Desarrollo de un Modelo de Seguridad para un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT)

Edwin Teodocio Suxo Arroba
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
edwinsuxo@gmail.com

***Resumen*—Este trabajo propone la elaboración de un modelo de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), de tal forma que facilite la creación de otros CSIRTs que ayuden a otras comunidades objetivo. Se describirá las normas y estándares internacionales de seguridad más relevantes para el modelo. Se analizará la necesidad de implementación de un equipo interno de respuesta a incidentes de seguridad informática en base a políticas de seguridad en la gestión de incidentes en las áreas críticas de una Empresa de Transporte Marítimo.**

Palabras clave—CSIRT, Gestión, Incidentes, Información, Seguridad.

I. INTRODUCCIÓN

En la actualidad las tecnologías de la información abarcan muchas innovaciones y servicios tecnológicos, estos ayudan en nuestra vida cotidiana, como medio de trabajo y producción. Sin embargo, el tema de seguridad informática o ciberseguridad está en boca de todos.

Existen varios perfiles profesionales dentro de las compañías y Gobiernos que se dedican a la Seguridad de la Información, con el fin de identificar intentos de acceso o posibles intrusiones a recursos informáticos no autorizados para que puedan ser bloqueados en su intento o corregidos ante una detección de violación de accesos; sin embargo con la gestión de incidentes y un equipo de apoyo, se puede mejorar no solamente la detección sino la prevención de intrusiones a servicios, sistemas y equipamiento informático.

Los ataques informáticos tanto externos como internos pueden afectar a los sistemas y la información de una organización. Es así como un evento originado en la década de los 80, cuando un virus denominado Moris infecto a miles de computadores en poco tiempo, produciendo pérdidas cercanas a los 96 millones de dólares. Este ataque llevo a la creación del Equipo de Repuesta a Emergencia Computacionales (CERT) localizado en la Universidad de Carnegie Mello en Pittsburg Pensilvania con la finalidad de brindar soporte ante eventos similares [1].

El crecimiento y la sofisticación de las amenazas informáticas plantean un nuevo panorama en el cual algunos creen que solo es cuestión de tiempo hasta padecer las consecuencias de algún incidente de seguridad, que podría estar relacionado con la información. Pero, además de la comunidad de expertos e investigadores, existen equipos dedicados a responder con rapidez ante nuevos riesgos.

Dado este escenario de evolución del malware y otras amenazas, cobran relevancia los equipos de respuesta a incidentes de seguridad (CSIRT por las siglas de *Computer Security Incident Response Team*).

Su importancia tiene que ver con distintos factores, entre los que se pueden destacar:

- El incremento del tipo y número de amenazas informáticas.
- La aparición de leyes y regulaciones orientadas a la protección de la información.
- La contribución en los procesos de gestión de riesgos y seguridad de la información.

Por lo anterior, cuando se presenta un incidente, el CSIRT debe cumplir diferentes propósitos. El primero de ellos consiste en controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias [2].

Existen varios tipos de CSIRT como académico, comercial, nacional o interno.

Los CSIRT Nacionales, los cuales ya fueron implementados en muchos países de Sudamérica como Brasil, Argentina, Venezuela, Colombia, Uruguay, Chile y Bolivia [4] tienen como principal enfoque ser el punto de contacto principal que brinda soporte a todo un país sobre aspectos de prevención, identificación, tratamiento y resolución de ataques e incidentes de seguridad sobre sistemas informáticos.

Los CSIRT Internos, brindan soporte a organizaciones privadas y los cuales generalmente no dan a conocer sobre las amenazas informáticas de las que fueron objeto de ataque, ni de los procesos que efectúan para prevenirlas o tratarlas.

Para referenciar este artículo (IEEE):

[N] E. Suxo, «Desarrollo de un Modelo de Seguridad para un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT)», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 30-33, 2020.

También se debe comprender lo que es la Gestión de Incidentes de Seguridad de la Información, para el objetivo de esta, hay que recurrir a las siguientes definiciones base:

A. *Evento de seguridad de la información*

Un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

B. *Incidente de seguridad de la información*

Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización [3].

C. *Contexto institucional*

La Empresa de Transporte Marítimo es una empresa internacional que trabaja en el sector del transporte marítimo de contenedores y la logística. Esta transporta bienes y ofrece servicios a comunidades locales, clientes y socios internacionales. Con acceso a una red integrada de medios de transporte por carretera, tren y mar, la empresa se enorgullece de ofrecer un servicio mundial con expertise local. La mayor parte de estos servicios se realizan haciendo uso de diferentes medios, uno de ellos la Internet, a través del cual el área comercial, área logística, trasportistas y clientes realizan varios tipos de operaciones y tramites de importación y exportación de productos en contenedores, todos estos son de gran importancia para el continuo funcionamiento y crecimiento de la empresa, el constante avance de las tecnologías, a su vez permite la facilidad de comunicación, también abre puertas que permiten que la información que se genera sea puesta en peligro, debido al mal manejo de recursos tanto por personal interno como externo y también por actividades externas como ataques de intrusión realizadas por Hackers.

Después de describir lo anterior, las organizaciones privadas están obligadas a contar con personal especializado en seguridad y manejo de incidentes informáticos, involucrados en los procesos de monitoreo, análisis de nuevas amenazas y vulnerabilidades en equipos y sistemas informáticos, diseño de metodologías para la resolución de incidentes de seguridad informáticos, planteando un modelo de un equipo de respuesta ante incidentes de seguridad informáticos dentro la infraestructura de TI de la organización privada.

II. MÉTODOS

A. *Política de seguridad*

Cuando se habla de seguridad de la información, es importante conocer el termino CIA (Confidencialidad, Integridad, Disponibilidad), que presenta los principios básicos de la seguridad de la información. Realizar una correcta gestión de la seguridad de la información establece como principio básico que sin los tres elementos mencionados no existe nada seguro, con que solo falle uno de los componentes nos encontramos ante un peligro para nuestra seguridad de la información. Tenemos que recordar que ningún sistema de seguridad es completamente seguro, siempre debemos tener claro que un sistema es mucho más vulnerable de lo que pensamos. Es necesario que tengamos en cuenta las causas de los riesgos y la posibilidad de que ocurran fallos [5].

Un CSIRT busca contribuir a preservar estas características en las organizaciones.

B. *Controles de seguridad*

También llamadas Salvaguardas por la metodología MAGERIT (Esquema Nacional de Seguridad, 2012) los controles de seguridad son mecanismos de protección frente amenazas, reduciendo la frecuencia de las amenazas y limitan el daño causadas por éstas. Pueden ser buenas prácticas, software o hardware [6].

C. *CSIRT Equipos de respuesta ante incidentes de seguridad informática*

Su razón de ser radica en que, aunque resulte casi imposible evadir todos los riesgos, en caso de que alguno se materialice, sus consecuencias puedan ser mitigadas y las actividades primordiales restablecidas en el menor tiempo posible, con el impacto mínimo aceptable para las organizaciones.

Las principales características y los beneficios de contar con personal que integre este estratégico grupo de profesionales.

El primero de ellos consiste en controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias.

También debe coordinar las actividades para una recuperación rápida y eficiente de las actividades que se han visto afectadas, en conjunto con los equipos de TI, de manera que la organización pueda operar con normalidad en el menor tiempo posible y con el menor impacto tolerable.

Además, debe prevenir que eventos similares puedan ocurrir en el futuro, de tal forma que puedan erradicarse las causas raíz del incidente, junto con mantener una base de conocimientos que permita registrar las lecciones aprendidas de estos sucesos, con el objetivo de que no se repitan y si esto sucede, se pueda contar con un antecedente de la solución o soluciones posibles.

Una función adicional incluye actividades para compartir información relacionada con incidentes de seguridad con otros CSIRT, con fines de difusión, e intentando mitigar el impacto de nuevas amenazas, vulnerabilidades o ataques.

D. *Servicios ofrecidos por los CSIRT*

Los servicios reactivos se realizan debido a un evento de seguridad indeseado e inesperado detectado o como solicitud de algún miembro de la organización que haya identificado alguna anomalía en la infraestructura tecnológica. Este tipo de actividades son el componente principal de los CSIRT y están directamente relacionados con los planes de gestión de seguridad.

Existen distintos incidentes de seguridad que requieren la reacción de los equipos de respuesta a incidentes, por ejemplo, cuando un equipo o servidor ha sido comprometido debido a la explotación de vulnerabilidades, la infección de equipos por algún código malicioso, o la detección de intrusiones en los

sistemas o la red corporativa, solo por mencionar algunos ejemplos.

Por otro lado, los servicios proactivos están diseñados para brindar información que contribuya a la protección de la infraestructura tecnológica, así como mejorar los procesos de seguridad, por lo que su objetivo principal es evitar ataques o incidentes. Entre otras actividades, pueden incluir auditorías y evaluaciones, la instalación, correcta configuración y mantenimiento de herramientas de seguridad.

Finalmente, una tercera categoría de servicios de los CSIRT está relacionada con la gestión de la seguridad, que, aunque no se trata de su foco principal, puede participar y contribuir en el desarrollo de actividades como evaluaciones de riesgos, desarrollo de planes de continuidad del negocio, recuperación ante desastres, así como en lo relacionado a la concientización y educación de los usuarios [7].

E. Estándares y Códigos de Buenas Prácticas

La documentación existente que se mencionara las cuales orientan a los grupos de investigación y entes gubernamentales que desean crear un Centro de Respuesta ante Incidentes Informáticos ya sea público o privado.

1) RFC 2196 - Site Security Handbook

Este documento es un código de buenas prácticas para administradores de sistemas y de red en la forma de abordar los problemas de seguridad dentro de la comunidad de Internet. Esta guía es sólo un marco para el establecimiento de políticas y procedimientos de seguridad. A fin de tener un conjunto efectivo de políticas y procedimientos, un sitio tendrá que tomar muchas decisiones, el acuerdo de ganancia, y luego comunicar y poner en práctica estas políticas [8].

2) RFC 2350 - Expectations for Computer Security Incident Response

El objetivo de este documento es proporcionar una perspectiva para la divulgación de temas de importancia en relación con la respuesta a incidentes que en la actualidad son de importancia para toda la comunidad. Además, establece políticas de publicación y de procedimientos, respuesta y coordinación a incidentes [9].

3) ISO / IEC 27035-1: 2016

Es la base de esta norma internacional multiparte. Presenta conceptos básicos y fases de la gestión de incidentes de seguridad de la información y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a incidentes, y aplicar las lecciones aprendidas [5].

4) ITIL v3.0 :2011

Mejores Prácticas para la gestión de servicios. Biblioteca de infraestructura de tecnologías de información, es una guía de buenas prácticas en la gestión de incidentes de servicios de IT [10].

5) Modelo de gestión de resiliencia CERT (CERT-RMM) Versión 1.2

Es la base para un enfoque de mejora de procesos para la gestión de resiliencia operativa. Define las prácticas organizativas esenciales que son necesarias para gestionar la resiliencia operativa. Puede usar CERT-RMM para determinar la capacidad de su organización para gestionar la resistencia, establecer objetivos y metas y desarrollar planes para cerrar las brechas identificadas. Al usar una vista de proceso, CERT-RMM puede ayudar a su organización a responder al estrés con un rendimiento maduro y predecible [11].

F. Metodología de Investigación

Diseño de la investigación.

La investigación será de tipo propositiva por cuanto se fundamenta en una necesidad o vacío dentro de la institución.

Nivel de la investigación.

Exploratorio, focaliza el tópico de interés, formula problemas y delimita futuras investigaciones

Evaluativa, en el cual impartirá recomendaciones con base a la evaluación de los resultados.

Universo o población de estudio.

Empresa de Transporte Marítimo el cual cuenta con 40 usuarios (empleados) el cual será la población de estudio.

Determinación y elección de la muestra.

La muestra se limitará a la infraestructura critica de la empresa la cual cuenta con 5 personas, el Responsable de Sistemas, Encargados de infraestructura, Encargados de desarrollo, Helpdesk.

Procesamiento y análisis de datos.

Se usará la Estadística Descriptiva que es un conjunto de técnicas usadas para describir, representar, inferir y resumir la información del fenómeno de estudio, apoyado con programas computacionales. Iniciando con la estructuración, transcripción y análisis de datos.

El tipo de estudio será con intervención, nivel investigativo exploratorio, longitudinal y analítico, además al ser controlado se va a utilizar el método cuasi experimental.

Se determinará el estado actual en cuanto a temas de seguridad de la información en la Empresa de Transporte Marítimo, realizando una encuesta al personal de IT como al personal de las diferentes áreas.

III. Discusión

Por el estudio realizado en la Empresa de Transporte Marítimo y por los resultados iniciales de la investigación se confirma la necesidad de implementar un CSIRT.

En el presente trabajo, se realizó un recorrido de forma general por el mundo de los Centros de Respuesta ante Incidentes Informáticos, permitiéndonos conocer generalidades conceptuales de estos, modelos de operación, servicios y casos de éxito, todo esto como antesala a la presentación de una propuesta metodológica para la implementación de un CSIRT, producto preliminar de un proceso de normalización investigativo que se somete a juicio a través de la escritura de este artículo, con el que se espera aportar un ápice de luz en la oscuridad de las metodologías para la creación de CSIRT's.

IV. Conclusiones

Es un camino largo y bastante complejo debido a la escases de información acerca de este tema, quizás para muchos investigadores y teóricos desarrollar una metodología basado en modelos empíricos que científicamente posiblemente no tendrían sustento sin un proceso de validación seria poco

ortodoxo, pero después de realizar parte de este trabajo que aún no termina hemos comprobado que es posible y bastante productivo visto desde los resultados de la investigación el uso de este estilo de trabajo para esta temática en particular. Para futuras investigaciones entraremos a describir el proceso de validación de esta metodología a través de un proceso de implementación real de un CSIRT Privado.

Se recomienda que las empresas consideren implementar y/o fortalecer la gestión de incidentes de seguridad para proteger sus activos y mitigar riesgos.

REFERENCIAS

[1] West-Brown, M. (1998). Hand Book for Computer Security Incident Response Team. Pensilvania: Universidad Carnegie Mellon.

[2] Mendoza, Miguel Ángel. (18 mayo 2015). www.welivesecurity.com.

[3] Cárdenas, Fabian. (1 Sept 2018). *ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI*. Colombia: http://www.novasec.co/en/blog/62-gestion-integral-de-la-seguridad-de-la-informacion

[4] Hernández, José Carlos. (27 feb 2018). Estrategias Nacionales de Ciberseguridad en América Latina. http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina

[5] ISO/IEC 27035-1:2016, Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management

[6] ISO 27001: El método MAGERIT. (16 de marzo de 2015).

[7] Organización de los Estados Americanos (OEA). (abril de 2016). Buenas prácticas para establecer un CSIRT nacional. Washington, USA.

[8] Rfc2196, http://www.ietf.org/rfc/rfc2196.txt - 25 octubre 2010

[9] Rfc2350, http://www.ietf.org/rfc/rfc2350.txt - 18 Octubre 2010

[10] ITILv3:2011. https://es.wikipedia.org/wiki/Information_Technology_Infrastructure_Library

[11] CERT Resilience Management Model (CERT-RMM) Version 1.2. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084