Constitución de un CSIRT para una Entidad Financiera en Colombia

Héctor Mauricio Sánchez, Alexander Rodríguez Parra
Estudiantes Maestría en Seguridad de la Información
Departamento de Ingeniería de Sistemas y Computación
Universidad de Los Andes. Bogotá, Colombia
Diciembre de 2019

1 Introducción

1.1 El Estado Colombiano y el Sector Financiero en Colombia

El Estado Colombiano, a través del Consejo Nacional de Política Económica y Social (Conpes), genera en 2011 el **CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa**[1] y en 2016 el **CONPES 3854 Política Nacional de Seguridad Digital**[2], con el fin de establecer un marco normativo e institucional para generar una postura de seguridad digital propia del Estado, que salvaguarde a la nación de los riesgos que nos presenta la transformación digital y el ciberespacio.

Estas políticas garantizan que Estado Colombiano promueva todos los esfuerzos necesarios para lograr establecer una estrategia de ciberseguridad y ciberdefensa basada en la gestión de riesgos en seguridad digital, que se fundamente bajo principios y objetivos claros que le permitan fortalecer sus capacidades para enfrentar las amenazas de una manera estratégica frente a la adopción de la era digital, tales como:

- Crear y fortalecer las instancias y/u organismos que ejercen responsabilidades de ciberseguridad y ciberdefensa como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), Comando Conjunto Cibernético de las Fuerzas Militares (CCOC), Centro Cibernético Policial de la Policía Nacional (CCP), Ministerio TIC (CSIRT Gobierno), entre otras.
- Establecer las responsabilidades de gestión y atención de amenazas e incidentes informáticos que puedan comprometer al Estado.
- Fomentar el desarrollo de las capacidades del Estado para la protección, prevención, atención y respuesta de ataques cibernéticos, desde diferentes actores y a todo nivel:
    - Estado, instituciones y organismos con responsabilidades de ciberseguridad y ciberdefensa.
    - Entidades y servidores públicos, Empresas del sector privado.
    - Ciudadanía.
- Establecer mecanismos estratégicos de colaboración y cooperación con países, entidades y otros organismos (públicos y privados, internacionales, de industria, etc.), que permitan desarrollar las capacidades en términos de atención y respuesta ante las amenazas, vulnerabilidades, eventos e incidentes de ciberseguridad que puedan poner en riesgo la seguridad digital del país y de sus habitantes.

[1] CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa. Julio de 2011 https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.
[2] CONPES 3854 Política Nacional de Seguridad Digital en Colombia https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.

- Fortalecimiento del marco legislativo en Colombia, a través de la inclusión de políticas y decretos que permiten robustecer el marco de las políticas de ciberseguridad y ciberdefensa dadas en el CONPES 3701 y 3854.
- Diseñar y fortalecer los planes de capacitación y formación de las personas responsables de ciberseguridad y ciberdefensa, así como de los habitantes del Estado colombiano.

Las Entidades Financieras en Colombia reconocen que están en un ecosistema digital cambiante, en el cual todos los actores evolucionan y así como aparecen nuevas riesgos, amenazas y vulnerabilidades, incluso nuevas metodologías de ataque conocidas en la industria como Tácticas, Técnicas y Procedimientos, debemos establecer y **construir las metodologías necesarias para crear esa capacidad y cultura de prevención, reacción, respuesta, recuperación e investigación, en procura de ser resilientes**, y en tal propósito, el desarrollo de las capacidades para gestionar a los incidentes de seguridad digital se vuelven un punto primordial en la estrategia digital de la Entidad.

1.2 Impacto de los Incidentes de Seguridad Digital

En el contexto local es complejo relevar información relacionada con incidentes de seguridad relacionados con el sector financiero, así como monetizar el impacto de su materialización, sin embargo, se toman como referencia algunas cifras de estudios internacionales, tales como el estudio de IBM "***Cost of a Data Breach Report 2019***[3]", realizados en otros contextos geográficos, muestran que en promedio el 10% de brechas de seguridad suceden en el sector financiero, con un impacto económico importante, presentando un valor de referencia de 210 dólares el costo promedio por registro para el sector Financiero.

En el ámbito Latinoamericano la Organización de los Estados Americanos (OEA) realizó un reporte que muestra los principales aspectos de ciberseguridad en Entidades financieras bancarias, "***Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe***"[4]. En el análisis se muestra cifras interesantes en un ámbito más cercano, para las cuales se destacan algunas como:

- El 55% de las entidades bancarias obtuvieron un EBITDA a 31 de diciembre de 2017 entre US $0 y USD $10 millones, de los cuales el 43% de las entidades asignan entre el 1% y el 5% del EBITDA en seguridad digital.
- ACCENTURE (2017) encontró que "cuatro de cada diez entidades bancarias gastan entre un 7% y un 10% de su presupuesto de TI en ciberseguridad".
- El 40% de los Bancos identificaron ocurrencia de eventos de malware diariamente y el 65% manifiestan que fueron víctimas de ataques exitosos.
- Respecto a la gestión, respuesta y recuperación ante incidentes de seguridad digital, el 51% de las entidades bancarias de la región contaron con estrategias de gestión, respuesta y recuperación ante incidentes de seguridad digital, sin embargo, manifiestan que sus procesos deben ser actualizados y optimizados.
- Se estima que el retorno sobre la inversión en seguridad digital (incluidos aspectos de seguridad de la información, ciberseguridad y prevención del fraude usando medios digitales) equivale aproximadamente a un 24,1%.

---

[3] "IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years.

[4] "Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf.

El estudio presenta el estado de ciberseguridad y, para nuestro caso, la capacidad de responder ante un ciber incidente por parte de las compañías del sector, lo que presenta una aproximación argumentada del entendimiento y claridad de las organizaciones en detectar diferentes vectores de ataques a los cuales está expuesto, y plantea la necesidad de fortalecer las capacidades necesarias para dar respuesta a los ciber incidentes.

1.3 ¿Por qué fortalecer dichas capacidades en el Sector?

Es fundamental contar en las organizaciones con Equipos de Respuesta a Incidentes de Seguridad de la Información y Ciberseguridad con el fin de tener capacidades necesarias para gestionarlos adecuadamente y reaccionar de manera oportuna, óptima y eficaz, y sí minimizar los riesgos y el impacto que puede ocasionar la materialización de los mismos.

Como punto inicial, el Estado Colombiano propone a través de las políticas CONPES 3701 y 3854 objetivos estratégicos alineados a la prevención y protección del ecosistema digital frente a los ciber incidentes tal y como se muestra en el siguiente apartado: *"Promover el desarrollo de capacidades locales/sectoriales así como la creación de CSIRTs sectoriales para la gestión operativa de los incidentes de ciberseguridad en la infraestructura crítica nacional, el sector privado y la sociedad civil."* Esto muestra la importancia de establecer Equipos de Respuesta a Incidentes de Seguridad a nivel empresarial, sectorial y Nacional. Es fundamental entender que la implicación del desarrollo de un CSIRT Sectorial, supone una responsabilidad inmediata frente a las Entidades en pro de tener las capacidades que le permitan la interacción y la entrega de valor en el ámbito de colaboración en la comunidad que se genera.

El ámbito Regulatorio Colombiano, a través de los organismos de control y vigilancia, y alineado con las políticas dictadas por el Estado, constituyen políticas y regulaciones específicas que buscan promover el establecimiento de Centros de Respuesta a Incidentes de Seguridad para la gestión y respuesta de los riesgos cibernéticos. Algunos de estos requerimientos, están estipulados como parte de la **Circular Básica Jurídica 029 de la Superintendencia Financiera de Colombia - Parte I - Título 4 Capítulo Ciberseguridad**[5], en la cual se estipulan las necesidades de establecer y fortalecer las capacidades de gestión de riesgos y respuesta a incidentes cibernéticos.

Adicionalmente, la seguridad digital es un componente que debe abordarse de manera estratégica en las organizaciones, tal y como se reconoce en la industria de ciberseguridad y en las políticas nacionales emitidas por el Estado. Por lo cual es fundamental contar con los mecanismos necesarios que promuevan el desarrollo de capacidades de las empresas del sector, para responder de manera oportuna y eficaz frente a la gestión de los riesgos e incidentes de ciberseguridad.

2 Propuesta de la Solución

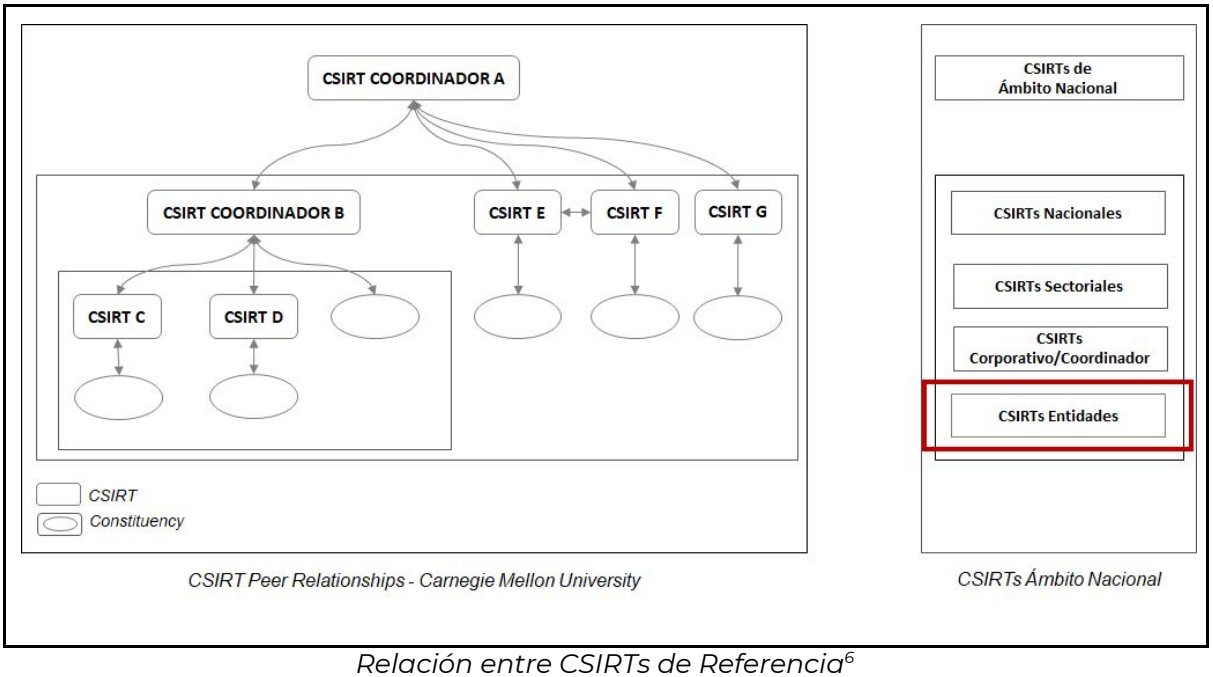
Realizar el planteamiento de la **Constitución de un Equipo de Respuesta a Incidentes para una Entidad del sector Financiero en Colombia**, con el propósito de fortalecer la estrategia de Ciberseguridad con respecto a las exigencias de los estándares internacionales, los lineamientos de la normatividad nacional y las mejores prácticas de la industria.

---

[5] (n.d.). Circular Externa 007 de 2018 - Superintendencia Financiera. https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc

2.1 Ámbito de los CSIRTs en Colombia

En el ámbito de los CSIRTs se establecen diferentes tipos de Equipos de Respuesta a Incidentes y en el ámbito colombiano, empiezan a sobresalir algunos que interactúan de manera consistente en el Sector Financiero. Los **CSIRTs Nacionales** como el ColCERT, CCP de la Policía Nacional y el Comando Conjunto Cibernético tienen responsabilidades en términos de protección del Estado, la infraestructura crítica cibernética del país y la ciudadanía en general, esto hace que los incidentes que puedan afectar a cualquiera de los sectores, incluidos el Financiero cuenten con un apoyo transversal para el manejo de los mismos. Los **CSIRTs Sectoriales**, se establecen con el propósito de colaborar en el ámbito de aplicación de las empresas y organizaciones de negocios similares, por lo cual se encuentran CSIRTs Financieros los cuales se especializan en establecer y estructurar servicios específicos para el sector. Los **CSIRTs Coordinadores o Corporativos**, surgen en la estructura, como estructuras que permiten utilizar unidades de negocio compartidas y especializadas para grupos económicos y financieros, por lo que se cuentan con iniciativas de forma de contar con equipos de respuesta a incidente especializados que respondan no solo a las necesidades de una entidad u organización, sino que puedan prestar sus servicios a todas las entidades de un holding o grupo económico y para nuestro caso, Financiero. Finalmente, se encuentran los **CSIRTs de las Entidades**, los cuales son equipos de respuesta específicos y propios para gestionar y atender los incidentes de seguridad propios a su entidad.



Relación entre CSIRTs de Referencia[6]

El desarrollo de la propuesta de solución, está orientada al CSIRT de la Entidad, identificando los principales componentes a ser considerados en la estructuración de los equipos e identificando las recomendaciones de acción hacia un camino efectivo de implementación.

[6] *Tomado de Handbook for Computer Security Incident Response Teams*
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf

2.2 Componentes de la Solución Propuesta y Resultados Obtenidos

La constitución de los equipos de respuesta a incidentes de seguridad de las Entidades Financieras en Colombia debe considerarse como estratégica para la organización.

La metodología considerada representa las principales consideraciones para la definición, estructuración, implementación, operación y sostenibilidad del CSIRT de la Entidad, tales como las consideraciones corporativas para la constitución del equipo de respuesta, las capacidades en todo ámbito (tecnológicas, personas, procesos), los servicios que se prestan hacia la Entidad, así como las interacciones con los organismos de control y de colaboración y aspecto fundamentales en el apoyo a la estrategia de respuesta a incidentes como los planes de respuesta, alineación con el plan de continuidad de negocio y de recuperación ante desastres, interacción con el comité de crisis y soporte frente al manejo de las comunicaciones.

Estas consideraciones, que aunque se encuentran en el visible de las metodologías y estándares de la industria, se propone que se encuentren claramente identificadas, definidas o aplicadas en la hoja de ruta de los equipos estructurados.

A partir de las fuentes de información investigadas y del conocimiento del sector financiero a través de escenarios de entendimiento y profundización, se identifican y determinan los componentes abordados, y se mencionan algunos de ellos, como muestra referencial de la solución y de los resultados logrados:

Establecer una **estrategia en la respuesta a ciber incidentes** para la definición, estructuración, implementación, operación y sostenibilidad del CSIRT de la Entidad, así como de los servicios que serán prestados a la organización, con el propósito de establecer los lineamientos adecuados para la entrega de valor tanto a la organización, como a la comunidad a la cual pertenece.

Presentar la **estructuración del portafolio de servicios del CSIRT** para proteger y asegurar al negocio frente a la materialización de incidentes de seguridad de una manera adecuada y oportuna acorde a las necesidades y requerimientos a resolver. La estructuración detallada de los servicios permite reconocer de forma adecuada y consistente las características presentadas y el valor que tienen la Entidad al establecerlo. El **servicio de Gestión de Incidentes de Seguridad** consiste en recibir, analizar, responder y coordinar el programa y los planes de respuesta a incidentes de seguridad digital de la organización.

La estrategia de respuesta a incidentes de seguridad digital, promueve porque las operaciones sean **Ciber Resilientes**, lo que implica que el CSIRT estará en una continua interacción con los equipos de BCP y DRP orquestando las implicaciones de un ataque cibernético y probando continuamente las capacidades de respuesta cuando éste tipo de incidentes se materialicen. Así mismo, se considera el **Manejo de la Ciber Crisis** como componente fundamental para apoyar la toma de las decisiones de frente a la materialización de un ciber incidente.

Los lineamientos a nivel **legal** y de **cumplimiento**, se establecen como pilar del tratamiento y respuesta de los ciber incidentes, para lo cual se denota los principales ítems a ser valorados para dar el manejo adecuado de los mismos.

Las **capacidades humanas** es un factor primordial para que el CSIRT preste servicios de valor a la Entidad y a la comunidad a la cual pertenece. Es imprescindible que el personal que conforma el CSIRT esté compuesto por perfiles con un alto grado de conocimiento y experiencia que aporte en los diferentes niveles y responsabilidades en el proceso de gestión y respuesta a incidentes de seguridad digital.

Establecer las capacidades físicas, operativas y tecnológicas necesarias para la prestación de los servicios a la organización y que permitan apropiar y optimizar el tratamiento de los ciber incidentes. En tal sentido se **establecen los recursos** a ser considerados para la entrega y optimización de los servicios.

Realizar la aproximación a un **presupuesto de inversión y de operación del CSIRT** que permite obtener el entendimiento de la estructura del CSIRT como un área de valor para el negocio, la cual debe contar con asignaciones específicas para su implementación y sostenibilidad. La relación costo - beneficio de implementar recursos tecnológicos con valores de mercado, pretende dar un valor cercano de la realidad de inversión, así como definir los esquemas para encontrar el punto de equilibrio a un plazo razonable.

La **implementación de herramienta para gestión y automatización de incidentes** de gestión de incidentes de seguridad y ciberseguridad, y contar con un sistema de información centralizado para registrar, documentar y dar seguimiento a los incidentes identificados para lo cual, se ha seleccionado la herramienta RTIR (Request Tracker for Incident Response), solución ampliamente usada por diferentes CERTs a nivel mundial.

El propósito de la razón de ser de los CSIRT se fundamenta en los **principios de colaboración e intercambio de información**, con el fin de robustecer las capacidades propias actuales.

3 Recomendaciones

Estar preparados y con las capacidades necesarias para enfrentar los retos que la evolución tecnológica trae consigo, es fundamental para el negocio, es por ello que contar con una estrategia sólida, eficiente y eficaz para gestionar y responder a los ciber incidentes, permite garantizar valor desde muchas aristas, como:

- Proteger al negocio ante los efectos negativos que tienen los incidentes de seguridad digital (Impacto Reputacional, pérdida de clientes, pérdidas económicas, incumplimientos y sanciones regulatorias, etc.)
- Crear y fortalecer las capacidades para gestionar y responder a los incidentes de seguridad digital, a través de la constitución de un CSIRT y el establecimiento de estrategias de gestión y respuesta.
- Minimizar los riesgos de ciberseguridad durante todo el ciclo de vida de los incidentes (prevenir, proteger, contener, mitigar, erradicar, recuperar y realizar acciones post incidente).
- Ser un negocio Ciber Resiliente, través de apropiación de estrategias de respuesta que involucren escenarios de recuperación y continuidad frente a ataques digitales.

4 Referencias

- CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa - MinTIC 14. Julio de 2011 https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf.
- CONPES 3854 Política Nacional de Seguridad Digital en Colombia https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf.
- Circular Externa 007 de 2018 - Superintendencia Financiera. https://www.superfinanciera.gov.co/descargas/institucional/pubFile1031741/ce007_18.doc
- IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years.
- *RTIR for Incident Manager* del International for Telecomunication Union https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RTIR.pdf
- Handbook for Computer Security Incident Response Teams
- https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
- CSIRT Services Framework - FIRST - Improving Security Together
- https://www.first.org/education/csirt_services_framework_v2.0
- Computer Security Incident Handling Guide - NIST Page. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf