SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO IV
DEBERES Y RESPONSABILIDADES

CAPÍTULO V:
REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

CONTENIDO

SUPERINTENDENCIA FINANCIERA DE COLOMBIA

PARTE I
INSTRUCCIONES GENERALES APLICABLES A LAS ENTIDADES VIGILADAS

TÍTULO IV
DEBERES Y RESPONSABILIDADES

CAPÍTULO V:
REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

1. ÁMBITO DE APLICACIÓN

Las instrucciones de que trata el presente Capitulo deben ser adoptadas por las entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia (SFC) y operadores de información de la PILA, con excepción del Fondo Nacional de Garantías (FNG), Fondo Financiero de Proyectos de Desarrollo (FONADE), los Almacenes Generales de Depósito, los Fondos de Garantía que se constituyan en el mercado de valores, los Fondos Mutuos de Inversión, los Fondos Ganaderos, las Sociedades Calificadoras de Valores y/o Riesgo, las Oficinas de Representación de Instituciones Financieras y de Reaseguros del Exterior, los Corredores de Seguros y de Reaseguros, los Comisionistas Independientes de Valores, las Sociedades Comisionistas de Bolsas Agropecuarias y los Organismos de Autorregulación. En todo caso, las entidades exceptuadas deben hacer periódicamente una autoevaluación del riesgo de ciberseguridad y seguridad de la información, que incluya una identificación de las mejoras a implementar en su Sistema de Administración de Riesgo Operativo.

Los resultados de la autoevaluación, así como el plan de acción para implementar los ajustes a que haya lugar, deben estar a disposición de la SFC.

2. DEFINICIONES

Para efectos del presente Capítulo, se establecen las siguientes definiciones:

2.1. Activo de información

Conocimiento o datos que tienen valor para la entidad o el individuo.

2.2. Ciberamenaza o amenaza cibernética

Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.

2.3. 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 comisión de un crimen.

2.4. 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.

2.5. Ciberiesgo o riesgo cibernético

Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos.

2.6. Ciberseguridad

Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

2.7. CSIRT (*Computer Security Incident Response Team*)

Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.

2.8. Evento de ciberseguridad

Ocurrencia de una situación que podría afectar la protección o el aseguramiento de los datos, sistemas y aplicaciones de la entidad que son esenciales para el negocio.

2.9. 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.

2.10. Información en reposo

Datos guardados en dispositivos de almacenamiento persistente (por ejemplo, cintas, copias de seguridad externas, dispositivos móviles, discos duros, entre otros).

2.11. 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.

2.12. 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.

2.13. Seguridad de la información

Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad.

2.14. SIEM (*Security Information and Event Management*)

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. Suelen ser sistemas de centralización de *logs*.

2.15. SOC (*Security Operation Center*)

Unidad encargada de monitorear, evaluar y defender los sistemas de información empresarial (sitios web, aplicaciones, bases de datos, centros de datos, servidores, redes, escritorios y otros dispositivos).

2.16. Terceros críticos

Terceros con quien se vincula la entidad y que, de acuerdo con los parámetros establecidos por la propia entidad, pueden tener incidencia directa en la seguridad de su información.

2.17. 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.

3. OBLIGACIONES GENERALES EN MATERIA DE CIBERSEGURIDAD

Las entidades deben contar con políticas, procedimientos y recursos técnicos y humanos necesarios para gestionar efectivamente el riesgo de ciberseguridad. En ese sentido, deben adoptar, como mínimo, las medidas que se relacionan a continuación en materia de ciberseguridad:

3.1. Establecer una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad en la entidad. Esta política debe tener las siguientes características:

3.1.1. Ser aprobada por la junta directiva.

3.1.2. Documentar las responsabilidades, procesos, procedimientos, etapas y la gestión que se realiza frente a la ciberseguridad.

3.1.3. Establecer las funciones de la unidad de seguridad de la información y la ciberseguridad.

3.1.4. Establecer los 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.

3.2. Establecer una unidad que gestione los riesgos de seguridad de la información y la ciberseguridad. Esta unidad debe tener, al menos, las siguientes características y responsabilidades:

3.2.1. 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.

3.2.2. Debe realizar una gestión efectiva de la seguridad de la información y la ciberseguridad en la entidad.

3.2.3. Debe reportar a la junta directiva y a la alta dirección, 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.

3.2.4. Debe 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.

3.2.5. Debe sugerir las capacitaciones que deben recibir regularmente los funcionarios de la entidad en temas relacionados con ciberseguridad y mantenerlos actualizados sobre las nuevas ciberamenazas.

3.2.6. Ser la principal 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.

3.2.7. Asesorar a la alta gerencia y la junta directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que estas últimas puedan hacer seguimiento y tomar las decisiones adecuadas en esta materia.

3.2.8. Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un SOC, que puede ser manejado desde el exterior. El análisis debe identificar las características del proveedor y herramientas y servicios que se contratarán.

3.2.9 Sugerir los presupuestos de seguridad de la información y ciberseguridad. Dichos presupuestos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.

3.2.10. Verificar el cumplimiento de las obligaciones contenidas en el Capítulo I del Título II de la Parte I de la CBJ, en lo que sea pertinente con sus funciones.

3.2.11. Debe realizar las demás actividades establecidas en este Capítulo que por su naturaleza les sean asignadas

Sin perjuicio de las funciones que debe realizar la unidad de la que trata este subnumeral 3.2., las funciones de gestión de riesgos relacionadas con respuesta a incidentes pueden ser desagregadas en diferentes áreas de la entidad.

3.3. Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (*Information Security Forum*), CIS *Critical Security Controls* (CSC) o *Cobit 5 for Information Security,* y sus respectivas actualizaciones.

3.4. Implementar controles para mitigar los riesgos que pudieran afectar la seguridad de información confidencial, en reposo o en tránsito.

3.5. 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.

3.6. Establecer procedimientos para la retención y destrucción final de la información, sin que se desconozca lo establecido en el Artículo 96 del EOSF y demás normas aplicables.

3.7. Establecer una estrategia de comunicación e información que contemple los siguientes ejes, sin perjuicio de las obligaciones de reporte a la SFC y demás autoridades de acuerdo con la normatividad aplicable:

3.7.1. Información que reportará a la SFC, 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.

3.7.2. Información que reportará a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos, sobre incidentes cibernéticos.

3.7.3. Información que reportará a los consumidores financieros, sobre incidentes cibernéticos que hubiesen afectado la confidencialidad o integridad de su información, así como las medidas adoptadas para remediar la información.

3.8. Incluir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y *apps*, que procesan la información confidencial de la entidad o de los consumidores financieros (desde las etapas iniciales tales como levantamiento de requerimientos hasta las pruebas de seguridad pertinentes y producción), aspectos relativos con la seguridad de la información que permitan mitigar dicho riesgo.

3.9. 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 seguridad de la información y ciberseguridad.

3.10. Verificar periódicamente el cumplimiento de las obligaciones y medidas establecidas conforme al subnumeral 3.9. de este Capítulo, para lo cual pueden implementar los mecanismos adecuados para el efecto.

3.11. Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad.

3.12. Gestionar la seguridad de la información y la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

3.13. Considerar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.

4. ETAPAS

Para la gestión de la seguridad de la información y la ciberseguridad las entidades deberán considerar, como mínimo, las siguientes etapas:

4.1. 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 cuando menos:

4.1.1. 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.

4.1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.

4.1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.

4.1.4. La unidad de la que trata el subnumeral 3.2. de este Capítulo debe contar con los recursos necesarios para realizar una adecuada gestión de la seguridad de la información y la ciberseguridad.

4.1.5. 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.

4.1.6. 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.

4.1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques cibernéticos.

4.1.8. Contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.

4.1.9. De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

4.1.10. Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.

4.1.11. Informar a los consumidores financieros de la entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

4.2. Protección y detección

Las 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. Las entidades deben:

4.2.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.

4.2.2. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad.

4.3. 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 deben:

4.3.1. 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.

4.3.2. Evaluar los elementos de la red para identificar otros dispositivos que pudieran haber resultado afectados.

4.3.3. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los ataques cibernéticos que requieran de su gestión.

4.3.4. Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

4.3.5. En la medida de lo posible, preservar las evidencias digitales para que las áreas de seguridad o las autoridades puedan realizar las investigaciones correspondientes.

4.4. Recuperación y aprendizaje

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. Las entidades deben:

4.4.1. 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.

4.4.2. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.