# Plan Sectorial de Protección y Defensa

## para la Infraestructura Crítica Cibernética del Sistema Financiero

2018

# Contenido

## RESUMEN

El presente plan define los lineamientos generales que deben adoptar los diversos actores, dueños y operadores de las infraestructuras críticas cibernéticas (ICC) del sector financiero colombiano, el cual está compuesto tanto por entidades del sector privado, principalmente las bancarias agrupadas en ASOBANCARIA, FASECOLDA, ASOFIDUCIARIAS, ASOBOLSA; y las entidades públicas del sector hacienda, conformadas por el Ministerio de Hacienda y sus entidades adscritas y vinculadas, así como Banco de la República, Superintendencia Financiera de Colombia y los actores fundamentales en el desarrollo de este plan.

Este documento busca ser un compendio de lineamientos y buenas prácticas para todo el sector financiero, orientado a definir una hoja de ruta para trabajar de manera conjunta entre gobierno y sector financiero ante ataques cibernéticos o incidentes que afectan la prestación de servicios esenciales específicos del sector. Reconociendo que, para lograr una estrategia efectiva de la ICC, es necesario establecer las interdependencias que se tengan entre sectores.

Para este fin, el documento establece una serie de objetivos asociados a la resiliencia sectorial ante incidentes de ciberseguridad, mediante técnicas de acción, mecanismos sectoriales de cooperación, los protocolos de comunicación y divulgación, así como la hoja de ruta para la identificación y acción de incidentes cibernéticos al interior del sector y entre sectores. Estos mecanismos y herramientas de acción buscan ser coherentes con las estrategias internas de atención y respuestas a incidentes, lo que se garantiza gracias al permanente diálogo entre diferentes actores del sector financiero.

Es importante señalar que el documento busca articular las acciones que la iniciativa privada venga fortaleciendo en materia de riesgos digitales y resiliencia, con la política pública que el Comando Conjunto Cibernético (CCOCI) lidera a nivel nacional en materia de ciberdefensa y ciberseguridad. Adicionalmente, el documento incluye los principales lineamientos que a nivel regulatorio la Superintendencia Financiera de Colombia y la Superintendencia Solidaria han reglamentado en temas de seguridad de la información y ciberseguridad. Garantizando que las acciones aquí consignadas estén en coherencia con el marco legal y constitucional de acción.



**Palabras clave:** atención a incidentes cibernéticos, interdependencias sectoriales, servicios esenciales, Infraestructuras Críticas Cibernéticas (ICC), resiliencia cibernética, protocolo de respuesta.

# INTRODUCCIÓN

La globalización y el uso de las Tecnologías de la Información y las Comunicaciones (TIC) y las tecnologías de operación (TO), han incidido de manera fundamental en el desarrollo económico de los últimos años. Las últimas décadas se han consolidado como el periodo de mayor innovación para distintas industrias, gracias al importante proceso de incorporación de TI y TO en servicios y procesos. Como se anticipaba, las nuevas tendencias tecnológicas vienen propiciando cambios fundamentales en la forma en que las industrias se articulan con la economía; lo que redunda en importantes beneficios para la economía del país, al consolidar la migración del aparato productivo a ecosistemas de innovación que aprovechan los beneficios de la economía digital.

La economía digital ha promovido el desarrollo de distintos sectores económicos y ha consolidado la formalización de logros económicos y sociales, que redundan en mayor crecimiento económico y en la reducción de la pobreza (Cepal, 2013a). La estrategia de desarrollo y promoción de la economía digital en el país ha estado acompañada por un renovado marco regulatorio, que busca afianzar las capacidades del aparato productivo de apropiarse de las tecnologías de la información, articulando y afianzado las oportunidades de la convergencia tecnológica.

Las anteriores se suman a otras políticas asociadas sobre todo a la inversión en infraestructura en telecomunicaciones, la cuales promueven el acceso y la demanda por internet. En la actualidad el país viene mejorando el acceso y cobertura de la provisión de Banda Ancha y otros bienes públicos asociados a la conectividad. De acuerdo con MinTIC (2018), la tasa de penetración registrada en 2016 fue de 32.5%, donde el 91.9% de la población con acceso a internet se ha visto beneficiada de los programas de acceso cobijados por el gobierno nacional. Por lo cual, el reto de mejorar la calidad y la cobertura de la conectividad continua vigente (ver Gráfico 1).


**Gráfico 1. Tasas de penetración de banda ancha (%) Total Nacional[1]**

Un aspecto fundamental en la consolidación de la economía digital se trata de la seguridad. Por un lado, la incorporación de las TIC en el sector privado involucra distintas fases. Aquellas fases más maduras se caracterizan por mayores niveles de productividad y de una mayor conciencia sobre la necesidad de fortalecer la seguridad digital. A la vez que

[1] Gráfico extraído de Colombia TIC, Documento MinTIC 2016. Diponible en:

deben afianzarse Políticas de Estado que presten atención a las amenazas de seguridad y privacidad (Cepal, 2013b). En este sentido, la correcta articulación entre sector privado y público resulta clave para consolidar y profundizar la economía digital en el contexto nacional, es decir, contar con una adecuada gobernanza digital para Colombia.

La ciberseguridad resulta fundamental para el desarrollo de la economía digital, considerando que permite generar los vinculos de confianza necesarios para garantizar una conectividad fluida. Sobre este punto, la OEA (2016) indica que con la profundización de la economía digital, los riesgos cibernéticos son cada vez más preocupantes y se están convirtiendo en un factor de mayores consideraciones en seguridad y formulación de políticas económicas, "*la conciencia de seguridad cibernética ha ido creciendo a medida que se ha reconocido que las amenazas y vulnerabilidades tienen el potencial de frenar la innovación y el avance de la economía basada en Internet, a la vez que ponen en riesgo a los individuos y las organizaciones*". El diagnóstico general entregado porla OEA para los países latinoamericanos es que necesitan mejorar su estrategia nacional en seguridad, lo cual involucra un adecuado marco jurídico nacional, capacidades técnicas, recursos humanos y la articulación de estado y privados para establecer un entorno digital seguro.

Un reto fundamental para afianzar los objetivos del desarrollo de la economía digital es fortalecer resiliencia en la era de la economía digital. Son claros los beneficios de la conectividad y de la integración tecnológica a nivel económico y social, pero si se tienen en cuenta los costos asociados a la interrupción del (de los) servicio (s), el delito electrónico, el robo de identidad, el robo de propiedad intelectual, el fraude y otras actividades de impacto negativo; los beneficios que empiezan a cuestionarse facilmente. En este sentido, "…*si los países no invierten por igual en la seguridad de su infraestructura básica y la resistencia de sus sistemas, los costos impuestos por las actividades cibernéticas nefastas gravarán su crecimiento económico*.."

Conforme con esta necesidad, las organizaciones han empezado a invertir más recursos en fortalecer sus capacidades contra atqques cibernéticos. A su vez, los gobiernos enfrentan aún más retos en materia de ciberseguridad, principalmente debido a que se enfrentan a amenazas contra la seguridad nacional, lo que implica mayores retos y el desarrollo de estrategias transversales que involucran a un amplio conjunto de sectores económicos. Basado en lo anterior es fundamental adoptar un marco de política que permita articular los esfuerzos institucionales, estatales y privados en configurar una estrategia de seguridad a nivel nacional sectorial. Por ejemplo, el desarrollo de capacidades nacionales de respuesta a incidentes para el intercambio y gestión de amenazas cibernéticas a nivel sectorial y nacional. Esto sumado al diseño de políticas bien definidas que comprometan al gobierno y a la industria en acciones reglamentadas por un marco jurídico apropiado. Adional a la necesidad de vincular un adecuado marco penal, que logre desincentivar oportundamente las ganancias del crimen organizado.

Sin duda, el país ha apostado por consolidar un marco de políticas para abonar terreno en este frente.Desde el Viceministerio de Economía Digital del Ministerio de Tecnologías de Información y Comunicaciones (MinTIC) se viene promoviendo la generación de capacidades y emprendimiento en Tecnologías de Información y Comunicaciones (TIC) y la migración de los modelos de negocio a esquemas digitales, agenda en la cual los servicios financieros ocupan un espacio destacado. En esta misma línea, la Comisión de Regulación en Comunicaciones (CRC) hizo el diagnóstico de las necesidades regulatorias y la hoja de ruta hacia la economía digital del país para los próximos 10 años, reconociendo

la necesidad de contar con un adecuado esquema regulatorio desde las Empresas de Telecomunicaciones, camino normativo que debe iniciar en 2018. Mientras que la Fiscalía General de la Nación ha acelerado y promovido iniciativas de cooperación con distintos sectores para mejorar los procesos de judicialización, donde el sector financiero ha cumplido un lugar destacado.

De manera muy positiva, el Gobierno Colombiano desde hace algunos años ha orientado sus esfuerzos a realizar una política pública orientada a atender las necesidades de ciberseguridad en el país, así como promover la seguridad de la información a lo largo de todos los sectores de la economía. El primer acercamiento de la ciberseguridad y ciberdefensa como política pública en Colombia nace a partir del CONPES 3701 de 2011, con el que se logró fortalecer las capacidades del país en materia cibernética, considerando que la seguridad de la información era un objetivo nacional por cuanto Colombia había sido un foco importante de ataques dirigidos al Gobierno y empresas. Esto se esperaba lograr a través de 3 objetivos específicos (Gráfico 2).


**Gráfico 2. Ejes temáticos Política Pública en Ciberseguridad CONPES 3701/2011**

El problema en ciberseguridad identificado en 2011 era la falta de capacidad del país para responder ante las amenazas cibernéticas, lo que imposibilitaba una buena articulación y disponibilidad de soluciones frente a ataques cibernéticos. La política pública diseñada como respuesta, se orientó a fortalecer las capacidades del Estado en ciberdefensa y a la articulación funcional de organizaciones creadas por el estado responsables de la atención a incidentes cibernéticos a través del desarrollo de un colCERT (Gráfico 3).

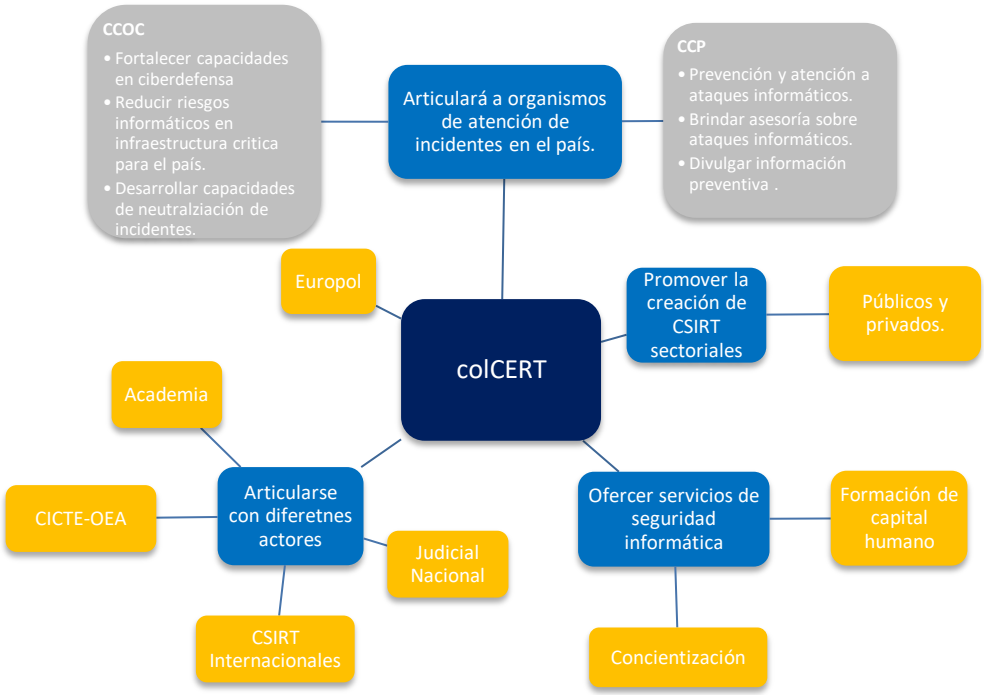


**Gráfico 3. Funcionamiento del colCERT y sus organismos asociados**

Como resultado, el país se convirtió enun referente regional en ciberseguridad y logró mitigar de manera activa los ataques a nivel nacional. Sin embargo, a pesar de que el CONPES fortaleció las capacidades del país, hacia 2016 solo se habían consolidado el 79% de sus iniciativas, por lo que aún había un importante espacio para la mejora de las capacidades del Estado y el sector privado. Para 2016 este diagnóstico reflejaba que colCERT era coordinador de la ciberdefensa y la ciberseguridad, más no representaba *"…una visión global y estratégica en torno a la seguridad digital…"* (CONPES, 2016, p. 33). La capacidad del colCERT, a pesar de tener importantes resultados en materia de detección y atención a incidentes, se veía reducida por cuanto la información a la que acudía era externa y no de manera coordinada con la sociedad.

Un nuevo enfoque de la política pública sobre la ciberseguridad se logró establecer mediante el CONPES 3854 de 2016, el cual señala que la política previa no era suficiente, para la necesidad de enmarcar la ciberseguridad en un entorno de prosperidad económica y derechos humanos. Para lograr este fin, se empezaron a implementar mejores prácticas internacionales que coinciden en que la mejor forma de integrar una estrategia eficaz en ciberseguridad era mediante un enfoque de gestión de riesgos de ciberseguridad (CONPES, 2016, p. 19), pasando *"…del diseño de estrategias de ciberseguridad y ciberdefensa, que se centran principalmente en objetivos de defensa y seguridad nacional en el entorno digital, hacia el diseño de estrategias integrales con un conjunto de principios que se enmarca en la gestión de riesgos de seguridad digital…"* (IBID, p. 20). Mediante este enfoque, es posible diseñar estrategias incluyentes, de carácter colaborativo y donde se comparten responsabilidades que solventan los vacíos mencionados por el CONPES de 2011, y reorienta la política nacional en torno a cinco dimensiones estratégicas (Gráfico 4).


**Gráfico 4. Dimensiones estratégicas de la estrategia en seguridad digital**

A partir del enfoque de la política pública de la ciberseguridad del CONPES 3854 de 2016, se espera que un mayor número de actores económicos hagan uso de las ventajas de las TIC para incorporarse a la economía en contribución a la prosperidad económica nacional. Además, que un entorno digital más seguro, permitirá que se reduzcan las prácticas inseguras de sus usuarios y sus posibilidades de ser víctimas de delitos. Adicionalmente, se refuercen las capacidades de los organismos de previsión e investigación de incidentes, quienes se enfrentan a un número creciente de estrategias delictivas (Gráfico 5).

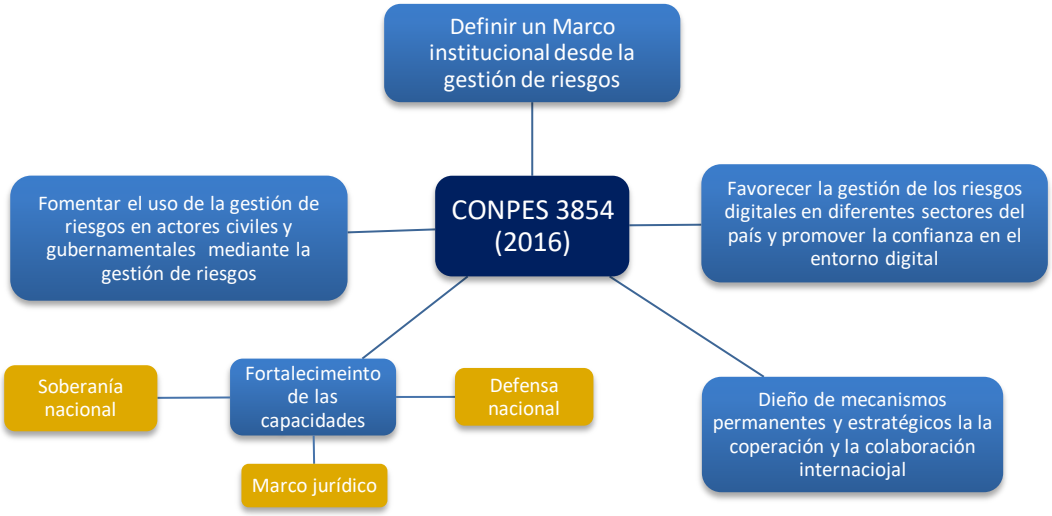


**Gráfico 5. Objetivos Política de Seguridad Digital - Conpes 3854 de 2016**

Por otra parte el marco jurídico es pilar fundamental para la aplicación de políticas y lineamientos. Colombia cuenta con la ley 1273 de 2009, "*..por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías dela información y las comunicaciones, entre otras disposiciones..*"(Ley 1273, 5 de Enero del 2009). Esta Ley nace para ampliar el alcance de la política nacional del país,

que no había tipificado delitos de carácter informáticos en la normativa penal, dificultando el papel de autoridades para perseguir y de las víctimas para denunciar ciberdelitos, orientados a la protección de los datos y la confidencialidad, siguiendo los estándares de la *International Criminal Investigative Training Assistance Program* (ICITAP). Con el propósito de fortalecer aún más la lucha contra los ataques cibernéticos Colombia expidió la ley 1928 del 24 de julio de 2018, con la cual se adhiere al convenio de Budapest, el cual establece una política penal común y armoniza la cooperación internacional. En 2018 se han adherido más de 56 países de todo el mundo, incluyendo a Chile, Costa Rica, República Dominicana, Panamá, Argentina. Paraguay, México y Perú han sido invitados a firmar el acuerdo y están próximos a concretar la adhesión. Los países que implementan el acuerdo tienen la obligación de armonizar su legislación interna a las exigencias penales y judiciales de los demás países, a la vez que deben mejorar los procesos para favorecer el flujo de información.

Desde el sector financiero, las entidades financieras incorporan prácticas internas de ciberseguridad y seguridad de la información, coherentes con la creciente integración de servicios esenciales mediante tecnologías de la información. Más allá de la gestión de los riesgos operacionales, tradicionalmente vinculadas con la gestión de eventualidades y el diseño de controles de contingencia, las áreas dedicadas a la seguridad de la información tenían un panorama técnico que articulaba acciones preventivas y tácticas no estrictamente vinculantes con los riesgos cibernéticos.

Desde los entes regulatorios, la Superintendencia Financiera de Colombia reglamenta las disposiciones en materia de riesgo operacional, mediante la Circular Externa 048 de 2006 a través del Sistema de Administración al Riesgo Operacional (SARO) en Colombia, la cual incorpora los primeros lineamientos referentes a la seguridad de la infraestructura y los procesos informáticos. Mientras que, frente a la seguridad de la información, en el Capítulo I del Título II de la Parte I de la Circular Básica Jurídica se establecen requisitos que deben cumplir las entidades financieras “Canales, medios, seguridad y calidad en el manejo de información en la prestación de servicios financieros”.

En armonía con lo señalado en precedencia, la Superintendencia expidió la circular externa 007 del 5 de junio de 2018, que establece los requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad, instructivo que entra a regir en tres fases, la primera de ellas, a partir del 8 de diciembre de este año. Lo que se suma al Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC, el cual ha sido de gran apoyo y orientación para las entidades públicas. Este permite hacer seguimiento de la implementación de los modelos de riesgos digitales al interior de cada entidad, afianzando las entidades nacionales y territoriales en formación frente a la seguridad digital.

Por su parte, sin ser regulaciones; los estándares y marcos de referencia internacional juegan un papel fundamental dentro del proceso de gestión de la seguridad digital en el sector. En el contexto de la seguridad digital los estándares contribuyen a definir lineamientos y buenas prácticas para la gestión de los incidentes dentro y entre distintas organizaciones (Deutscher y Yin, 2016). Entre las más conocidas están las familias de las ISO 27000, COBIT 5, los esquemas de NIST (*National Institute of Standards and Technology*) y ENISA (European Union Agency for Network and Information Security), o del WEF (World Economic Forum), los estándares ISF (*Information Security Forum*), los SANS Top 20 CIS y finalmente los IT *Capability Maturity Framework*. Por lo cual, la estrategia al interior de las entidades financieras ha sido el fortalecimiento de la arquitectura de

seguridad digital, orientada sobre todo a generar capacidades para defender y anticipar las amenazas digitales.

# CAPÍTULO I: GENERALIDADES

## 1.1. Alcance

Este documento se elaboró dando cumplimiento a lo establecido en la política pública, a través lineamientos generales que deben adoptar los diversos actores dueños y operadores de las infraestructuras críticas al interior del sector financiero colombiano (CCOC, 2016). El documento servirá como guía para articular los esfuerzos del gobierno y sector financiero ante eventos de ciberseguridad que pongan en peligro el funcionamiento de los servicios esenciales y la soberanía del país. Para esto, se incorpora la normativa vigente para el sector financiero por parte de la Superintendencia Financiera de Colombia y otros actores vinculados al sector.

Los lineamientos buscan promover la capacidad de prevenir, preparar, responder y recuperar en los eventos de ciberseguridad. A su vez, incrementar la efectividad de las infraestructuras críticas para hacer frente a un evento potencialmente perturbador. Para lo cual se establecen metas y procedimientos para que el sector financiero logre cumplir con sus responsabilidades como operador de Infraestructuras Críticas Cibernéticas.

Por último, incorporar en la aplicación de prácticas y lineamientos, al sector hacienda pública, cuyo rol en el manejo de los recursos públicos de la Nación, y en la supervisión, vigilancia y control a las entidades del sector financiero y del sector solidario, es de suma importancia a la hora de gestionar crisis e incidentes de ciberseguridad, adicional a la complementariedad natural de los actores públicos y privados que componen el sector financiero.

El Plan Sectorial Financiero de Protección y Defensa de Infraestructura Crítica Cibernética se constituye en un marco general, aplicable tanto para las entidades públicas como privadas que componen el sector financiero, que define y establece los lineamientos, estrategias y un modelo organizacional para la protección y defensa de la Infraestructura Crítica Cibernética que operan y/o administran las entidades del sector financiero, tendiente a la creación de un documento, orientado a establecerles un entorno operativo seguro y resiliente frente a los riesgos digitales, en respeto de los derechos constitucionales, para garantizar los servicios esenciales del Estado que son prestados por las entidades del sector, contribuyendo desde nuestra perspectiva y posición, al desarrollo y gestión del Plan Nacional de Protección y defensa de ICC.

## 1.2. Objetivo general y específicos.

### 1.2.1. Objetivo General

Prevenir los riesgos de seguridad cibernética de las infraestructuras críticas nacionales del sector financiero a través de la definición, socialización y aplicación de lineamientos estratégicos para el fortalecimiento de la ciberseguridad, la ciberdefensa y la adecuada gestión del riesgo tecnológico en dicho sector, buscando como fin último la confianza, resiliencia y monitoreo de los servicios esenciales del país.

### 1.2.2. Objetivos Específicos

- Definir un plan de trabajo con los lineamientos estratégicos en ciberseguridad para entidades del sector financiero consideradas como infraestructura crítica nacional. A la vez que se promueven como buenas prácticas para las entidades que no sean consideradas como infraestructura crítica.

- Definir y establecer un espacio de diálogo sectorial que permita dirigir y coordinar las actuaciones necesarias para proteger las infraestructuras críticas cibernéticas del sector financiero. Con el fin de movilizar y articular las capacidades logísticas, operativas y técnicas para la toma de decisiones y respuesta ante eventos e incidentes cibernéticos y en función de la resiliencia del sector.

- Definir y establecer una estrategia de actualización permanente y de manera especializada para estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar al sector financiero sobre las amenazas, vulnerabilidades y posibles impactos en caso de ataque a una o varias de las infraestructuras críticas nacionales del sector. Las entidades se pueden apoyar en los niveles de seguridad a través de la activación de acciones de respuesta a incidentes por medio de CSIRT sectoriales.

- Establecer una estrategia de comunicación que permita informar los incidentes cibernéticos a las autoridades que hacen parte del modelo nacional de gestión de incidentes cibernéticos como a las entidades designadas dentro del sector financiero, contando con una definición de procedimientos informativos para la prevención, reporte de incidentes, gestión de crisis, respuesta y recuperación para la protección de la infraestructura critica cibernética.

- Fomentar la generación y apropiación de conocimiento basado en la cooperación intersectorial, mejores prácticas y lecciones aprendidas en materia cibernética. Para este fin, se propone que el espacio de discusión sectorial, vincule las estrategias internas en favor de la resiliencia sectorial desde la ciberseguridad.

- Mejorar la capacidad de resiliencia cibernética nacional considerando dentro de las pruebas de los diferentes planes de continuidad de negocio, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos como lo indica la Circular 007 de 2018 de la SFC (2018).

- Generar espacios de cooperación e intercambio de experiencias, prácticas e información sobre incidentes de seguridad entre las entidades públicas y privadas que componen el sector.

- Asignar recursos para fortalecer las competencias de las personas encargadas de la seguridad informática y de la información de todas las entidades del sector público y privado.

## 1.3. Marco Legal

La normatividad que aplica a las entidades del sector financiero, en lo que respecta a la temática de ciberseguridad y seguridad de la información en general, se puede resumir en lo siguiente, haciendo la aclaración que algunos actos normativos son aplicables tanto para entidades privadas como públicas.

**La política pública.**

- CONPES 3701 de 2011: establece "LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA". En resumen, crea las instancias apropiadas para gestionar las amenazas y los riesgos que atentan contra la ciberseguridad y ciberdefensa nacional. Señala la importancia de la capacitación y líneas de investigación en ciberdefensa y ciberseguridad. Establece la legislación en ciberseguridad y ciberdefensa, cooperación internacional y adhesión de Colombia a los diferentes instrumentos internacionales en esta temática. Nota: Los lineamientos que se establecen pueden ser seguidos también por entidades privadas.
- CONPES 3854 de 2016: Establece la "POLÍTICA NACIONAL DE SEGURIDAD DIGITAL". En resumen, incorpora la gestión del riesgo en el entorno digital (modelo). Establece el marco institucional claro en torno a la seguridad digital. Señala las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad. Muestra la importancia del fortalecimiento de la defensa y seguridad nacional en el entorno digital.

**Para entidades privadas.**

- Circular Externa SFC 052 de 2007: por la cual se establecen los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios. ***(Nota:*** *Aplica para entidades vigiladas por la SFC)*
- Ley 1266 de 2008 (Habeas data): Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. *(**Nota**: Aplica para entidades públicas con servicios financieros)*
- Ley 1273 de 2009 (Delitos Cibernéticos): Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1581 de 2012 (Protección de Datos Personales): Por la cual se dictan disposiciones generales para la protección de datos personales.
- ***(Nota: aplica tanto para entidades privadas como entidades públicas).***
- Circular 007 SF de junio de 2018: Imparte instrucciones relacionadas con los requerimientos mínimos para la gestión del riesgo de ciberseguridad. Dentro de la Circular se colocaron marcos de referencia, establecidos en el numeral 3.3 que dice "...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...*". ***(Nota**: Aplica para entidades vigiladas por la SFC)*

- ley 1928 de 2018 (Adhesión Convenio de Budapest): Con la cual se adhiere al convenio de Budapest, el cual establece una política penal común y armoniza la cooperación internacional.

**Para entidades públicas.**

- Ley Estatutaria1581 de 2012: Por la cual se dictan disposiciones generales para la protección de los datos personales (Nota: Aplica tanto para entidades privadas como públicas).
- Decreto 1078 de 2015: Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Incluye formalmente la Estrategia Gobierno en Línea.
- Decreto 1499 de 2017: Crea el Modelo Integral de Planeación y Gestión II e incorpora Seguridad Digital como Política de Desempeño y Gestión Institucional para las entidades públicas.
- Decreto 1008 de junio de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1, del título 9, de la parte 2, del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, estableciendo la Política de Gobierno Digital.
- Adopción del Modelo de Seguridad y Privacidad de la Información (MPSI): en las entidades nacionales y territoriales del sector público.

## 1.4. Aprobación y Clasificación

El Plan Sectorial Financiero de Protección y Defensa para la Infraestructura Crítica Cibernética será aprobado por tres instancias, dado la participación de entidades públicas y privadas:

Junta Directiva de ASOBANCARIA, ASOBOLSA, FASECOLDA para las instituciones financieras participantes.
Comité Sectorial de Gestión y Desempeño Institucional, para las entidades públicas del sector hacienda.
Junta Directiva de Banco de la República, Superintendencia Financiera de Colombia y/o la Superintendencia Solidaria de Colombia.

El documento será de circulación restringida, teniendo acceso solo las entidades participantes o previa autorización.

## 1.5. Gestión y actualización.

La gestión para la actualización, mantenimiento y custodia de lo consignado en este documento, estará a cargo de la ASOBANCARIA, ASOBOLSA, FASECOLDA y del Ministerio de Hacienda y Crédito Público, Superintendencia Financiera de Colombia, así como entidades líderes de la Mesa de Trabajo. Este documento deberá ser revisado como mínimo cada dos años, donde los participantes de la Mesa de Trabajo pueden solicitar cambios y ajustes al mismo, los cuales deben ser revisados y aprobados por la Mesa, antes de generar las actualizaciones respectivas.

# CAPÍTULO II: SERVICIOS ESENCIALES E INTERDEPENDENCIAS

## 2.1. Servicios Esenciales

### 2.1.1. Definición

Conforme a lo establecido en el documento "Guía para la Identificación de Infraestructura Crítica Cibernética del año 2015, se define a un servicio esencial, como el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la educación, la seguridad, el bienestar social y económico de una comunidad, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas. Por otro lado, se denominan servicios esenciales aquellos que son prestados y soportados en su operación por la infraestructura crítica de la nación y que sustentan a la sociedad Colombiana, fungiendo como pilares en el desarrollo de la economía, la seguridad y la salud de nuestra nación (Home Land Security, 2018).

Este documento adopta el concepto de los servicios esenciales del sector financiero y los define como aquellos enfocados en el mantenimiento de las funciones económicas de la sociedad colombiana y en el eficaz funcionamiento del Estado desde el punto de vista financiero y de la política económica, los cuales se definen a continuación.

### 2.1.2. Servicio Esencial o servicios esenciales del Sector Financiero

De acuerdo con lo elaborado en el documento "Sectores Estratégicos de la República de Colombia desde la óptica Cibernética" de 2016, se estableció la tipología de segmentos y servicios esenciales que el sector financiero aporta a la sociedad colombiana. Se establecieron los siguientes servicios esenciales, de acuerdo con la tipología que conforma al sector financiero.

- **Intermediarios Financieros**

    - Recoger (captar) dinero del público por medio de productos y servicios ya establecidos ante la Superintendencia Financiera.
    - Cuenta de Ahorro / Cuenta Corriente.
    - Certificados de Depósito a Término.
    - Convenios de Recaudo.
    - Prestar (Colocar) dinero a través de los productos que tiene el banco ya establecidos ante la Superintendencia Financiera.
    - Tarjetas de Crédito.
    - Créditos de Consumo.
    - Créditos Educativos.
    - Créditos de Vehículo.
    - Créditos hipotecarios o para vivienda.
    - Créditos de libre inversión.
    - Crédito empresarial.
    - Disposición de Efectivo a cuentahabientes.
    - Transacciones de Tesorería en moneda local y/o extranjera.
    - Desarrollo de convenios indicados por el Gobierno (Caso particular para el Banco Agrario).

- **Portafolios de Inversión**

    - Administración de Inversión.
    - Operaciones de Bolsa.

- **Aseguradores e Intermediarios de Seguros y Reaseguros**

    - Seguros Generales.
    - Seguros de Vida.
    - Operaciones de Seguros y Reaseguradoras.

- **Pensiones, Cesantías y Fiduciaria**

    - Cesantías.
    - Pensiones Obligatorias.
    - Pensiones Voluntarias.
    - Fondos Comunes Ordinarios.
    - Fondos Comunes Especiales.
    - Fondos Comunes Especiales en moneda extranjera.
    - Fondos de Pensiones de Jubilación e invalidez Voluntarias.
    - Fondos de inversión o fondo país.
    - Fondos mutuos de inversión.

- **Intermediarios de Valores**

    - Almacenes Generales de Depósito.
    - Sistemas de Pago de Bajo Valor.
    - Intermediación Cambiaria.
    - Servicios Financieros Especiales.
    - Compensación y liquidación de operaciones sobre valores depositados.
    - Administración de sistemas de negociación y registro de valores.
    - Administración del mercado bursátil y garantía de su buen funcionamiento.

- **Entidades Públicas**

    - Administración del mercado bursátil y garantía de su buen funcionamiento
    - Regular en materia fiscal, tributaria, aduanera, de crédito público, presupuestal, de tesorería, cooperativa, financiera, cambiaria, monetaria y crediticia la economía del país.
    - Manejar el aprovechamiento e inversión de los recursos del ahorro público y el Tesoro Nacional Supervisar, vigilar y control a las entidades del sector financiero y del sector solidario a través de las entidades vinculadas.
    - Administrar rentas de juegos de azar, gestionar e incentivar la financiación y estructuración de proyectos de infraestructura, financiar proyectos de infraestructura públicos y privado.
    - Administrar la Liquidación de Recaudos Tributarios y de Aduanas, para el cumplimiento de las obligaciones tributarias, aduaneras y cambiarias
    - Proteger la defensa y seguridad nacional en el ámbito económico, mediante inteligencia estratégica y operativa sustentada en tecnología e innovación.

- Administrar bienes especiales que se encuentran en proceso de extinción o se les haya decretado extinción de dominio. El código de Extinción de Dominio, ley 1708 de 2014.

## 2.2. Interdependencias.

### 2.2.1. Definición de una interdependencia sectorial.

Las interdependencias sectoriales se refieren a las dependencias en la prestación de servicios esenciales, en las cuales interrupciones y afectaciones en la prestación del servicio de algún segmento del sector financiero afecta a los otros. Las interdependencias identificadas al interior del sector se observan en la Tabla 1.

| | Intermediarios financieros | Seguros y Aseguradores | Bolsa e intermediarios de valores | Gobierno, DIAN y BanRep |
|---|---|---|---|---|
| **Intermediarios financieros** | | Disponibilidad de servicios transacciones y líneas de crédito | Disponibilidad de servicios transacciones y líneas de crédito | **Banco de la República**<br>• Sistema de pagos de alto valor CUD y bajo valor CENIT.<br>• Ventanillas de liquidez (LOLR).<br><br>**MinHacienda y otros**<br>• Gasto público y social de la política económica.<br>• Sistema Integrado de Información Financiera (SIIF).<br><br>**DIAN**<br>• Disponibilidad de aduanas<br>• Disponibilidad de información fiscal |
| **Seguros y Aseguradores** | Ninguno de corto plazo | | Disponibilidad de inversiones, a efecto de liquidez y solvencia | |
| **Bolsa e intermediarios de valores** | Disponibilidad de sistema de proveedores de liquidez (Miembros Liquidadores de la CCRC y otros). | Disponibilidad de inversiones, a efecto de liquidez y solvencia | | |
| **Gobierno, DIAN y BanRep** | **Banco de la República**<br>• Sistema de pagos de alto valor CUD y bajo valor CENIT.<br>• Ventanillas de liquidez (LOLR). | Disponibilidad cuenta ECAD – eventos catastróficos | Pánico financiero por declaraciones públicas o eventos de riesgo reputacional | |

Tabla 1. Listado de Entidades e Interdependencias

**Nota:** para leer el gráfico, se debe tener en cuenta que las filas se observan los segmentos que componen al sector (ver Superfinanciera) seleccionados y en las columnas las afectaciones que cada sector podría incidir en los demás.

### 2.2.2.Interdependencias Sectoriales del Sector Financiero con otros sectores.

En coherencia con lo anterior, esta sección ofrece una perspectiva de las dependencias en la prestación de servicios esenciales, en las cuales las interrupciones y afectaciones en la prestación de estos servicios que puedan generarse a partir de afectaciones a partir de incidentes cibernéticos. Para este fin se han establecido de manera general las posibles afectaciones desde un punto de vista sectorial, que afectan la provisión de servicios esenciales desde y hacia el sector financiero.

| Hacia el sector financiero | Desde el sector financiero |
|---|---|
| **Energía**<br>• La provisión de servicios financieros está profundamente relacionada con la disponibilidad del servicio de energía eléctrica. | **Sector Financiero**<br>• Los eventos cibernéticos pueden conducir a pérdidas profundas de información de clientes (personas y empresas).<br>• Las posibles afectaciones se traducen a pánico financiero. |
| **Telecomunicaciones**<br>• La capacidad del funcionamiento del sistema de pagos y los canales transacciones, para efectos interbancarios, de cada entidad y hacia el consumidor depende de la disponibilidad de los servicios de conectividad como internet y redes telefónicas.<br>• Dependiendo del tipo de afectación, la indisponibilidad de canales como internet o telefonía móvil impide la correcta comunicación de la entidad con sus clientes. | **Intermediarios financieros**<br>• Indisponibilidad de servicios transaccionales.<br>• Indisponibilidad de líneas de crédito para financiamiento privado e interbancario.<br>• Indisponibilidad de recursos en calidad de ahorro del público. |
| **Industria y comercio**<br>• Indisponibilidad de la economía para generar flujos financieros, pone en peligro la solvencia y liquidez de las instituciones financieras. | **Bolsa e intermediarios de valores**<br>• Indisponibilidad de recursos del sector privado y público en el mercado de capitales.<br>• Pánico en los mercados financieros y volatilidad económica. |
| **Gobierno (No financiero)**<br>• Si hay indisponibilidad del sector gobierno, la dispersión de recursos y la pagabilidad de los actores gubernamentales hacia el sector se puede ser entorpecida, lo que se traduce en riesgos para la estabilidad financiera. | **Seguros y Aseguradores**<br>• Incapacidad de materializar o solicitar seguros.<br>• Pérdida de confianza en instituciones que contraigan seguros. |
| **Defensa**<br>• En caso de ataque, la indisponibilidad del sector defensa conduce a mayores riesgos para el ecosistema digital y a una mayor probabilidad de afectación al sistema. | **Banco de la República**<br>• Sistema de pagos de alto valor CUD y bajo valor CENIT, conduce a pánico financiero.<br>• Inactividad de la política monetaria y problemas de la política económica. |

Tabla 2. Interdependencias desde y hacia del sector financiero.

# CAPÍTULO III: RIESGOS, VULNERABILIDADES E IMPACTO CIBERNÉTICO SECTORIAL

## 3.1. Riesgos Cibernéticos Sectoriales

Según la SFC, son los "*Posibles resultados negativos asociados a los ataques cibernéticos*", donde un ciberataque o ataque cibernético es la "Acción organizada o premeditada de uno o más agentes para causar daño o problemas a un sistema a través del ciberespacio".

Como se estableció en el numeral 2.1.1 de este documento, se adopta el concepto de los servicios esenciales del sector financiero y los define como aquellos enfocados en el mantenimiento de las funciones económicas de la sociedad colombiana y en el eficaz funcionamiento del Estado desde el punto de vista financiero y de la política económica, es decir la gestión de los riesgos cibernéticos en el sector es fundamental para mantener la estabilidad económica y financiera del país, a través de preservar la confianza y tranquilidad de la ciudadanía en la instituciones del sector, la confianza y estabilidad de los mercados e inversionistas, así como cumplir la regulación y normatividad vigente.

Por último, según el FMI (Fondo Monetario Internacional), "El sector financiero es particularmente vulnerable a los ataques cibernéticos. Las instituciones financieras son blancos interesantes por su función vital en la intermediación de fondos. Un ataque cibernético exitoso contra una institución podría propagarse rápidamente a través del sistema financiero, ya que está sumamente interconectado. Muchas instituciones siguen empleando sistemas más antiguos, que podrían no resistir a los ataques cibernéticos. Además, un ataque exitoso puede tener consecuencias sustanciales directas por las pérdidas financieras causadas, pero también costos indirectos, como el perjuicio a la reputación", conceptos que refuerzan la necesidad de gestionar el riesgo cibernético en las entidades del sector.

## 3.2. Vulnerabilidades Cibernéticas

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.

## 3.3. Análisis de Amenazas y Riesgos Sectoriales.

### 3.3.1. Identificación de activos críticos sectoriales.

De acuerdo con lo establecido en el Catálogo de Infraestructura Crítica Cibernética del CCOC y bajo metodologías sectoriales.

### 3.3.2. Análisis de las amenazas y riesgos

Para este fin se propone hacer uso del instrumento metodológico desarrollado por Jeimy Cano (2017). De acuerdo con Cano, se establece la metodología de la Ventana de AREM, la cual permite la adecuada identificación de riesgos cibernéticos, comprendiendo que estos riesgos son dinámicos.

De acuerdo con esta metodología, se establecen los siguientes riesgos:

- **Conocidos:** la amenaza se ha conversado o comunicado dentro de la organización y se conoce de su existencia.
- **Latente:** se ha enterado de que tal amenaza existe y que no sabe si la organización tiene alguna estrategia de mitigación.
- **Focales:** la amenaza ya se visto o materializado en la industria particular a la que pertenece la empresa.
- **Emergente:** nunca había escuchado de tal amenaza.

A partir de la aplicación de la metodología, se obtuvieron distintas percepciones de riesgos particulares para el sector financiero. A partir de lo anterior, fue posible identificar las distintas vulnerabilidades del sector, en un contexto digital y en relación con la provisión de servicios esenciales. Los resultados se muestran en la Tabla 3, los cuales fueron aportados por cada uno de los participantes de la Mesa del Sector Financiero.

| Lo que conoce la organización | Lo que desconoce la organización | Lo que conoce la organización | Lo que desconoce la organización |
|---|---|---|---|
| **Riesgos Conocidos** | **Riesgos Latentes** | **Riesgos Focalizados** | **Riesgos Emergentes** |
| • Malware que ya se presentó, pero sobre el cual no se han tomado las medidas de control pertinentes<br>• Ingeniería Social (Phishing, smishing, vishing)<br>• Reconocimiento (Information Gathering)<br>• Denegación de servicios distribuida (DDoS)<br>• Acuerdos con proveedores externos y contratistas<br>• Redes sociales<br>• Uso de servicios en la nube (Cloud services)<br>• Posibilidad de que se presenten fallas del canal de telecomunicaciones para el desarrollo de sus operaciones<br>• Descarga y/o instalación se software base<br>• Fraude a usuarios del sistema financiero<br>• Divulgación de información de identificación personal<br>• Fraude interno o infidelidad<br>• Falta de interés por parte de la alta dirección para la gestión de los riesgos de ciberseguridad<br>• Falta de formación y concientización por parte de los colaboradores en la | • Vulnerabilidades de día cero (0 Day)<br>• Advanced Persistet Threats (APTs)<br>• Fallos en diseño asociados a software libre (como ejemplo Meltdown y Spectre)<br>• Posibilidad de que se presenten fallas en el hardware y/o en el software que destina la entidad como apoyo tecnológico en sus operaciones.<br>• Incumplimiento en el tiempo de entrega para la puesta en producción de los sistemas de información desarrollados o adquirido<br>• Obsolescencia del software o hardware<br>• Falta de recursos para una adecuada gestión<br>• Sistemas de información mal configurados o no autorizados expuestos a Internet<br>• Compromiso de los sistemas de información organizacional para facilitar la filtración de datos / información | • Malware focalizado a vulnerar controles transaccionales (tipo de banca)<br>• Ataques en cajeros electrónicos (ATMs attacks)<br>• Reputacional por incumplimiento de regulación local e Internacional (Superfinanciera de Colombia y OSFI para el caso de Canadá).<br>• Acceso no autorizado a los sistemas de información no corporativos<br>• Uso indebido o inadecuado de los datos contenidos en las bases de datos corporativas<br>• Hacktivismo o ciberataques políticamente motivados<br>• Falsificación o alteración del hardware en la cadena de suministro | • Uso de nuevos algoritmos criptográficos<br>• Nuevas tecnologías asociadas a nuevas API (Fintech, Startups).<br>• IoT (Internet de las Cosas)<br>• Implementación de soluciones basadas en machine learning e inteligencia artificial<br>• Ingeniería inversa para explotar vulnerabilidades |

| Lo que conoce la organización | Lo que desconoce la organización | Lo que conoce la organización | Lo que desconoce la organización |
|---|---|---|---|
| **Riesgos Conocidos** | **Riesgos Latentes** | **Riesgos Focalizados** | **Riesgos Emergentes** |
| gestión de los riesgos de ciberseguridad<br>• Robo o secuestro de información sensible por ataques cibernéticos asociados a ransomware a la infraestructura<br>• Servicios corporativos no disponibles en Internet por fallas asociadas a la infraestructura tecnológica<br>• Interrupción de las actividades del negocio o de los procesos críticos por falta de gestión de los incidentes cibernéticos en los planes corporativos de recuperación de desastres y continuidad de negocios | | | |

Tabla 3. Resultados Ventana de AREM

## 3.4. Impacto Cibernético Sectorial.

Dentro de los elementos claves para la operación de las entidades financieras se requiere involucrar e interactuar con sistemas de entidades del mismo sector y de otros sectores tanto a nivel nacional como internacional, para poder brindar y atender a las necesidades de sus clientes y usuarios. Las exigencias de un mercado como el financiero, no podrían ser ejecutadas sin la intervención de estas tecnologías, las cuales son fundamentales en el uso de canales tradicionales como oficinas de atención al público, interconexión de sistemas entre entidades del mismo sector, sistemas de cajeros automáticos, movimientos de bolsa, sistemas de audio respuesta, negocios fiduciarios, puntos de venta, registros y operaciones de pensiones y cesantías, en general cualquier operación del sistema financiero Colombiano no podría ser ejecutado con las exigencias de un mercado intercomunicado a nivel nacional e internacional sin la intervención de estas tecnologías.

A continuación, se incluye una gráfica estilo mapa de calor que identifica los riesgos conocidos, latentes, focalizados y emergentes junto con su respectivo impacto o severidad y probabilidad de ocurrencia. En general, se puede concluir que hay una relación inversa entre la severidad de los riesgos y la ocurrencia de los mismos respecto de la ICC del sector.

| Color | Estado |
|---|---|
| | **Crítica** |
| | Alta |
| | Media |
| | Baja |
| | Muy Baja |

Tabla 4. Definición de colores y relación de estados.

| IMPACTOS CIBERNÉTICOS SECTORIALES | | |
|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Severidad** | **Ocurrencia** |
| **Riesgos Conocidos** | | |
| • Malware que ya se presentó pero sobre el cual no se han tomado las medidas de control pertinentes | ALTA | BAJA |
| • Ingeniería Social (Phishing, smishing, vishing) | ALTA | MEDIA |
| • Reconocimiento (Information Gathering) | BAJA | BAJA |
| • Denegación de servicios distribuida (DDoS) | MEDIA | BAJA |
| • Acuerdos con proveedores externos y contratistas | MEDIA | BAJA |
| • Redes sociales | MEDIA | BAJA |
| • Uso de servicios en la nube (Cloud services) | ALTA | MUY BAJA |
| • Posibilidad de que se presenten fallas del canal de telecomunicaciones para el desarrollo de sus operaciones | ALTA | BAJA |
| • Descarga y/o instalación se software base | MEDIA | BAJA |
| • Fraude a usuarios del sistema financiero | ALTA | BAJA |
| • Divulgación de información de identificación personal | ALTA | BAJA |
| • Fraude interno o infidelidad | ALTA | BAJA |
| • Falta de interés por parte de la alta dirección para la gestión de los riesgos de ciberseguridad | ALTA | MUY BAJA |
| • Falta de formación y concientización por parte de los colaboradores en la gestión de los riesgos de ciberseguridad | MEDIA | BAJA |
| • Robo o secuestro de información sensible por ataques cibernéticos asociados a ransomware a la infraestructura | ALTA | MUY BAJA |
| • Servicios corporativos no disponibles en Internet por fallas asociadas a la infraestructura tecnológica | ALTA | MEDIA |
| • Interrupción de las actividades del negocio o de los procesos críticos por falta de gestión de los incidentes cibernéticos en los planes corporativos de recuperación de desastres y continuidad de negocios | CRITICO | MUY BAJA |
| **Riesgos Latentes** | | |
| • Vulnerabilidades de día cero (0 Day) | ALTA | MUY BAJA |
| • Advanced Persistet Threats (APTs) | MEDIA | MUY BAJA |
| • Fallos en diseño asociados a software libre (como ejemplo Meltdown y Spectre) | BAJA | BAJA |
| • Posibilidad de que se presenten fallas en el hardware y/o en el software que destina la entidad como apoyo tecnológico en sus operaciones. | ALTA | BAJA |
| • Incumplimiento en el tiempo de entrega para la puesta en producción de los sistemas de información desarrollados o adquirido | MEDIA | MEDIA |
| • Obsolescencia del software o hardware | MEDIA | MEDIA |
| • Falta de recursos para una adecuada gestión | MEDIA | BAJA |
| • Sistemas de información mal configurados o no autorizados expuestos a Internet | MEDIA | BAJA |

| IMPACTOS CIBERNÉTICOS SECTORIALES | | |
|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Severidad** | **Ocurrencia** |
| • Compromiso de los sistemas de información organizacional para facilitar la filtración de datos / información | MEDIA | MUY BAJA |
| **Riesgos Focalizados** | | |
| • Malware focalizado a vulnerar controles transaccionales (tipo de banca) | ALTA | BAJA |
| • Ataques en cajeros electrónicos (ATMs attacks) | MUY BAJA | MUY BAJA |
| • Reputacional por incumplimiento de regulación local e Internacional (Superfinanciera de Colombia y OSFI para el caso de Canadá). | ALTA | BAJA |
| • Acceso no autorizado a los sistemas de información no corporativos | ALTA | BAJA |
| • Uso indebido o inadecuado de los datos contenidos en las bases de datos corporativas | ALTA | BAJA |
| • Hacktivismo o ciberataques políticamente motivados | ALTA | MUY BAJA |
| • Falsificación o alteración del hardware en la cadena de suministro | MEDIA | MUY BAJA |
| **Riesgos Emergentes** | | |
| • Uso de nuevos algoritmos criptográficos | MEDIA | BAJA |
| • Nuevas tecnologías asociadas a nuevas API (Fintech, Startups). | MEDIA | BAJA |
| • IoT (Internet de las Cosas) | MEDIA | BAJA |
| • Implementación de soluciones basadas en machine learning e inteligencia artificial | MEDIA | MUY BAJA |
| • Ingeniería inversa para explotar vulnerabilidades | ALTA | BAJA |

Tabla 5. Impactos sectoriales y riesgos cibernéticos – sector financiero

Para este desarrollo, se ha empleado la siguiente metodología de diligenciamiento.

**Anexo metodológico**

| SUGERENCIA METODOLÓGICA SEVERIDAD | | |
|---|---|---|
| **TIPO DE IMPACTO** | **UNIDAD** | **PUNTAJE (Índice)** |
| **1. FINANCIERO** | COP ($) - MILLONES | 0 - 10 |
| **2. FRAUDE CONFIRMADO** | COP ($) - MILLONES | 0 - 10 |
| **3. CAPITAL EN RIESGO** | COP ($) - MILLONES | 0 - 10 |
| **4. EN CLIENTES** | No. clientes afectados /Total clientes | 0 - 10 |
| **5. EN HOST** | No. End Point comprometidos /Total EndPoints | 0 - 10 |
| **6. EN SERVICIO** | Horas de indisponibilidad | 0 - 10 |
| **7. EN INFORMACIÓN** | No. registros comprometidos /Total No. registros | 0 - 10 |
| **8. PERDIDA DE CONTROL** | No. de Host comprometidos /Total No. Host | 0 - 30 |

Fuente: Elaboración propia

**Anexo metodológico**

| SUGERIDO | Severidad | Total (Índice de Severidad) | SUGERIDO | Ocurrencia | Frecuencia o probabilidad |
|---|---|---|---|---|---|
| Se calcula como la **suma de los puntajes** totales de los 8 campos de tipo de impacto | Muy baja | 0 - 10 | Se calcula como la **frecuencia u ocurrencia** de aparición durante un año (1 año) | Muy baja | 0% - 10% |
| | Baja | 10 - 30 | | Baja | 30% |
| | Media | 30 - 60 | | Media | 50% |
| | Alta | 60 - 90 | | Alta | 80% |
| | Crítico | 90 - 100 | | Muy alta | 90% |

Fuente: Elaboración propia

El ciberespacio es un asunto relevante, dado los riesgos a los que los servicios, las actividades y en especial la información manejada por sector se están viendo expuestos. En la medida en que el sector financiero se convierte a plataformas y servicios virtuales, se deberá enfocar en protegerse de los riesgos a los que expone a través del ciberespacio.

El ciberespacio ya es parte de la vida de cada individuo, por lo que la importancia que el sector financiero trabaje en conjunto para atender a estas y otras tendencias en cuanto a la seguridad de la información y ciberseguridad se refieren, no se hacen esperar.

# CAPITULO IV. PLANEACIÓN ESTRATÉGICA SECTORIAL PARA LA PROTECCIÓN DE LA ICC

## 4.1 Líneas Estratégicas, Acciones y Métricas

Para el desarrollo y fortalecimiento de la protección y defensa de las ICC del sector financiero, se desarrollarán cinco estrategias, las cuales se fundamentan en un conjunto de actividades a ser desarrolladas en el mediano (2018-2019) y largo plazo (2020-2022).

El desarrollo de las líneas estratégicas se asocia de manera fundamental con los controles y acciones propuestas para mitigar cada uno de los riesgos tecnológicos identificados en la ventana de AREM del sector.

### 4.1.1. Línea Estratégica 1. Resiliencia y Continuidad del Negocio:

A través de la gestión de la resiliencia se definirán los procesos, controles y las prácticas organizacionales a utilizar, para diseñar, desarrollar, implementar y controlar las estrategias, que hagan operativamente más resilientes los servicios esenciales del sector, así como los procesos y activos que lo soportan tales como personas, información, y tecnología en las ICC, todo bajo la normatividad expedida por la Superintendencia Financiera, así como el Ministerio de las TIC (especialmente para el componente público del sector).

Bajo esta línea estratégica se desarrollarán las siguientes acciones e implementación de controles:

a) Definición, Elaboración y Pruebas continuas de Planes de continuidad y recuperación de incidentes cibernéticos, con el fin de mantener en operación los servicios esenciales definidos y el normal desempeño de las interdependencias en las cuales participa el sector.
b) Revisión periódica de los Acuerdos de Niveles de Servicio con terceros, que intervengan o tengan responsabilidad en la administración y/o gestión de ICC del sector, para su maduración de acuerdo a la evolución del contrato.
c) Establecer planes para la gestión de BackUps que incluyan la restauración periódica de los mismos.
d) Conocer detalladamente de los planes de recuperación definidos por lo proveedores.
e) Realizar evaluaciones sobre la calidad del software, ya sea el desarrollado “in house”, así como por terceros, para prevenir riesgos asociados específicamente a software.
f) Mejorar los procesos de validación de la identidad de la persona y de la verificación de la información que suministra, tema fundamental en el sector financiero y regulado por la SFC
g) Implementar Procesos y procedimientos acompañados de implementación de controles tecnológicos.
h) Realizar una cooperación centralizada con las entidades del sector (CSIRT Financiero).
i) Definir un seguro de Fidelidad, para la prevención de riesgos de fraudes internos e infidelidad financiera.

j) Alinear la Alta Gerencia a una metodología para definir un procedimiento de medición y valoración de riesgos y oportunidades, para lograr y mantener.
k) Realizar planes de capacitación y formación focalizados, para mitigar la falta de formación y concientización por parte de los colaboradores, funcionarios y terceros (contratistas) relacionados con las entidades.
l) Llevar a cabo evaluaciones continuas y mejoras a los programas de seguridad cibernética y gestión de riesgos.
m) Diseñar y ejecutar simulaciones de ataques incluidos en los planes de recuperación sectoriales.

### 4.1.2. Línea Estratégica 2. Cumplimiento regulatorio y normativo.

La protección de las ICC del sector financiero requiere del compromiso de todas las instituciones comprometidas en el presente plan, y del apoyo de los diferentes organismos a nivel nacional e internacional con experiencia en la materia. Por tanto, es necesario reglamentar las actuaciones y los criterios establecidos por todos los agentes de la estructura definida para la protección y defensa de las ICC.

Bajo esta línea estratégica se desarrollarán las siguientes acciones e implementaciones de controles:

a) Generar consciencia a través de campañas y capacitaciones de seguridad para funcionarios y colaboradores de las entidades.
b) Madurar controles y barreras físicas tecnológicas.
c) Implementación de estándares internacionales y buenas prácticas de la industria en temas de seguridad.
d) Hacer un monitoreo de indicadores de cumplimiento y efectividad de los controles de seguridad
e) Realizar control interno y auditorias (internas y externas), es decir, realización de ejercicios independientes desarrollados por áreas de control interno.
f) Efectuar pruebas de seguridad y rendimiento, después de cambios mayores a la infraestructura.
g) Pactar ANS son proveedores que incluyan los temas de seguridad y continuidad, con cláusulas claras y exigentes sobre el cumplimiento de controles y cuyo incumplimiento tenga sanciones y multas, que vayan contra la facturación y que lleven a una evaluación y re-evaluación permanente de los proveedores externos.
h) Cambiar la aptitud por actitud para que la Alta Gerencia asuma el liderazgo que la norma le adjudica.
i) Se cuenta con una Directiva enfocada al aseguramiento de dispositivos ATMs, de igual forma se cuenta con un estándar técnico que apoya la definición de controles de seguridad, la cual se debe madurar y desarrollar de acuerdo con los escenarios de riesgos que se vayan presentando e identificando.
j) Implementar plataformas de Correlación de eventos, FW perimetrales, herramienta de DLP, WAF, Analítica de Amenazas, administración de cuentas de usuarios, medios de transmisión de información cifrados.
k) Elaborar y actualizar permanente de Manuales de Seguridad de la información en los cuales se describan las políticas y normas de seguridad de la información definidas.

### 4.1.3. Línea Estratégica 3. Mitigación y Gestión de Incidentes Cibernéticos.

Para la protección de las ICC del sector financiero se requiere fortalecer y ampliar las capacidades para mitigar y gestionar los incidentes cibernéticos, en especial los que tienen un impacto transversal para entidades del sector o que , al afectar por lo menos un servicio esencial de los establecidos, puede tener implicaciones y efectos a nivel nacional.

Bajo esta línea estratégica se desarrollarán las siguientes acciones e implementaciones de controles:

a) Controlar los riesgos asociados a temas de malware por medio de controles consistentes en combinar soluciones tecnológicas y gestión de Seguridad de la Información, aumentando los niveles de protección para dispositivos móviles, implementando SOC´s y realizando de manera formal el Análisis e interpretación de información.
b) Capacitar a los operadores de las herramientas de detección, para una mayor efectividad en la detección de las amenazas cibernéticas.
c) Implementar bloqueo con infraestructura de seguridad perimetral
d) Identificar riesgos propios del proveedor y subcontratistas si aplican
e) Definir esquemas alternos de comunicación y acceso a aplicaciones claves para el negocio (aplicaciones “core”).
f) Implementar Controles basados en infraestructura de seguridad perimetral avanzada y controles de acceso
g) Fortalecer los sistemas con soluciones tecnológicas y analíticas que permitan pasar de acciones reactivas a preventivas
h) Implementar controles asociados con Tokens OTP para realizar operaciones en lapsos
i) Fortalecer el programa de aseguramiento de ATMs con el que se cuenta en las entidades bancarias. Se deben incluir controles antimalware, monitoreo de eventos, restricciones de nivel de red, aislamientos de cajeros.
j) Fortalecer los programas con los que se cuenta actualmente. Se cuenta con:

    - Programa de gestión de vulnerabilidades a sistemas de información críticos
    - Monitoreo de eventos de seguridad enfocados a las actividades de usuarios privilegiados (Administradores).
    - El modelo de Atención de Incidentes define escenarios y procedimientos asociados a los tipos de riesgos definidos.

### 4.1.4. Línea Estratégica 4. Cooperación, Articulación e Inteligencia de Amenazas

A través de la cooperación intersectorial e intersectorial, se pueden generar espacios y sinergias que lleven a una mejor gestión de los riesgos y a una detección oportuna de las amenazas, en ambientes cada vez más cambiantes. El desarrollo de este documento es una oportunidad para divulgar el tema cada vez a más actores del sector financiero y establecer los acuerdos y convenios para su participación en la protección y defensa de las ICC financieras.

Bajo esta línea estratégica se desarrollarán las siguientes acciones e implementación de controles:

a) Establecer escenarios y canales para compartir signos y síntomas observados de infección para su identificación
b) Establecer mecanismos y espacios de articulación con entidades referentes en el sector.
c) Participar en foros de interés.
d) Vincular a las entidades del sector al CSIRT Financiero, iniciativa promovida por la Asobancaria y que se constituirá en el espacio y foro de referencia para la articulación, divulgación y difusión de lo relacionado con el tema de ciberseguridad en el sector.
e) Fomentar la conformación y participación en ellos, de grupos de interés gremiales y estatales.

### 4.1.5. Línea Estratégica 5. Divulgación y Sensibilización

Una de las lecciones que deja el desarrollo conjunto de este documento por parte de las diferentes entidades que participaron, es que el compartir la información de incidentes, avances en gestión de riesgos, información y documentación sobre nuevas amenazas, es clave para la protección de las ICC del sector, enfatizando que este "compartir" información debe hacerse sobre protocolos estrictos de confidencialidad y reserva.

Bajo esta línea estratégica se desarrollarán las siguientes acciones e implementaciones de controles:

a) Concientización sobre la seguridad de los empleados para convertirlos en "Firewalls humanos".
b) Elaboración de protocolos de comunicaciones sectoriales.
c) Programas de sensibilización y capacitación a funcionarios, terceros y clientes.
d) Campañas sobre el hecho de que existe la posibilidad de que nuestros sistemas sean atacados.
e) Poner en marcha el concepto de asociarse y compartir conocimiento e información.
f) Desarrollar ejercicios conjuntos de innovación en temas de seguridad.
g) Campañas de conocimiento específico en el derecho de Habeas Data y protección de datos personales (Leyes 1266 y 1581).
h) Concientizar en ciberseguridad a los directivos, ya consideramos que el riesgo es mayor por el poder de decisión que tienen.
i) Desarrollar al interior del sector y de las entidades, Campañas de sensibilización y cursos regulatorios sobre Seguridad de la Información y Ciberseguridad.

En la siguiente tabla se presenta el cuadro resumen de las líneas estratégicas:

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| **Riesgos Conocidos** | **Controles** | | | | |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| • Malware que ya se presentó pero sobre el cual no se han tomado las medidas de control pertinentes | Planes de continuidad y recuperación de incidentes cibernéticos | Generar consciencia a través de campañas y capacitaciones de seguridad | Combinar soluciones tecnológicas y gestión de Seguridad de la Información | Compartir signos y síntomas observados de infección para su identificación | Elaboración de informes posteriores |
| • Ingeniería Social (Phishing, smishing, vishing) | Planes de continuidad y recuperación de incidentes cibernéticos | Madurar controles y barreras físicas | Aumentar niveles de protección para dispositivos móviles | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Concientización sobre la seguridad de los empleados para convertirlos en “Firewalls humanos” |
| • Reconocimiento (Information Gathering) | Planes de continuidad y recuperación de incidentes cibernéticos | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Denegación de servicios distribuida (DDoS) | Realizar pruebas periódicas para la definición de líneas base | Efectuar pruebas de seguridad y rendimiento después de cambios mayores a la infraestructura | Implementar bloqueo con infraestructura de seguridad perimetral | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Elaboración de informes posteriores |
| • Acuerdos con proveedores externos y contratistas | Revisión periódica de los ANS para su maduración de acuerdo a la evolución del contrato | Pactar ANS y que se castiguen contra la facturación Re-evaluación de los proveedores externos | Identificación de Riesgos propios del proveedor y subcontratistas si aplican | Articulación con entidades referentes en el sector. Participación en foros de interés. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | | | | Vinculación a CSIRT Financiero. | funcionarios, terceros y clientes |
| • Redes sociales | | | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector.<br>Participación en foros de interés.<br>Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Uso de servicios en la nube (Cloud services) | Establecimiento de planes para la gestión de BackUps que incluyan la restauración periódica de los mismos. | Implementación de estándares internacionales y buenas prácticas de la industria<br>Monitoreo de indicadores de cumplimiento.<br>Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector.<br>Participación en foros de interés.<br>Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Posibilidad de que se presenten fallas del canal de telecomunicaciones para el desarrollo de sus operaciones | Conocimiento detallado de los planes de recuperación definidos por lo proveedores | Implementación de estándares internacionales y buenas prácticas de la industria<br>Monitoreo de indicadores de cumplimiento.<br>Control interno y auditorias (internas y externas) | Definir esquemas alternos de comunicación y acceso aplicaciones core. | Articulación con entidades referentes en el sector.<br>Participación en foros de interés.<br>Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Descarga y/o instalación se software base | Realizar evaluaciones sobre la calidad del software | Establecer responsabilidades, propietarios y vigilantes | Controles basados en infraestructura de seguridad perimetral avanzada y controles de acceso | Articulación con entidades referentes en el sector.<br>Participación en foros de interés. | Campañas sobre el hecho de que existe la posibilidad de que nuestros sistemas sean atacados |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | | | | Vinculación a CSIRT Financiero. | |
| • Fraude a usuarios del sistema financiero | Mejorar los procesos de validación de la identidad de la persona y de la verificación de la información que suministra | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Fortalecimiento de los Sistemas con soluciones tecnológicas y analíticas que permitan pasar de acciones reactivas a preventivas | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Poner en marcha el concepto de asociarse y compartir conocimiento e información Innovar!!! |
| • Divulgación de información de identificación personal | Procesos y procedimientos acompañados de implementación de controles tecnológicos. Cooperación centralizada con las entidades del sector (CSIRT Financiero) | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Campañas de conocimiento específico en el derecho de Habeas Data. |
| • Fraude interno o infidelidad | Definir un seguro de Fidelidad | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Concientizar en ciberseguridad a los directivos ya que el riesgo es mayor por el poder de decisión que tienen |
| • Falta de interés por parte de la alta dirección para la gestión de los riesgos de ciberseguridad | Alinear la Alta Gerencia a una metodología para definir un procedimiento de medición | Cambiar la aptitud por actitud para que la Alta Gerencia asuma el liderazgo que la norma le adjudica | Implementación de SOC.<br><br>Análisis e interpretación de información. | Articulación con entidades referentes en el sector. Participación en foros de interés. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | y valoración de riesgos y oportunidades | | Capacitación a los operadores de las herramientas de detección | Vinculación a CSIRT Financiero. | y capacitación a funcionarios, terceros y clientes |
| • Falta de formación y concientización por parte de los colaboradores en la gestión de los riesgos de ciberseguridad | Planes de capacitación y formación focalizados | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Robo o secuestro de información sensible por ataques cibernéticos asociados a ransomware a la infraestructura | Evaluaciones continuas y mejoras a los programas de seguridad cibernética y gestión de riesgos | Actualizarnos constantemente en buenas prácticas | Definición de indicadores | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Concienciar a la organización sobre la importancia de protegerse |
| • Servicios corporativos no disponibles en Internet por fallas asociadas a la infraestructura tecnológica | Planes de continuidad y recuperación de incidentes cibernéticos | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. Control interno y auditorias (internas y externas) | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las herramientas de detección | Articulación con entidades referentes en el sector. Participación en foros de interés. Vinculación a CSIRT Financiero. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a funcionarios, terceros y clientes |
| • Interrupción de las actividades del negocio o de los procesos críticos por falta de gestión de los incidentes cibernéticos en los planes corporativos de | Planes de continuidad y recuperación de incidentes cibernéticos | Implementación de estándares internacionales y buenas prácticas de la industria Monitoreo de indicadores de cumplimiento. | Implementación de SOC.<br><br>Análisis e interpretación de información.<br><br>Capacitación a los operadores de las | Articulación con entidades referentes en el sector. Participación en foros de interés. | Elaboración de protocolos de comunicaciones sectoriales.<br><br>Programas de sensibilización y capacitación a |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| recuperación de desastres y continuidad de negocios | | Control interno y auditorias (internas y externas) | herramientas de detección | Vinculación a CSIRT Financiero. | funcionarios, terceros y clientes |
| **Riesgos Latentes** | **Simulaciones y acciones** | | | | |
| • Vulnerabilidades de día cero (0 Day) | Actualizaciones (parches) de seguridad no aplicadas a estaciones y servidores | Ejercicios independientes desarrollados por áreas de control interno | Seguridad perimetral. Bloqueo de dispositivos. Participación en grupos de ciberseguridad | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Advanced Persistet Threats (APTs) | | Ejercicios independientes desarrollados por áreas de control interno | Seguridad perimetral. Bloqueo de dispositivos. Participación en grupos de ciberseguridad | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Fallos en diseño asociados a software libre (como ejemplo Meltdown y Spectre) | Capacitación interna y a proveedores | Ejercicios independientes desarrollados por áreas de control interno | Evaluar la obsolescencia de las soluciones para cambiarlas o actualizarlas | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Posibilidad de que se presenten fallas en el hardware y/o en el software que destina la entidad como apoyo tecnológico en sus operaciones. | * Diseño de planes de continuidad y contingencia con simulaciones de presencia de incidentes similares | Ejercicios independientes desarrollados por áreas de control interno | | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Incumplimiento en el tiempo de entrega para la puesta en producción de los sistemas de información desarrollados o adquirido | * Diseño de planes de continuidad y contingencia con simulaciones de presencia de incidentes similares | Ejercicios independientes desarrollados por áreas de control interno | Gestión de proyectos | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Obsolescencia del software o hardware | * Diseño de planes de continuidad y contingencia con simulaciones de presencia | Ejercicios independientes desarrollados por áreas de control interno | Actualizaciones y parcheos de acuerdo con las nuevas versiones de los fabricantes | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | de incidentes similares | | | | |
| • Falta de recursos para una adecuada gestión | * Diseño de planes de continuidad y contingencia con simulaciones de presencia de incidentes similares | Ejercicios independientes desarrollados por áreas de control interno | Establecer una planeación estratégica para la administración recursos de ciberseguridad que incluya iniciativas de mitigación de nuevas amenazas. | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Sistemas de información mal configurados o no autorizados expuestos a Internet | * Diseño de planes de continuidad y contingencia con simulaciones de presencia de incidentes similares | Ejercicios independientes desarrollados por áreas de control interno | Pruebas de seguridad | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| • Compromiso de los sistemas de información organizacional para facilitar la filtración de datos / información | * Diseño de planes de continuidad y contingencia con simulaciones de presencia de incidentes similares | Ejercicios independientes desarrollados por áreas de control interno | Procedimento de cambios Segregación de ambientes Pruebas de seguridad | Participación en grupos de interés gremiales y estatales. | Elaboración de protocolos de comunicaciones sectoriales |
| **Riesgos Focalizados** | **Simulaciones y acciones** | | | | |
| • Malware focalizado a vulnerar controles transaccionales (tipo de banca) | Simulación de ataques incluidos en los planes de recuperación sectoriales | | Token OTP para realizar operaciones en lapsos | | |
| • Ataques en cajeros electrónicos (ATMs attacks) | Simulación de ataques incluidos en los planes de recuperación sectoriales | Se cuenta con una Directiva enfocada al aseguramiento de dispositivos ATMs, de igual forma se cuenta con un estándar técnico que apoya la definición de | Se cuenta con un programa de aseguramiento de ATMs en el Banco. Se incluyen controles antimalware, monitoreo de eventos, restricciones de nivel de red, | | |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | | controles de seguridad. | aislamientos de cajeros. | | |
| • Reputacional por incumplimiento de regulación local e Internacional (Superfinanciera de Colombia y OSFI para el caso de Canadá). | Simulación de ataques incluidos en los planes de recuperación sectoriales | Contratos con terceros<br><br>Control de acceso<br>Se cuenta con programa de monitoreo (Matriz regulatorio) a todos los requerimientos exigidos por reguladores | | | |
| • Acceso no autorizado a los sistemas de información no corporativos | Simulación de ataques incluidos en los planes de recuperación sectoriales | Contratos con terceros<br><br>Control de acceso | Se cuenta con:<br><br>Programa de gestión de vulnerabilidades a sistemas de información críticos<br><br>-Monitoreo de eventos de seguridad enfocados a las actividades de usuarios privilegiados (Administradores). | | Campañas de sensibilización y cursos regulatorios sobre Seguridad de la Información y Ciberseguridad |
| • Uso indebido o inadecuado de los datos contenidos en las bases de datos corporativas | Simulación de ataques incluidos en los planes de recuperación sectoriales | Contratos con terceros<br><br>Control de acceso<br><br>Correlación de eventos, FW perimetrales, herramienta de DLP, WAF, Analítica de Amenazas, administración de cuentas de usuarios, medios de transmisión de | El modelo de Atención de Incidentes define escenarios y procedimientos asociados a este tipo de riesgo. | | |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | | información cifrados | | | |
| • Hacktivismo o ciberataques políticamente motivados | * Simulación de ataques incluidos en los planes de recuperación sectoriales | Contratos con terceros<br><br>Control de acceso | | | |
| • Falsificación o alteración del hardware en la cadena de suministro | * Simulación de ataques incluidos en los planes de recuperación sectoriales | El supervisor del contrato informa al jefe de la oficina de tecnología sobre el vencimiento de soportes o de las garantías cuando hayan soportes o garantías vigentes | | | |
| **Riesgos Emergentes** | **Planes de Contención** | | | | |
| • Uso de nuevos algoritmos criptográficos | | Manual de Seguridad de la información en el cual se describen las políticas y normas de seguridad de la información definidas | | Se cuenta con el apoyo del equipo de Ciberseguridad de casa matriz el cual considera alianzas, así como grupos para análisis de nuevas tendencias. | |
| • Nuevas tecnologías asociadas a nuevas API (Fintech, Startups). | Planes de continuidad<br><br>Prueba de planes | | Se realizan evaluaciones de riesgo a todas las nuevas iniciativas que buscan ser implementadas en el Banco.<br><br>Se cuenta con el apoyo del equipo de Ciberseguridad de casa matriz el cual considera alianzas, así como grupos | | |

| LINEAMIENTOS ESTRATÉGICOS | | | | | |
|---|---|---|---|---|---|
| **Tipos de riesgo Ventana de AREM (en relación con la prestación de servicios esenciales)** | **Resiliencia y Continuidad del Negocio** | **Cumplimiento regulatorio y normativo** | **Mitigación y Gestión de Incidentes Cibernéticos** | **Cooperación, Articulación e Inteligencia de Amenazas** | **Divulgación y Sensibilización** |
| | | | para análisis de nuevas tendencias. | | |
| • IoT (Internet de las Cosas) | Planes de continuidad<br><br>Prueba de planes | Se cuenta con políticas asociadas al uso de este tipo de tecnologías. | No se permite la conexión de este tipo de tecnologías a la red de datos del Banco.<br><br>Se cuenta con el apoyo del equipo de Ciberseguridad de casa matriz el cual considera alianzas así como grupos para análisis de nuevas tendencias. | | |
| • Implementación de soluciones basadas en machine learning e inteligencia artificial | | Herramientas SIEM Enterprise Security y Analítica de Amenazas | Se cuenta con el apoyo del equipo de Ciberseguridad de casa matriz el cual considera alianzas así como grupos para análisis de nuevas tendencias. | | |
| • Ingeniería inversa para explotar vulnerabilidades | | | Las pruebas de Hacking Ético incluyen este escenario de evaluación considerando aplicaciones críticas de negocio. | | |

Tabla 6. Acciones sectoriales – ventana de AREM

En general, el sector financiero cuenta con unas líneas de acción claras ante riesgos cibernéticos conocidos, focalizados, latentes y emergentes. No obstante, es necesario realizar pruebas y simulaciones para probar la efectividad de los lineamientos estratégicos establecidos.

## 4.2 Estrategias de Comunicación y Divulgación

El presente plan debe ser difundido, a todo nivel, en el esquema de protección y defensa de las ICCN del sector. En su componente privado, el esquema de divulgación lo debe definir la mesa de infraestructura crítica cibernética del sector. En su componente Público, el Ministerio de Hacienda, como cabeza del sector hacienda, lo divulgará a través del Comité Sectorial de Gestión y Desempeño Institucional, estableciendo los lineamientos para su desarrollo e implementación en las entidades de este sector, en lo que les corresponda.

También debe ser socializado al interior del Comité de Seguridad Digital, creado mediante el Acuerdo 2 del Consejo para la Gestión y el Desempeño Institucional, del 5 de junio de 2018, Este Comité tiene, dentro de las temáticas de estudio, la “Protección y Defensa de la Infraestructura Crítica Cibernética Nacional (ICCN)”.

# CAPITULO V. ESTRUCTURA SECTORIAL DE PROTECCIÓN Y DEFENSA DE LA INFRAESTRUCTURA CIBERNÉTICA

Lo establecido en el siguiente capítulo busca definir las directrices generales que permitan hacer un seguimiento, análisis y evaluación de las amenazas sobre las infraestructuras críticas cibernéticas del sector, así como, la puesta en marcha de acciones y la coordinación de los agentes del sistema en una situación de crisis cibernética.

Estas medidas deberán ser incorporadas a los instrumentos de planificación, operación y por los propietarios de infraestructuras críticas cibernéticas.

## 5.1. Organigrama (GRAFICA)

Con el fin de responder adecuadamente a situaciones de crisis cibernética, se requiere conformar comités que lideren la estrategia sectorial para el manejo de la misma, así como desarrollar planes de respuesta y comunicación, que protejan la reputación y garanticen la resiliencia cibernética de los servicios esenciales identificados en el capítulo II de este documento.

Entidades participantes:

- Superintendencia Financiera de Colombia
- Establecimientos de crédito: Establecimientos Bancarios, Corporaciones Financieras, Compañías de Financiamiento Comercial, Cooperativas Financiera.
- Banco de la República
- Intermediarios financieros y de valores
- Sociedades Fiduciarias
- DIAN
- Ministerio de Hacienda
- Sociedades Administradoras de Pensiones y Cesantías
- Entidades Aseguradoras

**Comité Técnico:** conformado por un (1) delegado en cada uno de los gremios que representan a las entidades financieras que prestan servicios esenciales[2] (*), más un (1) representante del comité de seguridad digital del Gobierno, más un representante de la Superintendencia Financiera de Colombia, más el coordinador del CSIRT[3]. (**)

**Comité Directivo:** compuesto por tres (3) delegados de cada uno de los gremios que representan a las entidades financieras, es decir, los presidentes, vicepresidentes jurídicos y vicepresidentes de comunicaciones, más el Superintendente Financiero, más el Ministro de Hacienda, más el presidente de FOGAFÍN, más el Gerente Ejecutivo del Banco de la República, más el coordinador del CSIRT financiero

2 Se citarán a los responsables de los procesos críticos afectados en cada entidad financiera, en caso de requerir su participación en el Comité, quienes deben tener un perfil directivo y técnico dentro de las áreas de seguridad de la información y ciberseguridad de las entidades financieras.

3 En los casos requeridos, el comité podrá sesionar de forma virtual mediante videoconferencia.

## 5.2. Niveles de alerta y criterios de activación

| Niveles | ALERTA | DESCRIPCIÓN | ACTIVIDADES |
|---|---|---|---|
| **1** | **Normalidad** | La operación de las ICC del sector se encuentra en estado habitual y/o normal. No hay presencia de incidentes cibernéticos reportados o conocidos, dirigidos a las ICC de las entidades financieras, diariamente se conocen nuevas vulnerabilidades y amenazas, pero no constituyen un riesgo a estas. No existen alertas de ataques a nivel mundial, regional o local, sobre la materialización de una o varias amenazas reales o potenciales contra las ICC. | Acciones de tipo preventivo, monitoreo y protección a cargo de los propietarios/operadores de la ICC del sector.<br>Reportar información sobre incidentes cibernéticos y vulnerabilidades a las autoridades de Ciberseguridad y Ciberdefensa.<br><br>Se prueban los planes de continuidad y recuperación.<br><br>Se verifica la efectividad de los controles y el cumplimiento de las medidas de seguridad impartidas; así como se crean e implementan nuevos controles de requerirse, para evitar situaciones de riesgo en la ICC.<br>Mantenimiento de medidas de Ciberseguridad generales y actuaciones para evitar situaciones de riesgo en la ICC. |
| **2** | **Bajo** | Se identifican o presentan incidentes cibernéticos o amenazas aisladas, independientes entre sí, que afectan hasta en su 20% las entidades y/o servicios esenciales, cuyo efecto no impacta potencialmente a los clientes. | Se implementan medidas de monitoreo y protección a las ICC por parte de sus operadores y propietarios; asegurando su óptimo control y segura operación. |

| Niveles | ALERTA | DESCRIPCIÓN | ACTIVIDADES |
|---|---|---|---|
| | | Los incidentes se pueden controlar y mitigar haciendo uso de las estrategias de prevención y atención básicas. | |
| **3** | **Medio** | Se presentan incidentes cibernéticos relacionados entre sí, en varias entidades del sector, existiendo probabilidad de indisponibilidad de los servicios básicos o esenciales, en hasta un 40% en las entidades financieras.<br><br>Las estrategias preventivas pueden ser insuficientes.<br><br>Existen informaciones aisladas a nivel mundial, sobre potenciales amenazas a las ICC. | Se refuerzan las medidas de protección, y se activan e implementan planes y mecanismos de contingencia y resiliencia en las ICC, por parte de sus operadores y propietarios, reforzando el control de posibles objetivos y fortaleciendo la protección de los centros de IT/OT críticos.<br><br>Los líderes de la mesa sectorial citarán al Comité Técnico, quien determinará la necesidad de convocar al Comité Directivo. |
| **4** | **Alto** | Los incidentes cibernéticos o amenazas potenciales o reales han comprometido o pueden comprometer y afectar activos cibernéticos en entidades que brindan servicios esenciales. Se ha producido o pueden producir indisponibilidad de servicios críticos provistos por el sector, hasta en el 50% de sus entidades o servicios. | Aprobar, modificar, complementar y crear estrategias a seguir para operar o prestar el servicio afectado.<br><br>El Comité Técnico convocará al Comité Directivo. |
| **5** | **Emergencia** | Los incidentes cibernéticos o amenazas reales o potenciales han comprometido o pueden comprometer y afectar activos cibernéticos en entidades y compañías de criticidad muy alta.<br>Se ha producido o podrá producir indisponibilidad de | El Comité Directivo solicitará al Gobierno y a las Fuerzas Militares el apoyo necesario para la gestión de los incidentes que hayan comprometido la infraestructura crítica cibernética nacional. |

| Niveles | ALERTA | DESCRIPCIÓN | ACTIVIDADES |
|---|---|---|---|
| | | servicios críticos provistos por el sector, en más del 50% de sus compañías o servicios. Así como se ha estimado un Impacto crítico a la población, la economía colombiana, su medio ambiente, la seguridad y defensa nacional. | |

## 5.3. Roles, Funciones y Responsabilidades

**Comité Técnico:** tendrá una supervisión primaria sobre los eventos cibernéticos que afecten al sector, coordinará las acciones durante una crisis y será el principal punto de control para el nivel de alerta de amenaza cibernética. El Comité se apoyará en el CSIRT Financiero para obtener información técnica y el diagnóstico de la situación.

Así mismo, cada miembro debe mantener informada a la alta dirección de su entidad sobre novedades importantes, deberá actualizar el plan sectorial de protección y defensa de ICC teniendo en cuenta los análisis de riesgo cibernético y sus lineamientos estratégicos.

Después del incidente, deberá evaluar las lecciones aprendidas y definir una propuesta de comunicado de la información a transmitir a la opinión pública al finalizar el incidente para que sea revisado por las áreas de comunicaciones de cada entidad.

**Comité Directivo**[4]
Deberá activarse en caso de presentarse una alerta alta o emergencia cibernética.
Deberá definir qué miembro será el vocero para transmitir información a los medios de comunicación y a la comunidad en el momento de la crisis cibernética, esta persona será el único vocero de las comunicaciones masivas ante las diferentes audiencias relacionadas con el incidente.
Gestionar y definir las políticas necesarias para la atención de la crisis cibernética.
Dar conformidad para el retorno a la normalidad.
Evaluar la gestión realizada durante la crisis con el fin de mejorar las políticas de respuesta a incidentes cibernéticos.

**Respuesta y comunicación**: las entidades vigiladas se acogen a lo dispuesto en la Circular 007 (Requerimientos Mínimos Para La Gestión De La Seguridad De La Información Y La Ciberseguridad) de 2018 numeral 7.3.

> *7.3.1. 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] Cada vez que se active el Comité Directivo, este toma el liderazgo de la gestión de la crisis cibernética, sin desactivar al Comité Técnico, el cual seguirá funcionando con sus actividades de monitoreo, seguimiento y control.

*7.3.3. 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.*

### 5.3. Componente Sector Hacienda

Para les entidades Públicas que conforman el sector financiero, el Ministerio de Hacienda y Crédito Público en su calidad de cabeza de sector, propondrá la conformación y formalización de un Comité Técnico de Seguridad, que en la práctica ha venido funcionando con el acompañamiento de MinTic, con el objetivo de desarrollar las Estrategias de Gobierno en Línea (incluyendo su componente de Seguridad) y la actual de Gobierno Digital (que reemplazó a Gobierno en Línea), además de la de Seguridad Digital.

El Director de Tecnología del Ministerio de Hacienda, dentro de las atribuciones que establece el Decreto 415 de 2016, tiene la responsabilidad de generar los lineamientos para el desarrollo de lo contenido en este plan, tanto para la entidad como para el sector hacienda. A saber:

*"Artículo 2.2.35.5. Roles. Para lograr el funcionamiento armónico de la dependencia o instancia ejecutora del accionar estratégico de las Tecnologías y Sistemas de la Información, el director, jefe de oficina o coordinador, deberá cumplir los siguientes roles:*
*1-Orientadores. Este rol será ejercido por las dependencias de Tecnologías y Sistemas de la Información pertenecientes a los organismos cabeza de sector o a los que hagan sus veces y serán los responsables de proponer, coordinar y hacer seguimiento a la implementación de* ***las normas y políticas públicas a las cuales deben sujetarse los entes adscritos o vinculados al sector respectivo****, en materia de gestión de las tecnologías de la información y las comunicaciones,"*

Por tanto, el Comité Técnico del Sector Hacienda estará conformado por el Director de Tecnología o quien haga sus veces y por el responsable de la Seguridad de la Información de cada entidad del sector, más un representante del CSIRT Gobierno (Administrado por MinTic).

Este Comité, coordinará las acciones durante una crisis y será el principal punto de control para el nivel de alerta de amenaza cibernética. El Comité se apoyará en el CSIRT Gobierno y en el colCERT, para obtener información técnica y el diagnóstico de la situación.

Así mismo, cada miembro debe mantener informada a la alta dirección de su entidad sobre novedades importantes; después del incidente, deberá evaluar las lecciones aprendidas y preparar un informar para el Comité Sectorial de Gestión y Desempeño Institucional del sector, que realizaría las funciones equivalentes al Comité Directivo del componente privado del sector.

Se adoptarán como buena práctica, y con miras a estandarizar los conceptos, los niveles de alerta y criterios de activación definidos en este documento.

Cabe anotar que, aunque no todas las entidades del sector hacienda administran y/o gestionan Infraestructuras Críticas, deben participar en el Comité técnico como mecanismo de cooperación y apoyo sectorial

## 5.4 Directorio

| Entidad | Rol | Teléfono o Celular |
|---|---|---|
| **ASOBANCARIA** | Dirección de Gestión Operativa y Seguridad | 3266600 Ext 1382 |
| **DAVIVIENDA** | Departamento Seguridad de la Información | 3300000 ext. 53320 |
| **BANCOLOMBIA** | Ciberseguridad y Seguridad de la Información | (4) 4041531 |
| **BBVA** | Seguridad de la Información | 3822600 |
| **COLPATRIA** | Riesgo de TI y Ciberseguridad | 7456300 |
| **CITIBANK** | Seguridad de la Información | 4854000 ext. 1-12796 |
| **ITAU** | Seguridad de la Información | 5818181 ext 2-4079 |
| **FASECOLDA** | Seguridad de la Información | 5940200 |
| **Sociedad de Activos Especiales S.A.E** | Oficina Gestión de la Información | 7431444 |
| **ASOBOLSA** | Seguridad de la Información | |
| **ASOFIDUCIARIAS** | Seguridad de la Información | 60 60 700 |
| **SUPERSOLIDARIA** | Seguridad de la Información | 7560557 ext. 10152 |
| **SEGUROS DEL ESTADO** | Seguridad de la Información | |
| **Superintendencia Financiera de Colombia - SFC** | Delegatura para Riesgos Operativos | 5940200 |
| **Ministerio de Hacienda y Crédito Público.** | Dirección de Tecnología | 3811700Ext. 2502 |
| **Unidad de Proyección Normativa y Estudios de** | Subdireción de Gestión Institucional | 3811700 Ext 2128 |

| | | |
|---|---|---|
| **Regulación Financiera - URF -.** | | |
| **Contaduría General de la Nación – CGN –** | Grupo de Apoyo Informático | 4926400 |
| **COLJUEGOS. (Empresa Industrial y Comercial del Estado Administradora del Monopolio Rentístico de los Juegos de Suerte y Azar)** | Oficina de Tecnologías de la Inormación | 7423308 Ext 201 |
| **FOGAFIN (Fondo de Garantías de Instituciones Financieras)** | Departamento de Tecnologías de la Información | 3394240 Ext. 176 |
| | Oficial de Seguridad | 3394240 Ext. 176 |
| **SAE (Sociedad de Activos Especiales)** | Oficina Gestión de Información | 7431444 Ext. 505 |
| | Oficial de Seguridad | 7431444 Ext. 505 |
| **UIAF (Unidad de Información y Análisis Financiero)** | Subdirección de Informática | 288 5222 Ext. 159 |
| **La Previsora Seguros** | Dirección de Tecnología | 3485757 Ext. 6899 |
| **Fiduciaria La Previsora (FIDUPREVISORA)** | Gerencia de Tecnología | 594 5111 Ext 1900 |
| **Superintendencia Financiera de Colombia (SFC)** | Dirección de Tecnología | 5940200 ext. 1314 |
| **POSITIVA Compañía de Seguros** | Oficina de Tecnologías de la Información | 6502200 Ext 10500 |
| | | 6502200 Ext 10500 |
| **Dirección de Impuestos y Aduanas Nacionales - DIAN** | Subdireción de Gestión de Tecnología de Información y Telecomunicaciones | 6079999 Ext 903401 |
| | | |

# CAPITULO VI. MONITOREO Y MEJORA CONTINUA

## 6.1. Monitoreo

Para el desarrollo y fortalecimiento de la protección y defensa de las ICCN en el país, la mesa de trabajo del sector financiero realizará una revisión anual del documento con el fin de actualizar las estrategias para el manejo de crisis cibernética (con base en buenas prácticas implementadas). Así mismo, deberá evaluar las lecciones aprendidas después de la ocurrencia de algún incidente que active los niveles de alerta establecido.

## 6.2. Mejora Continua

La mesa de trabajo de Protección de Infraestructura Crítica Cibernética del sector financiero debe generar espacios para obtener información que permita mejorar la respuesta ante futuros incidentes de ciberseguridad, esto con el fin de identificar buenas prácticas y oportunidades de mejora.

Se deben considerar las siguientes preguntas al momento de realizar la revisión del documento.

- ¿Cuáles fueron los hechos?
- ¿Se anticiparon las consecuencias para el sector financiero?
- ¿Los miembros de los comités establecidos para la gestión y recuperación de la ICC eran los adecuados?
- ¿Se compartió la información adecuadamente entre los miembros de los comités y demás personas involucradas?
- ¿Qué se hizo para contrarrestar los efectos negativos del incidente?
- ¿Hay algo que se pueda hacer para evitar un incidente similar en el futuro?
- ¿Puede el este incidente desencadenar otras crisis potenciales? ¿Cuáles?
- ¿Qué acciones correctivas y preventivas se pueden tomar?

# CAPITULO VII CONCLUSIONES

La protección y resiliencia de la ICC del sector financiero requiere de la participación y actuación de todas las partes intervinientes, así como de un trabajo articulado. Para ello es fundamental el apoyo y colaboración del Consejo Superior de Seguridad Digital, Protección y Defensa del Ciberespacio, así como el cumplimiento y seguimiento de las guías, certificación y programas de sensibilización que promuevan el fortalecimiento de capacidades de respuesta y recuperación de incidentes cibernéticos.

Es de resaltar la generación y desarrollo de diferentes dinámicas en la mesa de trabajo del sector, entre las cuales podemos resaltar:

El trabajo mancomunado y en equipo, no solo entre las entidades bancarias sino entre entidades públicas y privadas, compartiendo experiencias, iniciativas y buenas prácticas que redundarán en la mejora de los procesos de las mismas, en especial de las públicas que pueden aprovechar el conocimiento de prácticas y regulaciones, que, aunque no les sean exigibles, si podría adoptar como buena práctica.

La incorporación de diferentes actores a la mesa de trabajo del sector durante el desarrollo del proyecto, con aportes e ideas muy valiosas, y, aunque sus realidades no estén totalmente incorporadas en este documento, son una justificación y motivación desde ya, para realizar una segunda versión del documento, incluyendo las necesidades y expectativas de estos actores, entre los cuales podemos incluir a Aseguradoras, Fiduciarias, Corredores de bolsa, Pasarelas de pago, entidades bursátiles, entidades cooperativas y del sector solidario, entre otras.

## RECOMENDACION

El sector financiero colombiano destaca los esfuerzos del Comando Conjunto Cibernético y sugiere continuar generando iniciativas como esta, entre todas las partes de la estructura de protección, de manera conjunta, integrada, coordinada con personal idóneo y altamente calificado, con alto sentido de compromiso institucional, a fin de alcanzar el éxito en el fortalecimiento y consolidación de la Ciberseguridad y Ciberdefensa en el contexto nacional.

# BIBLIOGRAFÍA


Cano, J. (2017). La ventana de AREM. Una estrategia para anticipar los riesgos y amenazas en ciberseguridad empresarial. *Isaca Journal, 5*.

CCOC. (2016). *Sectores Estratégicos de la República de Colombia desde la Óptica Cibernética.* Comando General - Fuerzas Militares.

Cepal. (2013a). *Economía digital para el cambio estructural y la igualdad.* Cepal.

Cepal. (2013b). *Estrategias TIC ante el desafío del cambio estructural en América Latina y el Caribe: balance y desafíos de renovación.* Cepal.

CONPES. (2011). *Lineamientos de política para ciberseguridad y ciberdefensa - 3854.* Consejo Nacional de Política Económica y Social.

CONPES. (2011). *Política Nacional de Seguridad Digital - 3701.* Consejo Nacional de Política Económica y Social.

Deutscher, S., & Yin, W. (2016). Standards and Frameworks for Cybersecurity . En *The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity* (Antonucci, D. ed.). Wiley.

Home Land Security. (2018). Critical Infrastructure Security.

Katz, R. (2015). *El Ecosistema y la Economía Digital en América Latina.* Telefónica, CEPAL, CAF. Obtenido de http://repositorio.cepal.org/bitstream/11362/38916/1/ecosistema_digital_AL.pdf

Katz, R., & Callorda, F. (2015). *Impacto de arreglos institucionales en la digitalización y el desarrollo económico de América Latina.*

MinTIC. (2018). *Colombia TIC - Vive Digital*. Obtenido de Estadísticas sector TIC: Internet Nacional : http://colombiatic.mintic.gov.co/estadisticas/stats.php?&pres=content&jer=1&cod=&id=32#TTC

OEA. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* OEA-BID.

SFC. (junio de 2018). Circular Externa 007 de 2018.