, procesa, transmite y almacena la información relacionada con productos y servicios financieros que ofrece la entidad;
27. **Integridad:** propiedad por la que se salvaguarda que la información sea completa, exacta y válida;
28. **ISAE (Información de Seguridad para la Administración de Eventos):** 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;
29. **Junta Directiva:** órgano colegiado encargado de la administración de la entidad, con funciones de supervisión y control. Para el caso de las Asociaciones Cooperativas será el Consejo de Administración;
30. **Nube híbrida:** modelo de servicio de computación en la nube que combina el uso de nube pública con nube privada;
31. **Nube privada:** modelo de servicio de computación en la nube en la que la infraestructura o plataforma tecnológica del centro principal de datos se aloja dentro de las instalaciones de la entidad**;**
32. **Nube pública:** modelo de servicio de computación en la nube a través de internet, en la que la información de la entidad se aloja en las instalaciones del proveedor del servicio;
33. **Respaldo:** Copia de los datos originales que se realizan con el fin de disponer de un medio para su recuperación en caso de pérdida parcial o total de estos;
34. **Plan de Seguridad de la Información:** procedimientos documentados que guían al personal de las entidades en la aplicación de las instrucciones, actividades y tareas específicas propuestas en el Programa de Seguridad de la Información;
35. **Programa de Seguridad de la Información:** combinación total de las medidas técnicas, operativas y de procedimientos, así como las estructuras administrativas implementadas para preservar y mejorar continuamente la seguridad de la información, sobre la base de los requerimientos del negocio y el análisis de riesgos;
36. **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;
37. **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;
38. **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;
39. **Seguridad lógica:** aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo, quedando evidencia de ello;
40. **Sistema de Gestión de la Seguridad de la Información y de la Ciberseguridad (SGSCI**): 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;
41. **Sitio alterno de operaciones:** se refiere a una instalación, separada de la infraestructura física de la entidad, con una infraestructura tecnológica que garantice que la entidad podrá continuar con las operaciones críticas del negocio cuando el centro de datos principal no esté disponible;
42. **Superintendencia:** Superintendencia del Sistema Financiero;
43. **Terceros críticos:** terceros con quien se vincula la entidad y que, de acuerdo con los parámetros establecidos por la misma, pueden tener incidencia directa en la seguridad de su información;
44. **Tercerización de operaciones o servicios de tecnologías de la información:** se produce cuando la entidad encarga la realización de operaciones o procesos de tecnologías de la información, relacionado a servicios o productos financieros de la entidad a un tercero, es decir, a una persona natural o jurídica distinta a la entidad;
45. **UCIB:** unidad de ciberseguridad 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, servidores, redes, escritorios, dispositivos, entre otros; y
46. **Vulnerabilidad**: debilidad de un activo o control que puede ser explotado 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 GENERALES**

**Función de Seguridad de la Información y de Ciberseguridad**

1. Las entidades deberán contar con una estructura organizacional acorde a sus productos, servicios, operaciones, tamaño 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. La información cuya seguridad deberá preservarse, será aquella a la que se tiene acceso por estar laborando en la entidad; independientemente que la información pertenezca a la entidad, que pueda asociarse a un cliente o que esta sea sensible.

**Responsabilidades de la Junta Directiva**

1. La Junta Directiva será la responsable de establecer un gobierno y gestión de la seguridad de la información y ciberseguridad, por lo que deberá realizar como mínimo lo siguiente:
2. Aprobar las estrategias generales de seguridad de la información y de la ciberseguridad coherentes con la estrategia de negocio y los objetivos empresariales;
3. Aprobar las políticas que dan soporte a las estrategias de seguridad de la información y de la ciberseguridad;
4. Aprobar políticas y procesos en materia de tecnología informática para identificar, evaluar, vigilar y gestionar los riesgos tecnológicos, revisándoos al menos una vez al año;
5. Aprobar la metodología para la gestión de la seguridad de la información y de la ciberseguridad;
6. 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 administrar la seguridad de la información, el cual tendrá una comunicación permanente y directa con la Junta Directiva, y esta hará constar en Punto de Acta su nombramiento, el cual deberá ser remitido a la Superintendencia a más tardar 3 días hábiles después de dicho nombramiento;
7. Aprobar el plan de seguridad de la información y de la ciberseguridad; y
8. Asegurarse de que la Auditoría Interna verifique la existencia y el cumplimiento de la estructura del SGSl.

Las estrategias, políticas y metodologías para la gestión de la seguridad de la información y de la ciberseguridad deben ser revisadas al menos una vez al año o cuando haya modificaciones significativas en los procesos de la entidad.

**Responsabilidades de la Alta Gerencia**

1. 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:
2. Apoyar el programa de seguridad de la información y de la ciberseguridad;
3. Promover la mejora continua del SGSCI y velar por su vigencia permanente; y
4. Ante un incidente de seguridad de la información no previsto, apoyar al responsable de la seguridad de la información en la ejecución de estrategias y tácticas de seguridad de la información requeridas.

**Responsabilidades del Comité de Riesgos**

1. En materia de la gestión de la seguridad de la información y de la ciberseguridad, el Comité de Riesgos, o quien haga sus veces, será el responsable de llevar a cabo como mínimo, lo siguiente:
2. Proponer a la Junta Directiva la estructura del SGSCI;
3. Revisar, evaluar y proponer para aprobación de la Junta Directiva las estrategias y políticas para la gestión de la seguridad de la información y de la ciberseguridad;
4. Aprobar las metodologías de gestión de la seguridad de la información y de ciberseguridad;
5. Revisar, evaluar y proponer para aprobación de la Junta Directiva el plan y programa de seguridad de la información y de ciberseguridad; y
6. Efectuar el seguimiento de la gestión de la seguridad de la información y de la ciberseguridad.

Cuando el número de las operaciones o la estructura organizativa de la entidad no permita la creación del Comité de Riesgos, las funciones correspondientes podrán ser desarrolladas por la Junta Directiva de la entidad o por un Comité de Riesgos Corporativo, siempre que cumpla con lo dispuesto en el marco legal aplicable y con las disposiciones establecidas en las presentes Normas, garantizándose 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 las actas, informes y documentación de respaldo de los temas revisados.

La Junta Directiva de la entidad mantendrá la responsabilidad sobre la ejecución de las funciones definidas en las presentes Normas. En el caso de las sucursales de bancos extranjeros establecidos en el país y sucursales de Sociedades de Seguros Extranjeras establecidas en el país, el Comité de Riesgos estará constituido por su Representante o quien haga sus veces, un funcionario de la Alta Gerencia y un Ejecutivo que tenga como responsabilidad la gestión de los riesgos de la entidad.

El Comité estará presidido por uno de sus miembros que tenga conocimiento en finanzas. El Comité de Riesgos cumplirá como mínimo con las disposiciones establecidas en las Normas relativas a la Gestión de Riesgos que para tales efectos emita el Banco Central por medio de su Comité de Normas.

**Responsabilidad** **de la Unidad de Riesgos**

1. En cuanto a la gestión de la seguridad de la información, la Unidad de Riesgos, o quien haga sus veces, deberá realizar lo siguiente:
2. Evaluar si existe la necesidad de constituir Comités, unidades, áreas o cargos especializados para el cumplimiento de las responsabilidades relacionadas con la gestión de la seguridad de la información y de ciberseguridad. De ser necesario, presentar su propuesta al Comité de Riesgos, o quien haga sus veces; y,
3. Asegurar de que la gestión de la seguridad de la información y de ciberseguridad sea consistente con las políticas y metodologías aplicadas para la gestión de riesgos.

Cuando el número de las operaciones o la estructura organizativa de la entidad no permita la creación de la Unidad de Riesgos, la Junta Directiva deberá designar una persona de la entidad, según aplique, y proveerle los recursos suficientes para desempeñar su función conforme al tamaño, estructura y perfil de riesgo de la entidad; en todo caso, deberá asegurarse que exista independencia de ésta con las áreas de negocio y operativas, a fin de evitar conflictos de interés y asegurar una adecuada separación de funciones y responsabilidades.

Su posición jerárquica deberá asegurar que sus informes sean conocidos por la Junta Directiva o por la instancia que ésta delegue.

**Unidad o área especializada en Seguridad de la Información y de Ciberseguridad**

1. En función a su tamaño, naturaleza y complejidad de productos, servicios y operaciones, la función de la seguridad de la información y de ciberseguridad 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 y de ciberseguridad que será la responsable de implementar y mantener un Sistema de Gestión de la Seguridad de la Información y Ciberseguridad. Dicha unidad deberá realizar como mínimo lo siguiente:

1. Elaborar y proponer al Comité de Riesgos o quien haga sus veces, las políticas y metodología para la gestión de la seguridad de la información;
2. Coordinar entre las diversas áreas relevantes de la entidad la administración del Sistema de Gestión de la Seguridad de la Información y de Ciberseguridad;
3. Velar por una gestión competente de la seguridad de la información y de la ciberseguridad;
4. Proponer controles adicionales específicos para cubrir las brechas de seguridad de la información y de ciberseguridad existentes;
5. Coordinar y monitorear la implementación de los controles de seguridad de la información en toda la entidad y en las operaciones o procesos tercerizados;
6. Diseñar y proponer las métricas que permitan revisar y monitorear la seguridad de la información;
7. Desarrollar actividades de concientización y entrenamiento al personal en seguridad de la información;
8. Elaborar el plan y programa de seguridad de la información y de ciberseguridad proponerlo al Comité de Riesgos o quien haga sus veces, para su revisión y evaluación;
9. Evaluar los incidentes de seguridad de la información y de ciberseguridad y recomendar acciones preventivas y correctivas; y
10. Informar al Comité de Riesgos los aspectos relevantes de la gestión de la seguridad de la información y ciberseguridad 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 Y CIBERSEGURIDAD**

**Sistema de Gestión de la Seguridad de la Información (SGSCI) y Controles de Seguridad de la Información**

1. Las entidades deben establecer, mantener y documentar un Sistema de Gestión de la Seguridad de la Información 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:
2. Establecimiento de un SGSCI:
3. Especificar el alcance del SGSCI de acuerdo a las características del negocio de la entidad, sus activos, tecnología, entre otros;
4. 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;
5. Instaurar una infraestructura tecnológica para cubrir las necesidades actuales y previstas del negocio, tanto en circunstancias normales y como en periodos de tensión;
6. Aplicar un enfoque de evaluación de riesgos, el cual comprenderá un análisis y evaluación de los mismos;
7. Identificar, analizar y evaluar los riesgos asociados a los activos, considerando las amenazas y las vulnerabilidades a los que están expuestos, identificando los impactos; y
8. Definir objetivos de control y controles para dichos riesgos.

b) Operación de un SGSCI:

1. Elaborar e implementar un plan mediante el cual se dará tratamiento a los riesgos identificados con sus respectivos controles;
2. Especificar cómo medir la efectividad de dichos controles;
3. Establecer programas de capacitación y conocimiento;
4. Administrar los recursos que componen el SGSCI; y
5. Aplicar las instrucciones y controles que sean efectivos para una inmediata detección y respuesta a incidentes de seguridad de la información.

c) Monitoreo y Revisión del SGSCI:

1. Ejecutar revisiones periódicas del SGSCI;
2. Evaluar los controles definidos; y
3. Actualizar al menos una vez al año el plan de seguridad de la información.

d) Mantenimiento y Mejora del SGSCI:

1. Aplicar las mejoras encontradas al SGSCI;
2. Ejecutar acciones correctivas y preventivas a fin de eliminar o mitigar fallos en la seguridad de la información y ciberseguridad; y
3. 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**

1. Para la gestión de la seguridad lógica de la información que se administre, las entidades deben considerar como mínimo lo siguiente:
2. Procedimientos formales para la concesión, administración de derechos y perfiles, así como la inhabilitación de usuarios en los casos de goce de periodo de vacaciones o revocación del mismo por desvinculación laboral, ausencia temporal, entre otras;
3. Establecer segregación de funciones, de tal forma que la información que en ellas se administre, sea conforme a dichas funciones;
4. Revisiones periódicas sobre los derechos concedidos a los usuarios y el uso real de los derechos;
5. Los usuarios deben contar con factores de autenticación de uso personal, de tal manera que las responsabilidades asignadas puedan ser seguidas e identificadas;
6. Controles sobre aplicaciones informáticas y registros de auditoría;
7. Seguimiento sobre pistas de auditoría y el acceso y uso de los sistemas para detectar actividades no autorizadas; y
8. Controles sobre accesos remotos y dispositivos móviles.

**Seguridad de personal**

1. Las entidades, en lo aplicable, para la gestión de la información por parte de los empleados que en ella laboran, deben considerar como mínimo lo siguiente:
2. Procesos de selección del personal que incluyan la verificación de los antecedentes, de conformidad con la legislación laboral vigente;
3. Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad; y
4. 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.

**Seguridad física y ambiental de equipos o dispositivos**

1. Las entidades deben asegurarse de que se acceda apropiadamente a todos los equipos relacionados a tecnologías de información y que se encuentren en los lugares y condiciones óptimas, para tales efectos se considerará al menos lo siguiente:
2. Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales, al personal y a la información de la entidad; y
3. Controles para prevenir pérdidas, daños o robos de los activos, 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**

1. Para el inventario de activos de información y clasificación de la información la entidad debe realizar al menos lo siguiente:
2. Realizar y mantener un inventario de activos de información y asignar responsabilidades respecto a la protección de dichos activos; y
3. Clasificar la información, en términos de requerimientos legales 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**

1. Las entidades deben implementar una administración de las operaciones y comunicaciones 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 realizará como mínimo lo siguiente:
2. Procedimientos aprobados y documentados para la operación de los sistemas informáticos;
3. Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, la infraestructura tecnológica y los procedimientos;
4. Adecuada segregación de funciones para reducir el riesgo de error o fraude;
5. Separación de los ambientes de desarrollo, pruebas y producción de sistemas informáticos;
6. Monitoreo y supervisión de los servicios de tecnología de información dado por terceras partes;
7. Administración de la capacidad de procesamiento, almacenamiento y transmisión de información, realizándose análisis periódicos de estas capacidades;
8. Controles preventivos y de detección sobre el uso de programas informáticos de procedencia dudosa, virus y otros similares;
9. Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas, intercambio de la información a nivel interno y externo, incluido el correo electrónico de uso personal, tanto a nivel local como remoto, y sobre los canales electrónicos;
10. Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas; y
11. Efectuar pruebas o evaluaciones de vulnerabilidad e intrusión sobre los componentes de infraestructura de tecnología. Estos deberán realizarse una vez al año y cuando existan cambios en la infraestructura referida. Dichas actividades serán documentadas de acuerdo a lo dispuesto en el artículo 23 de las presentes Normas.

**Adquisición, desarrollo y mantenimiento de sistemas informáticos**

1. 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:
2. Incluir controles al ingreso, acceso, transmisión, procesamiento y salida de información;
3. Aplicar las técnicas de cifrado que garanticen efectivamente la protección del almacenamiento y transporte de la información crítica de la entidad;
4. Definir controles sobre la implementación de aplicaciones antes del ingreso a producción;
5. Controlar el acceso al código fuente de los sistemas informáticos desarrollados ya sea por la entidad o por terceras partes;
6. 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;
7. Controlar y analizar las vulnerabilidades técnicas existentes en los sistemas informáticos de la entidad, tanto durante su puesta en producción, ya sea en nuevos sistemas o cuando se hayan efectuado cambios a los mismos y, cuando dichos sistemas se encuentren en producción. Deberá efectuarse este tipo de análisis por lo menos dos veces al año y establecer los procedimientos de corrección adecuados; y
8. Establecer un procedimiento de instalación de actualización de software, con el objeto de prevenir vulnerabilidades ante el riesgo de finalización de soporte de parte del fabricante.

Si derivado de las actividades establecidas en el artículo 10 de las presentes Normas, las entidades determinen 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 estén relacionados a aquellos que la entidad ofrece a sus clientes, deberán presentar a la Junta Directiva o quien haga sus veces, la información siguiente:

1. Estudio de factibilidad técnica y financiera;
2. Requerimientos técnicos;
3. Estudio de las características de la plataforma actual;
4. Potenciales riesgos asociados a la sustitución o reemplazo del sistema informático principal;
5. Mecanismos de mitigación y contingencia en caso de materializarse los riesgos a que se refiere el literal anterior;
6. Ventajas y desventajas asociadas a la sustitución, reemplazo o adquisición del sistema informático;
7. Justificación de la actividad a realizar; y
8. Análisis y conclusiones de las ofertas de los proveedores.

La Junta Directiva en consideración a la documentación mencionada anteriormente, resolverá sobre la necesidad de realizar reemplazos, sustituciones o adquisiciones dejando constancia de su decisión en el Acta de Sesión correspondiente. Posteriormente, la entidad deberá notificarlo a la Superintendencia previamente a iniciar el proceso de contratación, desarrollo o adquisición de dichos sistemas.

Previo a que la entidad implemente las sustituciones o nuevas adquisiciones y cuando las pruebas internas de la misma hayan sido finalizadas y certificadas por los usuarios, deberán notificarlo a la Superintendencia, a fin de que la misma efectúe las pruebas que considere necesarias, para lo cual tendrá como plazo máximo 60 días calendario.

De haber observaciones como resultado de las pruebas realizadas por la Superintendencia, ésta se lo notificará a la entidad respectiva para que ésta última subsane dichas observaciones.

Para el caso de que las entidades necesiten sustituir programas informáticos críticos, se deberán mantener en paralelo con los programas informáticos en uso durante un tiempo prudencial definido por la entidad.

**Procesamiento, procedimientos de respaldo y restauración de la información**

1. 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.

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 5 días hábiles posteriores al haberse iniciado operaciones o cuando ocurra un cambio de ubicación de los mismos.

**Ubicación del centro de datos principal y sitio alterno de la información**

1. Las entidades deben informar a la Superintendencia la ubicación específica de su centro de datos principal, 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 sitio alterno de la información deberá demostrar a la Superintendencia el cumplimiento de los requisitos establecidos en el Anexo No. 1 de las presentes Normas.

Recibida completa la documentación y de haber observaciones a esta, la Superintendencia se lo notificará a la entidad respectiva para que esta subsane dichas observaciones.

**Gestión de incidentes de seguridad de la información y de ciberseguridad**

1. Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, las entidades deben considerar al menos los aspectos siguientes:
2. 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
3. Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

**Tercerización de operaciones o actividades**

1. 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 operaciones o actividades de tecnología de la información, deberán verificar que las empresas proveedoras de servicios de procesamiento y almacenamiento de datos, cumplan los criterios contenidos en las presentes Normas y lo establecido en el Anexo No 1.

Las operaciones tercerizadas deben ser formalizadas con un contrato vigente firmado por ambas partes. 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, en el contrato debe 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.

Las entidades que deseen contratar servicios de una nube privada, relacionados con productos y servicios financieros que esta ofrece, serán siempre las responsables en última instancia de la integridad, disponibilidad y confidencialidad de la información que se manipule en dichos modelos de servicios.

Las entidades que deseen contratar servicios de computación en la nube en la modalidad de nube híbrida, podrán realizarlo siempre y cuando sea la misma entidad la que gestione en una nube privada la información de sus clientes que esté relacionada con los productos y servicios financieros que ofrece. La demás información podrá alojarla o procesarla en una nube pública.

Las entidades podrán contratar servicios de una nube pública sólo para gestionar información que no esté relacionada a datos del cliente o productos y servicios financieros que la entidad ofrece.

**Conglomerados financieros**

1. 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 la entidad bancaria 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 plan 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 plan de seguridad de la información.

La unidad de seguridad de la información 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, las regulaciones locales y las de su casa matriz.

Los informes elaborados por la unidad de seguridad de la información de la casa matriz que sean recibidos por el banco, deberán hacerse del conocimiento de la Superintendencia, de conformidad a lo establecido en el artículo 23 de las presentes Normas.

**CAPÍTULO IV**

**GESTIÓN DE LA CIBERSEGURIDAD**

**Generalidades**

1. Las entidades deben contar con políticas, procedimientos, recursos técnicos y humanos para gestionar efectivamente el riesgo de ciberseguridad. Por lo que, deberán adoptar las medidas necesarias en materia de ciberseguridad.
2. La Junta Directiva de la entidad deberá aprobar una política de ciberseguridad, la cual, debe contener principios, procedimientos y lineamientos para la gestión y riesgo de ciberseguridad en la entidad. Esta política debe tener, al menos, las características siguientes:
3. Documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad; y
4. Establecer las tareas o actividades necesarias para la función de ciberseguridad.
5. La entidad debe establecer principios y lineamientos para promover una cultura de ciberseguridad que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes dentro de la política de ciberseguridad. Estas actividades deben realizarse periódicamente y pueden incluirse, adicionalmente, en los cursos sobre riesgo operativo que realice la entidad.

**Función de Ciberseguridad**

1. Para una gestión efectiva del riesgo de ciberseguridad, la entidad debe implementar una función de ciberseguridad, la cual, deberá cumplir como mínimo, con lo siguiente:
2. Se debe conformar considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de clientes, evaluación del riesgo y servicios prestados por la entidad;
3. Realizar una gestión del riesgo de ciberseguridad en coordinación con la función de seguridad de la información de la entidad;
4. Reportar a la Junta Directiva y a la Alta Gerencia, los resultados de su gestión, especialmente en la evaluación que haga de la confidencialidad, integridad y disponibilidad de la información, 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;
5. 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;
6. Sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas;
7. Será responsable en el monitoreo y verificación del cumplimiento de las políticas y procedimientos que se establezcan en materia de ciberseguridad, sin perjuicio a aquellas tareas que realiza la auditoría interna;
8. 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;
9. Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de una UCI, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán;
10. Sugerir los presupuestos de ciberseguridad. Dichos presupuestos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información;
11. Sin perjuicio de las actividades que debe realizar la función de ciberseguridad de la que trata el presente Capítulo, las funciones de gestión de riesgos relacionadas con respuesta a incidentes podrán ser desagregadas en diferentes áreas de la entidad.

**Controles**

1. La entidad debe implementar controles para mitigar los riesgos que pudieran afectar la seguridad de la información en tránsito y la que esté almacenada. Asimismo, emplear mecanismos para la adecuada autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información y ciberseguridad.

**Comunicación de incidentes de ciberseguridad a la Superintendencia**

1. La entidad deberá establecer una estrategia de notificación y comunicación que contemple, como mínimo, lo siguiente:
2. Información que reportará a la Superintendencia, sobre incidentes de ciberseguridad que afecten de manera significativa la confidencialidad, integridad o disponibilidad de la información de la entidad, haciendo una breve descripción del incidente, su impacto y las medidas adoptadas para gestionarlo; y
3. Información que reportará a sus clientes y usuarios de servicios financieros, sobre incidentes cibernéticos que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para remediar la información.

**Cobertura de riesgos**

1. La entidad, deberá incluir en los contratos que se celebren con terceros críticos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de ciberseguridad. 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.
2. La entidad podrá evaluar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.

**Etapas del proceso de gestión de riesgos de ciberseguridad**

1. Las entidades deberán contar con un proceso continuo documentado para la gestión de los riesgos de ciberseguridad, para lo cual deberá contemplar, al menos, las etapas siguientes:
2. **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:
3. 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;
4. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información;
5. Gestionar y documentar la seguridad de la plataforma tecnológica;
6. Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación;
7. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos;
8. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos;
9. Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un sistema ISAE;
10. Monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad; y
11. Informar a los clientes y usuarios de servicios financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad;
12. **Protección y detección:** En esta etapa**, l**as entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento 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:
13. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten;
14. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio; y
15. Realizar un monitoreo continuo de la infraestructura tecnológica de la entidad con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad;
16. **Respuesta y comunicación:** 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:
17. Establecer procedimientos de respuesta a incidentes cibernéticos 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;
18. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados;
19. 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; y
20. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades pertinentes puedan realizar las investigaciones correspondientes;
21. **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:
22. Ajustar sus sistemas de gestión de riesgo, seguridad de la información y ciberseguridad como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes; y
23. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la misma y con las entidades de su sector financiero.

**CAPÍTULO V**

**OTRAS DISPOSICIONES Y VIGENCIA**

**Privacidad de la información**

1. Las entidades deben adoptar medidas que aseguren la privacidad de la información bajo su responsabilidad, lo que incluye la información sensible que reciben de sus clientes, usuarios de servicios, proveedores, entre otros; sin perjuicio a lo establecido en el marco legal vigente.

**Documentación**

1. Las entidades deben presentar a la Superintendencia, dentro de los primeros ciento veinte (120) días calendario siguientes al cierre de cada ejercicio anual, un informe relativo a su SGSCI.

El informe deberá contener como mínimo lo siguiente:

1. Las estrategias y principales políticas utilizadas para la gestión de la seguridad de información y de la ciberseguridad;
2. Principales características de la estructura del SGSCI;
3. El plan de seguridad de la información y de ciberseguridad;
4. El resultado del programa de pruebas de los planes de continuidad;

Detalle de los responsables de la función de seguridad de la información y de ciberseguridad.

**Auditoría Interna**

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

**Auditoría Externa**

1. La Auditoría Externa deberá incluir en sus planes anuales de trabajo, la evaluación de la gestión de la seguridad de la información y deberá informar oportunamente a la Junta Directiva, a la Alta Gerencia y al Comité de Riesgos o quien haga sus veces, sobre cualquier asunto que sea de su conocimiento en relación con la seguridad de la información de la entidad.

**Contrataciones posteriores a la entrada en vigencia**

1. 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 literal d) del artículo 15 de las presentes Normas.

**Plan de Adecuación**

1. Las entidades, para cumplir las disposiciones establecidas en las presentes Normas, deberán presentar a la Superintendencia un plan de adecuación, dentro de los treinta días siguientes a la vigencia de las presentes Normas. Una vez presentado el plan, las entidades deberán implementarlo en un plazo máximo de once meses contados a partir de su presentación.

**Sanciones**

1. 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.

**Derogatorias**

1. Las presentes Normas, derogan los Instructivos siguientes:
   1. El “Instructivo de Informática para las Instituciones Fiscalizadas por la Superintendencia de Pensiones” (SP No. 01/98), aprobado el cuatro de febrero de mil novecientos noventa y ocho, por la Superintendencia de Pensiones, cuya Ley Orgánica se derogó por Decreto Legislativo No. 592 que contiene la Ley de Supervisión y Regulación del Sistema Financiero, publicada en Diario Oficial No. 23, Tomo No. 390, de fecha 2 de febrero de 2011; y
   2. Las “Normas Mínimas de Seguridad Informática de Sociedades Especializadas en el Depósito y Custodia de Valores” (RS-DC.23/2002), aprobadas el catorce de octubre del año dos mil dos por el Superintendente de Valores, cuya Ley Orgánica se derogó por Decreto Legislativo No.592 que contiene la Ley de Supervisión y Regulación del Sistema Financiero, publicada en el Diario Oficial No.23, Tomo No. 390, de fecha 2 de febrero de 2011.

**Disposición especial**

1. A partir de la fecha de entrada en vigencia de las presentes Normas, quedarán sin efecto las disposiciones contenidas en el Reglamento de Tecnología y Sistemas de Información para el Sistema de Ahorro para Pensiones y Sistema de Pensiones Público, emitido por el Presidente de la República mediante Decreto Ejecutivo número 116, de fecha 10 de noviembre de 1997 y publicado en el Diario Oficial No. 214, Tomo 377, del 17 de noviembre de 1997.

**Aspectos no previstos**

1. Los aspectos no previstos en temas de regulación en las presentes Normas serán resueltos por el Comité de Normas del Banco Central de Reserva de El Salvador.

**Vigencia**

1. Las presentes Normas entrarán en vigencia a partir del día XX de XXXX del dos mil diecinueve.

Anexo No. 1

**REQUISITOS PARA TERCERIZAR ACTIVIDADES U OPERACIONES DE TECNOLOGÍA DE INFORMACIÓN**

La entidad que desee iniciar una relación contractual con algún proveedor para efectos de tercerizar actividades u operaciones de tecnología de la información, deberá realizar la debida diligencia de dicho proveedor sobre su solidez financiera, reputación, capacidades administrativas, técnicas y operativas en relación con los servicios a ser tercerizados, cumpliendo con lo siguiente:

1. Información general
   1. Sobre el proveedor: Razón social y giro del negocio; experiencia {servicios, clientes, periodos de servicio); estados financieros de los dos últimos años; accionistas y principales funcionarios.
   2. Declaración Jurada en la que se confirma no existencia de conflicto de interés entre la entidad y el proveedor.
   3. Servicios u operaciones de tecnología de información que planean tercerizar y el tipo de información a ser procesada.
   4. Ubicación (país y ciudad u otro dato de ubicación espacial) de los centros de procesamiento del proveedor.
   5. Fortalezas o razones para la selección del proveedor.
   6. 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.
   7. Previo a la tercerización se deberá realizar una evaluación de riesgos a efecto de identificar aquellos riesgos relevantes derivados de los servicios contratados (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.
   8. Dicho análisis deberá ser realizado por la Unidad de Riesgos de la entidad y deberá ser de índole técnica, legal, reputacional y financiero.
   9. Equipos y aplicaciones que planean estar a cargo del proveedor.
   10. Procedimiento planeado de comunicación entre el proveedor y la entidad.
2. Se deben incluir en los contratos al menos las clausulas sobre los siguientes aspectos:
3. 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.
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 garantice 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

1. Definición de procedimientos de control, revisión y monitoreo de los servicios prestados, así como el procedimiento de escalamiento.
2. Obligación de establecer acuerdos de no revelación a ser firmados por los empleados del proveedor y otras personas ajenas al mismo.
3. Disposiciones sobre la propiedad de la información y la propiedad intelectual.
4. Establecer la disponibilidad sin restricciones del acceso a las instalaciones físicas del proveedor, y de forma directa a todos los datos sobre sus operaciones, en tiempo real, con fines de supervisión conforme artículo 32 de la Ley de Supervisión y Regulación del Sistema Financiero.
5. Confidencialidad de la información durante la vigencia del contrato y posteriormente, en caso de terminación del mismo.
6. Cumplimiento de la legislación y regulación vigente y aplicable, respecto la protección de datos y confidencialidad de la información.
7. Garantía de devolución y destrucción de la información involucrada en la prestación del servicio en caso de terminación del contrato.
8. Indemnizaciones para mitigar los impactos ocasionados por posibles deficiencias del proveedor del servicio.
9. Mecanismos de indemnización por medio de los cuales la entidad y/o el proveedor responderán por afectación a la seguridad de la información, en beneficio de los clientes.
10. Que el proveedor efectúe un análisis de riesgos (de tipo legal, reputacional y financiero) para el caso de realizar subcontrataciones para los servicios críticos prestados; además, cuando sea aplicable, debe 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.
11. El proveedor y el subcontratista, si hubiere, deberán garantizar a la Superintendencia el acceso y disposición de los datos o información relacionada con el servicio tercerizado sin restricciones; 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.
12. Establecer la ubicación física donde serán resguardados los datos.
13. Contar con el análisis documentado que justifique y soporte la decisión de utilizar uno o más proveedores de servicios críticos o funciones operacionales importantes.
14. Realizar una debida diligencia del proveedor y del servicio que considere, entre otros aspectos, el prestigio y experiencia del proveedor en el servicio, la adherencia a estándares internacionales reconocidos para la provisión y gestión de servicios de Tecnología de Información, seguridad de la información (incluyendo la ciberseguridad), la continuidad del negocio y la calidad del servicio; debiendo presentar evidencia de las garantías o certificaciones independientes que hayan sido otorgadas en cumplimiento a estándares internacionales.
15. La entidad deberá llevar a cabo una evaluación sobre la gestión de la seguridad de la información del proveedor del servicio.
16. La entidad debe verificar que los planes de continuidad y los recursos del proveedor sean los adecuados para garantizar la continuidad del servicio, así mismo verificar la capacidad para recuperar y reanudar el servicio ante interrupciones.
17. Definición de expectativas con respecto a la manipulación, el uso, el almacenamiento y la disponibilidad de la información, y especificar los compromisos de cada parte para la continuidad del negocio y la recuperación de desastres.

Anexo No. 1

1. La entidad deberá establecer procedimientos de respuesta, los cuales deben ser transparentes, para compartir información con la Superintendencia, durante y después de un incidente.
2. La entidad debe asegurarse de 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. Establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los servicios brindados por terceros y verificar periódicamente su cumplimiento.
4. Se deberán establecer los procesos a ser aplicados en caso de resolución o intervención, que considere la participación en lo concerniente del proveedor del servicio. Se deben documentar los mecanismos para garantizar que la Superintendencia tenga acceso a los datos y a las instalaciones en caso de resolución o intervención.
5. En el caso de contratación de servicios relativos a centros de datos, donde los equipos en los que se almacenara la información de la institución financiera sean propiedad del proveedor que brindara el servicio, la institución financiera deberá poner a disposición de la Superintendencia un mecanismo para llevar a cabo labores de supervisión de forma remota, de forma inmediata cuando esta lo considere conveniente y oportuno.
6. Establecer en los planes anuales de auditoria de la entidad, el alcance, forma y periodicidad de las revisiones de auditoria de sistemas considerando el nuevo esquema de procesamiento principal de la entidad.