REVISTA FAECO SAPIENS
ISSN L 2644-3821

Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens

Indexada

Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112

Recibido: 18/04/21 Aceptado: 01/5/21

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES CIBERNÉTICOS PARA EL SECTOR BANCARIO EN PANAMÁ

Proposal for the implementation of a cyber incident response team for the banking sector in Panama

Iván Ho
Universidad de Panamá, Facultad de Administración de Empresas y Contabilidad, Panamá,
Email: ivanhoq@gmail.com https://orcid.org/0000-0001-8634-0863
Damon Sánchez
Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales,
Panamá, Email: deimonalex@gmail.com https://orcid.org/0000-0002-0081-8510
Ericka Rodríguez
Universidad Tecnológica de Panamá, Facultad de Ingeniería de Sistemas Computacionales,
Panamá, Email: ericka1902@yahoo.es https://orcid.org/0000-0003-3465-1445

RESUMEN

El avance de la tecnología de la información ha abierto las puertas a nuevas posibilidades de delincuencia antes imaginables. Los perjuicios ocasionados a menudo no llegan a descubrirse o castigarse. El aumento de los ataques informáticos propone un nuevo reto en el cual algunos creen que solo es cuestión de tiempo hasta sufrir las secuelas de algún incidente de seguridad que podría estar relacionado con el robo de información sensitiva. En el caso de que estos sistemas sufran un ataque, causará un gran impacto en la economía y en la seguridad de los procesos administrativos y financieros, por consiguiente, además de la comunidad de expertos e investigadores, existen equipos dedicados a responder con rapidez ante nuevos riesgos. En este entorno de evolución los ataques informáticos y otras amenazas, cobran relevancia, los equipos de respuesta a incidentes de seguridad (**CSIRT** por las siglas de Computer Security Incident Response Team). CSIRT es un Centro de Respuesta a Incidentes de Seguridad, también conocido como CERT, que tiene como funciones atender y dar respuesta a incidentes de seguridad informática. Debemos evadir todos los riesgos, si se materializa, sus consecuencias puedan ser mitigadas y las actividades primordiales restablecidas en el menor tiempo posible, con el **impacto mínimo** aceptable para las entidades bancarias.

Palabras claves: CSIRT, CERT, incidente, cibernético.

ABSTRACT

The advancement of information technology has opened the doors to new crime possibilities previously imaginable. The damage done is often not discovered or punished. The increase in computer attacks poses a new challenge in which some believe that it is only a matter of time until suffering the consequences of a security incident that could be related to the theft of sensitive information. In the event that these systems suffer an attack, it will cause a great impact on the economy and on the security of administrative and financial processes, therefore, in addition to the community of experts and researchers, there are teams dedicated to responding quickly to new risks. In this evolving environment, computer attacks and other threats, security incident response teams (CSIRT for the acronym of Computer Security Incident Response Team) gain relevance. CSIRT is a Security Incident Response Center, also known as CERT, whose functions are to attend and respond to computer security incidents. We must avoid all risks, if they materialize, their consequences can be mitigated and the essential activities restored in the shortest possible time, with the minimum acceptable impact for banks.

Keywords: CSIRT, CERT, incident, cybernetic

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

INTRODUCCIÓN

Hoy día los equipos de respuesta a incidentes de seguridad de la información, juegan un papel crucial para todo tipo de empresa pública o privada, ya que sirven de apoyo en las etapas de detección, respuesta y mitigación del proceso de gestión de incidentes de seguridad de la información y ciberseguridad. Este artículo se enfoca en el estudio de los diferentes tipos de equipos de respuestas a incidentes de ciberseguridad, su historia, servicios, modelo estructural, así como los requisitos de infraestructura tecnológica y normativas bancarias panameñas relacionadas con la seguridad de la información y ciberseguridad, para la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que conforman la infraestructura crítica del sistema bancario del país.

Lo anterior permitirá determinar cuál será el mejor modelo estructural a implementar, servicios a prestar, tomando en cuenta la regulación bancaria que deben cumplir los bancos con licencias otorgadas por la Superintendencia de Bancos de Panamá y otros recursos necesarios para la propuesta con miras a la implementación de un equipo de respuesta a incidentes de ciberseguridad que beneficie al sector bancario panameño.

La República de Panamá, mediante el Decreto Ejecutivo No. 709 del 26 de septiembre de 2011, publicado en la Gaceta Oficial No. 26880, 27 septiembre 2011, donde se creó el “CSIRT PANAMÁ” Equipo Nacional de Respuesta a Incidentes de Seguridad de la Información del Estado Panameño, que tiene entre sus objetivos la prevención, tratamiento, identificación y resolución de ataques a incidentes de seguridad sobre los sistemas informáticos que soportan la infraestructura crítica del país.

El centro bancario de nuestro país está conformado por “dos (2) bancos oficiales, cincuenta y siete (57) bancos divididos en cuarenta (40) de licencia general y diecisiete (17) de licencia internacional”, de acuerdo al sitio web de la Superintendencia de Bancos de Panamá del 21 de marzo de 2021 (www.superbancos.gob.pa).

La competencia y demanda de los clientes ha llevado a los bancos, así como a otras industrias a la transformación digital de los productos y servicios que ofrece, teniendo así un abanico de canales electrónicos a través de los cuales sus clientes pueden acceder y efectuar sus diferentes consultas y transacciones y así tener el servicio de la banca.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

Lo anterior ha elevado el nivel de riesgo del sector bancario panameño a ser blanco de ataques de diferentes incidentes de seguridad (ataque de denegación de servicios (DDoS), app defacement, phishing, pharming, acceso no autorizado, entre otros) que los exponen a pérdidas monetarias, así como a daños en la reputación y confianza por parte de sus clientes y público en general, en caso de materializarse un incidente.

La norma bancaria panameña, a través del Acuerdo 3-2012 de la Superintendencia de Bancos de Panamá, del 22 de mayo de 2012, "por el cual se establecen lineamientos para la gestión del riesgo de la tecnología de la información", en su artículo 11, instaura funciones a la unidad de seguridad de la información, tales como el monitoreo y atención de los incidentes de seguridad de los sistemas informáticos, así como la notificación de los ataques al ente regulador antes mencionado.

Con lo cual se traza como objetivo de este artículo proponer la estructura para la implementación de un equipo de respuesta a incidentes de ciberseguridad para el sector bancario privado panameño. La transformación digital de los servicios ofrecidos por los bancos del centro bancario de Panamá, ha traído consigo el aumento del nivel de riesgo ante ataques cibernéticos por parte de los ciberdelicuentes. Es por ello que surge la necesidad de la creación de un equipo de respuesta a incidentes de seguridad de la información para el sector bancario, el cual puede ser de naturaleza semiautónoma, y así atienda a cualquier banco local ante aquellos incidentes que no puedan ser mitigados por el conjunto de controles preventivos, detectivos y correctivos que tenga cada entidad bancaria.

Esto nos lleva a cuestionarnos: ¿Estamos preparados como país para dar respuesta a incidentes de ciberseguridad simultáneos en la banca privada de Panamá? Tomando en cuenta el número de bancos en el centro bancario de Panamá es superior a cincuenta y que a nivel nacional solo se encuentra con un CSIRT tipo público, se hace necesaria la creación de un equipo de respuesta a incidentes de ciberseguridad para el sector bancario panameño el cual se encuentre dedicado a los bancos que se adscriban al mismo y reciban un servicio especializado.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

ABORDAJE TEÓRICO

De acuerdo a Fernando Puga, en su artículo "CSIRT: El equipo de respuesta, componente esencial en todo programa estratégico de seguridad de datos, el surgimiento del primer CERT fue en el año 1988, debido a la aparición del gusano de Morris, el cual afectó aproximadamente a 6,000 de los 60,000 servidores que se encontraban conectados a Internet de aquella época conocida como ARPANET".

El incesante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales, como a la aparición de nuevos actos ilícitos. "Tras este incidente surgió el primer Equipo de Respuesta ante Emergencias Informáticas (CERT, Community Emergency Response Team), concepto que luego mutó a CSIRT (Computer Security Incident Response Team/Equipo de Respuesta a Incidentes de Seguridad Informática). Un CSIRT es un equipo, interno o externo a la organización, cuyo objetivo principal es minimizar y controlar los daños ante un ciberataque. Este también cumple las funciones de asesorar, responder y recuperar la normalidad en las operaciones, así como prevenir que ocurran futuros incidentes, para lograrlo, actúa como coordinador de todas las áreas, individuos y procesos involucrados en un incidente".

Los conceptos de ciberdelincuencia, ciberterrorismo y ciberguerra son de uso generalizado por parte de amplios sectores de nuestra sociedad. Sería interesante pues, previamente a entrar en materia y pretender dar una definición clara. "En Estados Unidos, en su mayoría los CSIRT cooperan con el CERT-Coordination Center de Carnegie Mellon University, que funciona como el Centro de Coordinación a nivel nacional. Sin embargo a nivel global, existe el Foro de Equipos de Seguridad y Respuesta de Incidentes (Forum of Incident Response and Security Teams, FIRST)", que es la asociación global que coordina los diferentes equipos de respuesta. Los CSIRT miembros de FIRST pueden responder de manera más efectiva a los incidentes de seguridad, al disponer de acceso a las mejores prácticas y colaboración con los otros equipos miembros.

TIPOS

De acuerdo a la Guía de Seguridad (CCN-STIC-810), guía de creación de un CERT/CSIRT en España: Un Equipo de Respuesta ante Emergencias Informáticas

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

(CERT, del inglés Computer Emergency Response Team), un centro de respuesta a incidentes de seguridad en tecnologías de la información. “Se trata de un grupo de expertos responsables de prevenir, gestionar y responder a los incidentes de seguridad de la información que puedan surgir. Esta definición genérica viene materializándose en un equipo multidisciplinar de expertos que trabaja según unos procesos definidos previamente y que disponen de unos medios determinados para implantar y gestionar, de un modo centralizado, todas y cada una de las medidas necesarias para mitigar el riesgo de ataques contra los sistemas de la comunidad a la que presta el servicio y responder de forma rápida y efectiva en caso de producirse. También se puede utilizar el término CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad) para referirse al mismo concepto. De hecho el término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, que está registrado en EEUU por CERT Coordination Center (CERT/CC)”.

Según la agencia de la Unión Europea para la Ciberseguridad (ENISA) en su publicación de cómo crear un CSIRT paso a paso del año 2006, “La primera vez que apareció un gusano importante en la infraestructura global de los sistemas informáticos fue a finales de los años ochenta. El gusano, llamado Morris, se propagó rápidamente y logró infectar numerosos sistemas de TI de todo el mundo. Este incidente actuó como una alarma; de repente todo el mundo se dio cuenta de que existía una gran necesidad de cooperación y coordinación entre administradores de sistemas y gestores de los sistemas informáticos para enfrentarse a este tipo de casos. Por ser el tiempo un factor decisivo, se tenía que establecer un enfoque más organizado y estructural de la gestión de los incidentes relacionados con la seguridad de los sistemas informáticos, así, unos días después del «incidente Morris», la DARPA (Defence Advanced Research Projects Agency, Agencia de Investigación de Proyectos Avanzados de Defensa) creó el primer CSIRT: el CERT Coordination Center (CERT/CC3), ubicado en la Universidad Carnegie Mellon, en Pittsburgh (Pensilvania). Poco después, el modelo se adoptó en Europa, y en 1992 el proveedor académico holandés SURFnet puso en marcha el primer CSIRT de Europa, llamado SURFnet- CERT4. Prosiguieron otros equipos, y en la actualidad el «Inventario de actividades de CERT en Europa» de la ENISA incluye más de 100 equipos muy conocidos localizados en Europa”. De acuerdo a la Guía de Seguridad (CCN-STIC-810) Guía de Creación de un CERT / CSIRT, septiembre 2011.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

Debido al crecimiento de las comunicaciones y la dependencia que existe entre las empresas y la tecnología, hace crítica la inversión en sistemas de seguridad informática. Cabe señalar que debido a que la marca CERT está registrada, se utilizan otras nomenclaturas:

• "IRT (Incident Response Team, Equipo de Respuesta a Incidentes). • CIRT (Computer Incident Response Team, Equipo de Respuesta a Incidentes Informáticos). • CIRC (Computer Incident Response Capability, Capacidad de Respuesta a Incidentes Informáticos). • SERT (Security Emergency Response Team, Equipo de Respuesta a Emergencias de Seguridad). • ERI (Equipo de Respuesta a Incidentes)".

De acuerdo a la Agencia para la Seguridad de la Red e Información de la Unión Europea (ENISA), actualmente están constituidos cuarenta y ocho equipos CERT o CSIRT.

A continuación, se presentan algunos CSIRT del sector financiero existentes a nivel mundial:

- S-CERT: de acuerdo a su sitio web es el equipo de respuesta a emergencias informáticas del Grupo Financiero de Cajas de Ahorros, aseguradoras, y de otras empresas crediticias de Alemania (CERT Das Computer-Notfalteam). También ofrece sus servicios a nivel internacional como intermediario con las empresas crediticias.

  Los servicios ofrecidos por el mismo consisten en avisos preventivos tales como avisos de seguridad sobre agujeros en los productos de software de uso habitual, avisos de seguridad sobre malware.

  Entre los servicios reactivos se encuentran en el estudio y coordinación de incidentes de seguridad, análisis forense, elaboración de informes técnicos sobre ataques de delincuentes informáticos, entre otros.

- TB-CERT (Thailand Banking Computer Emergency Response Team): de acuerdo a su sitio web es el centro de respuesta a emergencia del sector bancario de Tailandia. Este CERT fue conformado en el año 2017 por el Banco de Tailandia y quince instituciones financieras bajo la Asociación Bancaria de Tailandia, para el intercambio de información sobre amenazas entre los bancos, por lo que sus servicios son de tipo informativo o colaborativo.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

- Nordic Financial CERT: de acuerdo a su sitio web es un equipo CERT para las instituciones financieras de los países nórdicos (Dinamarca, Suecia, Finlandia, Noruega e Islandia) con licencia de Nordic FSA (Agencia Supervisora Financiera Nórdica, por sus siglas en inglés).

  Entre los servicios que ofrece podemos mencionar ciberinteligencia, soporte y manejo de incidentes, coordinación para la respuesta a incidentes, compartir información con los miembros de la comunidad.

- CERTFin: de acuerdo a su sitio web es el CERT financiero de Italia, es una iniciativa de cooperación pública privada con el objeto de gestionar el riesgo cibernético del sector bancario y financiero.

  Entre los servicios que ofrece se encuentran el intercambio de información, campañas de sensibilización, análisis y coordinación para responder a incidentes de seguridad.

- FINCSIRT: de acuerdo a su sitio web es el equipo de respuesta a incidentes de seguridad informática del sector financiero. Surge como una iniciativa del Banco Central de Sri Lanka, el Centro de Respuesta a Emergencias Informáticas de Sri Lanka (Sri Lanka CERT) y la Asociación Bancaria de Sri Lanka, alojado en el LankaClear que es el mayor proveedor de infraestructura de pago de dicho país.

  Entre sus servicios principales están el manejo de incidentes, compartir información de ciberinteligencia, concienciación en seguridad a los cuales se encuentran suscritos treinta y ocho miembros.

  Brindan los servicios de un SOC (Centro de Operaciones de Seguridad) a través del cual ofrece herramientas para el monitoreo online, revisiones de seguridad externa, análisis de log, entre otros.

ALGUNOS ASPECTOS REGULATORIOS

Los bancos establecidos en la República de Panamá se encuentran regulados por la Superintendencia de Bancos de Panamá que ha emitido algunas regulaciones a

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

través de circulares y acuerdos que instauran lineamientos para la notificación de incidentes a este ente regulador, así como la colaboración entre los bancos.

De acuerdo al sitio web de la Superintendencia de Bancos de Panamá, en su sección Leyes y Regulaciones, en los numerales 6 y 11 del artículo 11, del Acuerdo 3-2012 del 22 de mayo de 2021, "por el cual se establecen los lineamientos para la gestión del riesgo de la tecnología de la información", establecen lo siguiente:

"Artículo 11 UNIDAD DE SEGURIDAD DE LA INFORMACIÓN.

> 6. Establecer comunicación con los miembros de seguridad de la información de otros bancos con la finalidad de trabajar en conjunto para fortalecer la seguridad del sistema bancario.
>
> 11. Notificar, en caso de sufrir ataques, a la Superintendencia mediante el formulario establecido."

Lo establecido en la norma bancaria panameña antes mencionada, nos sirve de base para el desarrollo de un CSIRT para el sector bancario panameño, ya que a través del mismo los bancos pueden recibir de forma centralizada información de las nuevas amenazas, avisos o notificaciones y así trabajar colaborativamente. De igual manera, el CSIRT puede efectuar la función de notificar al ente regulador en caso de que se presente un ataque, como parte de las funciones del mismo, las cuales deberán regirse por la regulación existente para la tercerización o outsourcing que se encuentra regulada a través del Acuerdo 9-2005 del 19 de octubre de 2005. Cabe mencionar, la tercerización de la función de notificación de ataques por parte del CSIRT, requiere la aprobación del ente regulador bancario panameño como parte de los servicios a tercerizar los cuales deben ser definidos en el objeto del contrato.

Luego de investigar sobre la existencia de grupos CERT o SCIRT en el mundo observamos que en latinoamericana hay escasez o ausencia de los mismos, a nivel del país, es decir un equipo de respuesta a incidentes de ciberseguridad que atienda los ataques o brinde servicios preventivos a nivel nacional y así se fortalezca el nivel de ciberseguridad de los bancos latinoamericanos.

Probablemente, algunos bancos reciban los servicios de un CSIRT privado en el país lo que les permite a las entidades que lo mantienen recibir los múltiples servicios que ofrecen este tipo de equipos. Sin embargo, se requiere mitigar el

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

riesgo reputacional como país y no solo por entidad bancaria, esto se puede lograr con la implementación de un CERT o CSIRT para el sector bancario a través de los servicios preventivos y reactivos, los cuales en conjunto permiten tener información sobre las modalidades de ataques o incidentes que pudiesen darse en alguna entidad local y comunicar a manera de aviso el hecho sin indicar el nombre de la entidad afectada al resto de las entidades, de esa forma el área de seguridad de la información – ciberseguridad puede tomar medidas necesarias a tiempo para evitar pérdidas económicas.

MODELO PROPUESTO

El modelo que proponemos para la implementación del CSIRT para el sector bancario privado panameño, es el CSIRT de Coordinación. Este modelo es el adecuado para brindar el servicio al sector bancario privado del país.

Un CSIRT de coordinación puede brindar sus servicios a una comunidad o miembros distribuidos, por lo general, entidades independientes, que deben pertenecer al mismo sector como el sector financiero, salud, militar, entre otros. Entre los servicios que ofrece este modelo de CSIRT están las alertas y advertencias, análisis de incidentes, soporte de respuesta a incidentes, concienciación a través de la educación y entrenamiento, anuncios debido a que tiene acceso a información de varias organizaciones dentro de su comunidad y el objetivo, otros expertos de seguridad y grupos pueden ilustrar o presentar la actividad de un incidente de la comunidad objetivo.

El CSIRT de coordinación no tendría autoridad sobre los miembros o comunidad objetivo, en este caso los bancos privados del centro bancario de Panamá, por lo que tendría que coordinar con el oficial de seguridad de la información de cada entidad dado que la regulación bancaria define la siguiente función para esta unidad en los artículo del 7 al 10 del Acuerdo 6-2011 del 6 de diciembre de 2011, por medio del cual se establecen lineamientos sobre banca electrónica, gestión de riesgos relacionados, monitoreo y atender los incidentes de seguridad de la información.

- “Artículo 7: UNIDADES RESPONSABLES. La unidad de riesgo o instancia responsable existente en cada banco, deberá tener entre sus funciones la identificación, evaluación y control de los riesgos tecnológicos, incluyendo los riesgos asociados al servicio de banca electrónica. Para la gestión diaria de la seguridad de la información, todo banco deberá tener dentro de su estructura organizacional una unidad de seguridad de la información, que reporte a un

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

funcionario de jerarquía e independencia. Por razones de su estructura organizativa, un banco podrá solicitar al Superintendente dispensas para el cumplimiento de lo establecido en el párrafo anterior, siempre que éste evidencie a satisfacción de la Superintendencia que la gestión de la seguridad de la información es llevada a cabo eficientemente ya sea por su casa matriz o un tercero proveedor de seguridad.

- Artículo 8: AUDITORÍA INTERNA. En materia de auditoría interna, serán responsabilidades del banco: 1. Velar porque se realicen auditorías periódicas de acuerdo al volumen y complejidad de las operaciones que realicen, asegurándose de incorporar dichas auditorías en su plan anual de auditoría, y 2. Contar con los programas necesarios y personal especializado en el área respectiva.

- Artículo 9: REVISIONES EXTERNAS. El banco deberá asegurarse de realizar revisiones externas de riesgo, con personal o empresas debidamente calificadas, para los canales de banca electrónica y de los medios de pago electrónicos.

- Artículo 10: PRUEBAS DE INTRUSIÓN Y VULNERABILIDAD. Con la finalidad de minimizar el acceso no autorizado a sus sistemas todo banco deberá ejecutar al menos las siguientes pruebas de intrusión y vulnerabilidad realizadas por profesionales idóneos externos al banco."

Aunado a esto, como lo establece la norma antes mencionada la unidad de seguridad de la información debe informar a la Superintendencia de Bancos de Panamá, en caso de sufrir ataques, por lo que es importante establecer en conjunto con el regulador bancario el orden de reporte en caso de ataque a fin de evitar incumplimiento con la norma establecida.

La Asociación Bancaria de Panamá cuenta con la comisión de riesgo tecnológico y ciberseguridad, a través de la cual se puede proponer la conformación o creación de un Equipo de Respuesta a Incidentes Cibernéticos para el sector bancario panameño. Es de suma importancia que dicho CSIRT sea neutral para evitar conflictos de intereses y que sus servicios sean brindados con la misma calidad y confianza a todos sus miembros o comunidad objetivo, por ende, al momento de su creación, debe legislarse con miras a esto.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

La posibilidad de un CSIRT semi-autónomo, el cual consistiría en una combinación entre la Asociación Bancaria de Panamá y la Superintendencia de Bancos de Panamá, dependería de una norma o legislación a nivel país, lo que conllevaría a la participación inclusive de la Autoridad Nacional para la Innovación Gubernamental, quien tiene bajo su mando al CSIRT Panamá, que seguiría siendo el CSIRT principal de la nación y que puede establecer contacto con otros equipos CSIRT a nivel mundial, en caso que el CSIRT del sector bancario privado requiera ayuda externa a través de CSIRT de otras jurisdicciones. Ambas figuras requerirán contribución económica para los gastos operativos que tenga el equipo CSIRT lo cual incluye instalaciones, servicio de energía eléctrica, agua, Internet, planilla del equipo o unidades que lo conformen, infraestructura tecnológica, mobiliario, utilería, entre otros.

El CSIRT requerirá de una oficina, con su respectivo mobiliario, y servicios de energía eléctrica, agua, Internet empresarial. Los miembros del CSIRT son los encargados de estos gastos que forman parte de la operatividad de cualquier organización. Su ubicación no debe ser dentro del espacio de cualquiera de los bancos que lo conformen, un lugar neutral son las oficinas de la Asociación Bancaria de Panamá, pero esto requerirá de la aprobación de sus miembros.

Los servicios que se proponen a ofrecer son proactivos, reactivos y de consultoría:

Servicios Proactivos

Los medios definidos para emitir comunicados son el sitio web del CSIRT y correo electrónico, para este último se enviará a la persona de contacto que selecione cada banco. Los servicios a ofrecer en esta categoría son:

- Comunicados: se pretende divulgar alertas sobre nuevas amenazas y vulnerabilidades las cuales deben ir acompañados del comportamiento, solución a implementar a fin de evitar afectaciones.

- Pruebas de penetración y vulnerabilidad: Pruebas de penetración y vulnerabilidad a la red interna y externa.

Por motivos regulatorios los bancos que contraten este tipo servicios no podrán contratar el servicio de valor agregado SOC o de consultoría para así cumplir con lo establecido en el artículo 19, Acuerdo 6-2011 del 6 de

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

diciembre de 2011, de la Superintendencia de Bancos de Panamá, que establece lo siguiente:

"Artículo 19: Relación con Terceros y Proveedores de Seguridad del Servicio de Banca Electrónica.

Cuando el Banco contrate los servicios de proveedores o terceros para que ejecuten procesos de los servicios de banca electrónica, se requerirá obtener la autorización previa de esta Superintendencia de Bancos, de conformidad con lo establecido en el Acuerdo sobre Tercerización emitido por esta Superintendencia. En caso tal de que se trate de un proveedor de seguridad, el mismo debe contar con personal idóneo para el manejo de los servicios contratados.

- Capacitación: brindar a los miembros o bancos adheridos al CSIRT información o formación de seguridad a través de talleres, seminarios, tutoriales, entre otros; enfocados principalmente en la gestión de incidentes de seguridad, los cuales les permita a los responsables de la seguridad de la información – ciberseguridad de las entidades bancarias fortalecer sus medidas preventivas, correctivas y detectivas.

- Pruebas de seguridad a aplicaciones: brindar el servicio de pruebas a productos o aplicaciones a adquirir a través de un sandbox (entorno controlado), con el objetivo de identificar posibles vulnerabilidades o agujeros de seguridad.

Servicios Reactivos

El CSIRT bancario podrá dar las recomendaciones necesarias para el tratamiento de los incidentes que las entidades bancarias le reporten, pero no podrá implementar la solución. Los servicios reactivos que se ofrecerán son los siguientes:

- Alertas: divulgación de información sobre ataques, vulnerabilidades, virus, malware, entre otros, con el plan de acción a ejecutar para contener o evitar un alto impacto en caso de materializarse.

- Manejo de Incidentes: atender los incidentes o ataques cibernéticos reportados, realizando el triage correspondiente con el objetivo de brindar las recomendaciones para la contención del incidente.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

- Análisis de Incidentes: consiste en determinar el origen, alcance y daños ocasionados por el incidente o ataque. Requiere técnicas de informática forense.

- Rastreo: consiste en dar seguimiento o rastrear los orígenes de los atacantes. Para esta actividad, se requiere de la colaboración de los proveedores de Internet locales e inclusive del CSIRT Panamá quien servirá de enlace con CSIRT internacionales para solicitar el apoyo y gestión necesaria en caso que el ataque provenga de otras jurisdicciones.

- Coordinación de respuesta a incidente: actuar como coordinador entre las partes involucradas tales como víctima, proveedores de Internet, administradores de la infraestructura de la víctima, CSIRT Panamá para enlace con los CSIRT internacionales.

Consultoría

Los servicios de consultoría a prestar están basados en el fortalecimiento de la gestión de la seguridad de la información – ciberseguridad tales como análisis de riesgos, definición del proceso para la gestión de incidentes de seguridad con el objeto de determinar los activos críticos y desarrollo de los planes de respuestas a incidentes tomando en cuenta la clasificación de incidentes establecidos en el análisis de riesgo.

El proceso para la divulgación de las amenazas serán de la siguiente forma**:** Los anuncios de las nuevas amenazas y recomendaciones para solución se divulgarán a través de correo electrónico a los bancos que se suscriban al CSIRT.
Los tipos de anuncios o alertas que se divulgarán son:

- Vulnerabilidades
- Amenazas
- Recomendaciones

El Departamento de Monitoreo y Ciberinteligencia, deberá completar la plantilla con la siguiente información mediante un resumen, detalles técnicos, medidas de mitigación, referencias. Una vez completada la plantilla correspondiente deberá enviarla al Departamento de Relaciones Públicas.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

El Departamento de Relaciones Públicas es el encargo de publicar los anuncios o alertas en los medios aprobados para tal fin, previa revisión del Gerente del Equipo de Respuesta a Incidentes, quien debe velar por el cumplimiento de las políticas de clasificación de la información.

El personal del Equipo de Respuesta a Incidentes de Ciberseguridad del Sector Bancario Panameño, requiere capacitación previa al inicio de las operaciones, los temas que se han identificado o se sugieren a incluir son:

- Análisis de Malware
- Auditoría Forense de Sistemas
- Ciberseguridad
- Ethical Hacking

Existen diversas empresas que ofrecen este tipo de capacitaciones localmente y a nivel mundial.

CONCLUSIONES

La implementación del Equipo de Respuesta a Incidentes de Ciberseguridad del Sector Bancario Panameño, requerirá la aprobación de los bancos del sector bancario panameño, los cuales deberán trabajar de forma colaborativa en la etapa de aprobación para que su constitución sea una realidad.

Al finalizar este trabajo de investigación consideramos que hemos presentado una propuesta de estrategias del modelo organizacional de monitoreo de incidentes de sistemas informáticos para el sector bancario panameño, como una alternativa de solución al problema de mitigar los ataques de ciberseguridad en Panamá. Para apoyar lo anterior presentamos las siguientes conclusiones más valiosas de la investigación. La seguridad de la información a nivel nacional es un punto crítico y se convierte en soporte básico para la seguridad de la infraestructura de telecomunicaciones y el sector financiero de nuestro país. Por esta razón se propone establecer un modelo de CSIRT de Coordinación para el sector bancario privado panameño.

Este Modelo de Monitoreo de Incidentes de Sistemas Informáticos propuesto, se encargará de coordinar los procesos de fortalecimiento de la información, para prevenir, combatir, mitigar, solucionar y protegerse los activos frente a los peligros, vulnerabilidades e incidentes de seguridad de la información de usuarios en Panamá

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

en el área de infraestructura de los sistemas informáticos. Igualmente este modelo servirá como centro de entrenamiento y difusión de la información en múltiples aspectos sobre la seguridad informática en Panamá. Adicionalmente, este modelo es replicable a instituciones públicas y privadas en nuestro país. El aumento de las actividades de los usuarios en el internet abre el camino para que el manejo de la información sea de interés a las organizaciones. Las instituciones que no tomen en cuenta estos procesos estarán destinadas al fracaso.

REFERENCIAS BIBLIOGRAFICAS

Acuerdo 3-2012, Superintendencia de Bancos de Panamá. (2012). Recuperado de en: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/acuerdos/2012/Acuerdo_3-2012.pdf.

Acuerdo 6-2011, Superintendencia de Bancos de Panamá. (2011). Recuperado de: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/acuerdos/2011/Acuerdo_6-2011.pdf.

Acuerdo 9-2005, Superintendencia de Bancos de Panamá. (2005). Recuperado de: https://www.superbancos.gob.pa/superbancos/documentos/leyes_y_regulaciones/acuerdos/2005/Acuerdo_9-2005.pdf.

Buenas prácticas para establecer un CSIRT nacional. (2016). Recuperado de: https://www.sites.oas.org/cyber/Documents/2016%20-%20Buenas%20Practicas%20CSIRT.pdf.

CERT Das Computer-Notfalteam. Funciones y Servicios. (2019). Recuperado de: http://www.s-cert.de/esp/mision.html/.

CERT Financiero Italiano (2019). Recuperado de: https://www.certfin.it/.

Como Crear un CSIRT Pasó a Paso, Agencia Europea de Seguridad de las Redes y de la Información (ENISA). (2006).

ENISA. CSIRTs by Country – Interactive Map. (2019). Recuperado de: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map.

Equipo de Respuesta ante Emergencias Informáticas. (2021). http://es.wikipedia.org/wiki/Equipo_de_Respuesta_ante_Emergencias_Inform%C3%A1ticas.

ETDA. Thailand Banking Sector Cert (2019). Recuperado de: https://www.etda.or.th/topics/thailand-banking-sector-cert.html.

REVISTA FAECO SAPIENS
ISSN L 2644-3821
Acceso Abierto. Disponible en:
https://revistas.up.ac.pa/index.php/faeco_sapiens
Indexada
Volumen 4 - Número 2
Julio-diciembre 2021
pp. 97-112
Recibido: 18/04/21 Aceptado: 01/5/21

Gaceta Oficial de Panamá. Decreto Ejecutivo No 709 de lunes 26 de septiembre de 2011. (2011). Recuperado de: https://www.gacetaoficial.gob.pa/pdfTemp/26880/GacetaNo_26880_20110927.pdf.

Guía de Seguridad-CCN-STIC-810. (2011). Guía de Creación de un CERT/CSIRT. Centro Cristológico Nacional.

Guía de Seguridad-CCN-STIC-810-Guía de Creación de un CERT / CSIRT. (2011).

FINCSIRT. (2017). Recuperado de: https://www.fincsirt.lk/about.html.

Killcrece, G, Kossakowski K, Ruefle, R., Zajicek M. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). Recuperado de: en:https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf.

Nordic Financial (2019). Recuperado de: https://www.nfcert.org/.

Puga, F. (2019). EBanking News. CSIRT: El equipo de respuesta, componente esencial en todo programa estratégico de seguridad de datos. Recuperado de: http://www.ebankingnews.com/columnas/csirt-el-equipo-de-respuesta-componente-esencial-en-todo-programa-estrategico-de-seguridad-de-datos-0043936.

Superintendencia de Bancos de Panamá. Bancos Licencia Internacional. Superintendencia de Bancos de Panamá. (2021). Recuperado de: https://www.superbancos.gob.pa/es/info-gen-bancos/licencia-internacional.

Superintendencia de Bancos de Panamá. Bancos Oficiales. Disponible en: Superintendencia de Bancos de Panamá. (2021). Recuperado de: https://www.superbancos.gob.pa/es/info-gen-bancos/bancos-oficiales.

Superintendencia de Bancos de Panamá. Bancos Licencia General. Disponible en: Superintendencia de Bancos de Panamá. (2021). Recuperado de: https://www.superbancos.gob.pa/es/info-gen-bancos/licencia-general.