risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido / Recibido: 7/3/2015
Aceitação /Aceptación: 28/3/2015

Estado actual de equipos de respuesta a incidentes de seguridad informática

Mirna Muñoz [1], Lizbeth Rivas [1]

Mirna.munoz@cimat.mx, Lizbeth.rivas@cimat.mx

[1] Centro de Investigación en Matemáticas, CIMAT A.C. Unidad Zacatecas, Av. Universidad No. 222, Fracc. La Loma, C.P. 98068, Zacatecas, Zacatecas, México

DOI: 10.17013/risti.e3.1-15

Resumen: Las organizaciones deben administrar una gran cantidad de información que debe ser accedida en diferentes lugares y personas, lo que genera un riesgo. Desafortunadamente, este riesgo se potencializa debido a que las organizaciones no siempre se cuenta con un departamento o personal del área de seguridad informática, dando como resultado información vulnerable. Esta situación es confirmada con datos publicados en el reporte de Symantec en 2013 donde se reportan 253 ataques a organizaciones que tienen como resultado 552.018.539 identidades expuestas. Para dar una solución a esta problemática se crearon los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) que apoyan con servicios y conocimientos para responder eficientemente a los ataques de seguridad (ya evitando y respondiendo a estos ataques). En este artículo se presenta una revisión sistemática para la obtención del estado actual de los CSIRTs existentes e identificar principales elementos a tener en cuenta para su establecimiento.

Palabras-clave: Seguridad, CSIRT, equipo de respuesta, modelos de seguridad.

Present state of Response Teams computer security incidents

Abstract: The organizations have to organize a big amount of information that should be acceded from different places and by different people, this is a big risk. Unfortunately this information it's vulnerable because the organizations doesn't have a proper computer security department or staff in that area. This situation it's confirmed with data published on Symantec's report on 2013, where it's reported 253 attacks to organizations that have as result 552.018.539 exposed identities. To avoid and to respond those attacks, the CSIRT (Computer Security Incident Response Team) was created, and helps with services and knowledge to respond efficiently those security attacks. In this article we present a systematic review performed to obtain a global vision of the actual state of the CSIRT's in existence and identify the main elements to keep in mind for its establishment.

Keywords: Security, CSIRT, response team, security models.

1. Introducción

La importancia que se debe brindar a los datos informáticos en una organización es comúnmente descuidada, de acuerdo a Maiwald (Caralli et al. 2010), "cuando las computadoras se unen en redes, surgen nuevos problemas de seguridad y los viejos problemas se comportan de diferentes formas". Desafortunadamente, no se brinda la seguridad necesaria, ignorando los riesgos de tener información vulnerable que pueden presentarse en diferentes entornos y criticidad (MAIWALD 2004), por ejemplo: los ataques a escuelas, donde pueden ser modificados los datos de los alumnos; los ataques a empresas, donde su información puede ser duplicada y usada con fines ventajosos o vendida a externos; y los ataques en el sector público de gobierno, donde la información puede ser eliminada o duplicada exponiendo directamente la seguridad de los ciudadanos.

En este contexto, la mayoría de las organizaciones no cuentan con la capacidad para prevenir y hacer frente de manera efectiva a los ataques informáticos.

Como una respuesta a estos ataques se crean los equipos de respuesta a incidentes de computación. El primer equipo fue creado en 1988 por la Universidad Carnegie Mellon para apoyar a DARPA (Defense Advanced Research Proyects Agency) por el ataque con gusano "Morris" que afectó a ARPANET (Advanced Research Projects Agency Network) (ENISA 2006) (Roldán 2011).

Estos equipos brindan la ayuda necesaria para mantener en una organización la privacidad de los datos, la integridad de los mismos e incluso la disponibilidad, que son propiedades fundamentales para reforzar un valor de negocio y aprovechar las sinergias y economías de escala en fuentes e infraestructuras de información.

El objetivo de este artículo se enfoca en la investigación del estado del arte actual de los CSIRT ya establecidos y caracterizar el panorama global de estos equipos. El artículo está estructurado como sigue: en la sección 2, se presenta una descripción del protocolo de revisión sistemática establecido para esta investigación y los resultados que se obtuvieron aplicados para este artículo; en la sección 3, se muestran los resultados obtenidos en la investigación y finalmente, en la sección 4, se presentan conclusiones y trabajos futuros.

2. Revisión sistemática

La revisión sistemática (RS) consiste en un método científico específico que permite a los investigadores obtener resultados relevantes y cuantificados de un tema específico (Kitchenham and Charters 2007). Una revisión sistemática de la literatura (a menudo referida como una revisión sistemática) es un medio de identificación, evaluación e interpretación de todos los estudios disponibles relevantes a una pregunta de investigación particular o área temática o fenómeno de interés (Mian et al. 2007) .

2.1. Fases de la revisión sistemática

En la revisión sistemática está compuesta por tres fases descritas a continuación:

- *Planificación*: se clarifica y delimita el tema con los objetivos que tendrá la investigación, se plantean las preguntas que el estudio debe responder, se listan

las palabras clave que serán los principales términos que se encuentran en las preguntas.
- *Ejecución*: se seleccionan las fuentes de los estudios primarios y los criterios que evaluarán los resultados obtenidos de las fuentes seleccionadas, esto delimitará los estudios primarios y secundarios.
- *Análisis de los resultados*: Establecidos los estudios primarios y secundarios se comienza con la extracción de la información y se establecen y publican los resultados.

La Figura 1 muestra las actividades contenidas en cada fase de la revisión así como su ejecución.

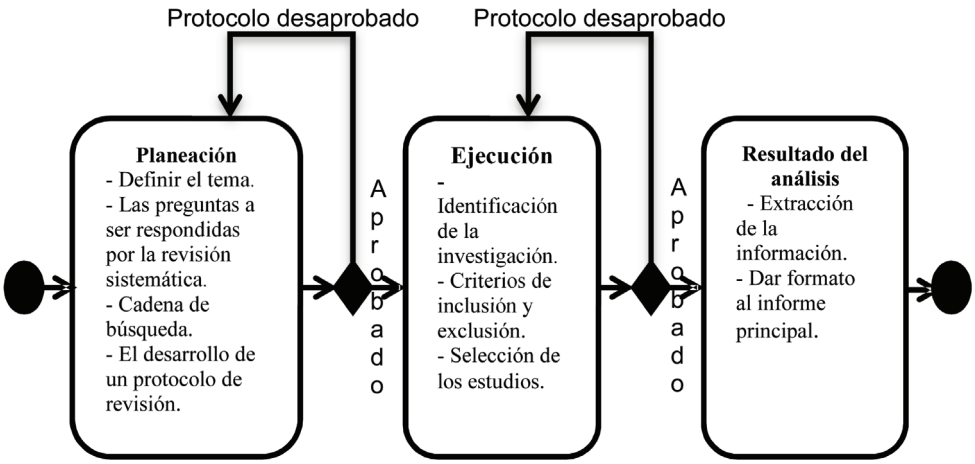

Figura 1 – Fases de la revisión sistemática

2.2. Definición del protocolo de revisión sistemática para los CSIRTs

En esta sección se muestra la definición del protocolo de revisión sistemática adaptada al tema de investigación.

a) Fase de Planificación: A continuación se muestra el desarrollo de las actividades realizadas.

- *Definición del tema*: El investigador debe establecer el estado actual de los equipos de respuesta a incidentes de seguridad CSIRTs
- *Preguntas de investigación*: las preguntas definidas apoyan en la obtención de información básica sobre las características de los CSIRTs, así como de los modelos y frameworks existentes para su creación, por lo tanto, se plantearon tres preguntas: (1) ¿En qué dominios se puede enfocar un CSIRT? (2) ¿Qué características o propiedades contienen los CSIRT enfocados al dominio al que está dirigido? y (3) ¿Qué modelos, frameworks, metodología, estándares existen para la creación de un CSIRT?

- *Cadenas de búsqueda*: previo a la definición de las cadenas de búsqueda se seleccionaron palabras clave que se utilizarían en las cadenas de búsqueda, las palabras elegidas son: CERT/CSIRT; Características / Propiedades; Estándar / Metodologías/ Frameworks / Modelos.

Con las palabras identificadas se crearon dos cadenas, que permitieron obtener la información necesaria para responder las preguntas planteadas:

1. (Características) OR (Propiedades) AND (CERT OR CSIRT)
2. (Estándar) OR (Metodologías) OR (Frameworks) OR (Modelos) AND (CERT OR CSIRT)

- Definir el protocolo de revisión: como se muestra en la Figura 2 el protocolo consta de 8 pasos.

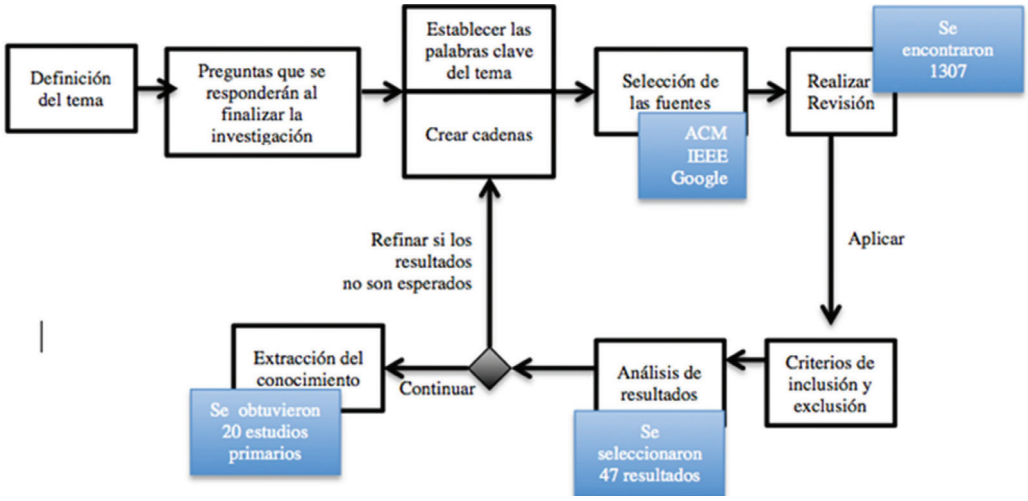

Figura 2 – Pasos del protocolo de revisión

b) Fase de Ejecución: A continuación se muestra el desarrollo de las actividades para esta investigación.

- Selección de las fuentes: las fuentes seleccionadas son IEEE, ACM y Google Scholar.
- Criterios de inclusión y exclusión: los criterios de inclusión y exclusión que se desarrollaron para este trabajo y que permitieron la selección de los artículos primarios y secundarios de la investigación se describen en la Tabla 1.
- *Selección de los estudios primarios*: se definieron 3 filtros como a continuación se describen: (1) La lectura del título, se seleccionaron aquellos artículos que el título tuviera palabras fuertemente relacionadas al tema; (2) La lectura del resumen y conclusiones, si el título era demasiado abstracto se procedió a leer

Tabla 1 – Criterios de inclusión y exclusión

Inclusión	Exclusión
– Fecha de publicación (no menor a 5 años), a menos que sea un artículo importante que se referencié en más 5 artículos o libros consultado.	– No estén dentro del rango de fechas.
– Contengan en el título palabras clave referente al tema. – Si el título es ambiguo se pasará al resumen y las conclusiones.	– Se omitirán los temas de seguridad como ataques, herramientas para evitar los ataques, despliegue de información.
– Se tomarán en cuenta artículos de revistas indexadas o congresos.	– Si el título no es suficiente, se leerá el resumen y las conclusiones si estas no demuestra contener valor se desechará la referencia.
– Se analizarán páginas de CERT certificados por el SEI.	– Artículos que no tengan información relevante.
– Las búsquedas de los artículos se realizarán en inglés y español con las cadenas mencionadas anteriormente.	– Artículos que no se encuentren en el idioma inglés o español.
– Se analizará los artículos con información estratégica sobre los CSIRT.	

el resumen, si aún quedaban dudas se prosiguió a leer las conclusiones y (3) texto completo, finalmente si al terminó de la lectura del resumen y conclusión no se estaba seguro de desechar el artículo se prosiguió a la lectura completa del mismo.

c) **Fase de Análisis de los resultados:** como se observa en la Figura 1, la tercera fase de la revisión sistemática consta de: extracción de la información, análisis de la información y presentación de los resultados (Kitchenham 2004). El desarrollo de las actividades de esta fase para esta investigación se muestra en la sección de resultados. Como se observa en la Figura 2, se obtuvieron 47 resultados en base a las cadenas y una vez aplicados los filtros se descartaron 27 artículos quedando 20 primarios que se encuentran en el anexo, de los cuales como se observa en la Figura 3: 8% fueron obtenidos de Google Scholar, 39% pertenecen a ACM Digital Library y finalmente 53% pertenecen a IEEExplore.

Cabe resaltar que para fortalecer la información se analizaron diferentes páginas de CSIRT que nos brindan documentación valiosa sobre el conocimiento que obtuvieron en su realización como: Symantec (www.symantec.com), INTECO (www.inteco.es), ENISA (www.enisa.europa.eu), First.org (www.first.org) y CERT.org (www.cert.org).

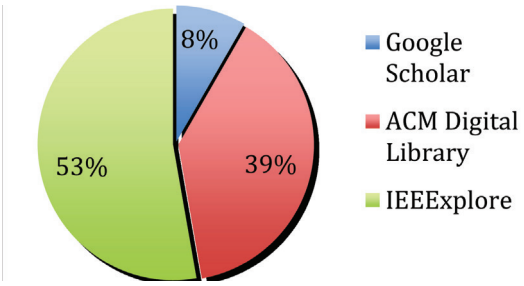

Figura 3 – Gráfica de Artículos encontrados en las diferentes fuentes consultadas

3. Resultados

En esta sección se muestran el análisis de los datos extraídos y los resultados obtenidos.

3.1. Características de los CSIRT's

Se analizaron los principales métodos para la creación de un equipo de seguridad tomando como base los ya establecidos, el análisis se enfocó en: CERT de la Carnegie Mellon; el CSIRT de ENISA de Europa y un CERT establecido en Honduras. En la Tabla 2, se muestra el análisis de los diferentes pasos para el establecimiento de los CSIRT's identificados(Caralli et al. 2010) (Roldán 2011) (ENISA 2006) (Marcos, Millar, Sw, Rager, & Road, 2011).

Tabla 2 – Pasos para la creación de un CSIRT

	CERT	**CSIRT**	**CERT Honduras**
Pasos primarios (se encuentran en más de dos CERT)	-Identificar los procedimientos de cada personal, el equipo y la infraestructura necesaria. -Entender y establecer los servicios que brindará. -Establecer el marco operacional, los servicios, las políticas, cómo se asegurará la calidad y la capacidad para adaptarse en un ambiente de cambio y cambiar los perfiles ante amenazas.	-Determinar el sector al que prestará servicios. -Entender qué es un CSIRT.	-Establecer los objetivos del CERT -Establecer el organigrama del CERT y cómo será compuesto -Se procede a establecer la gestión administrativa y técnica.

Pasos secundarios (Se encuentran en más de un CERT)	-Establecer los propósitos del CERT. -Identificar la Audiencia. -Analizar los incidentes de la región /organización -Analizar la administración y la organización consensuadamente. -Hacer coincidir las metas con la organización, las políticas y las metas de negocio. -Seleccionar un equipo de desarrollo para el CERT.	-Elección de los servicios que brindará. -Definir el enfoque que se adoptará para poner en marca el CSIRT -Análisis del grupo de clientes atendidos y los canales de comunicación adecuados. -Preparar la declaración de servicios, para dejar claro qué tipo de CSIRT representa y cuál es su cometido.	-Establecer las funciones del CERT.
Pasos Terciarios (Se encuentra en al menos un CERT)	-Construir la visión. -Analizar y mejorar el marco del CERT -Realizar una prueba del CERT interna. -Anunciar y promover el CERT -Comunicar los servicios y la construcción del mismo. -Obtener retroalimentación -Establecer la motivación. -Establecer la categoría a la que pertenecerá. -Comunicar el proceso. -Obtener retroalimentación	-Definir el plan comercial que consta del modelo financiero. -Equipamiento y ubicación de la oficina -Buscar cooperación con los socios -Promover el plan comercial -Poner el CSIRT en funcionamiento	-Se declara público la función del CERT. -Establecer el CERT en las instalaciones del consejo de ciencia y tecnología (COHCIT)

Resultado del análisis: los pasos mínimos para establecimiento del CSIRT: (1) Establecer el propósito que tendrá el CSIRT; (2) Determinar el sector al que prestará servicios; (3) Definir el enfoque que se adoptará para poner en marca el CSIRT; (4) Establecer los servicios que brindará; (5) Definir el plan comercial que consta del modelo financiero; (6) Construir la visión; (7) Hacer coincidir las metas con la organización, las políticas y las metas de negocio; (8) Definir el plan comercial que consta del modelo financiero; (9) Seleccionar un equipo de desarrollo para el CSIRT: (10) Identificar los procedimientos de cada personal, el equipo y la infraestructura necesaria; (11) Realizar una prueba del CSIRT interna; (12) Obtener retroalimentación; (13) Poner el CSIRT en funcionamiento; (14) Analizar y mejorar el marco del CSIRT.

3.2. Propiedades de los CSIRT

En esta sección se analizan las propiedades que son atributos esperados que deben contener los CSIRT. Para este análisis se enfocó en las propiedades de los CERT/CSIRT. La Tabla 3 muestra el análisis de las propiedades que debe contienen los diferentes equipos de seguridad analizados(Caralli et al., 2010) (ENISA 2006)(Roldán 2011), (Marcos, Millar, Sw, Rager, & Road, 2011) (Reyes, 2013).

Tabla 3 – Análisis de las propiedades de un CSIRT

Propiedades	CERT	CSIRT	CERT Honduras	CERT Militar
Cuentan con un propósito.	X	X	X	X
Delimitan los servicios.	X	X	X	X
Delimitan la audiencia.	X	X	X	X
Análisis de la región/organización.	X	X		X
Cuentan con una Misión.	X	X	X	X
Cuentan con una Visión.	X	X	X	X
Capacidad para identificar riesgos.	X	X	X	X
Cuentan con políticas.	X		X	X
Establecen como mejorar de la calidad.	X			
Cuentan con oficinas.		X	X	X
Cuentan con un equipo de coordinación	X	X	X	X
Cuentan con un modelo financiero.	X	X		
Cuentan con personal especializado	X	X	X	X
Cooperan con otros CERT	X	X	X	
Mejoran continuamente.	X			

Una vez analizadas las propiedades mencionadas por diferentes CSIRTs, se han identificado un conjunto de propiedades mínimas esperadas, es importante resaltar que como criterio de selección de las propiedades se estableció elegir aquellas que se mencionan por todos los CSIRTs analizados:

- *Visión*: camino al que estará dirigido el CSIRT.
- *Misión*: propósito general del CSIRT.
- *Región*: análisis de las necesidades y delimitación de la región que abarcara el CSIRT.
- *Financiamiento*: financiamiento monetariamente el CSIRT.
- *Administración*: autoridades que dirigirán el CSIRT.
- *Servicios*: servicios que ofrecerá a las organizaciones.
- *Modelo organizacional*: distribución del CSIRT, delimitación de los puestos y los trabajos que deben realizar en base a estos.
- *Recursos*: administración de los recursos de hardware, el personal, etc.

3.3. Nombramiento y sectores de aplicación de los equipos de respuesta ante incidentes informáticos

Se ha detectado que se utilizan diferentes nombramientos y abreviaturas de los equipos de respuesta ante incidentes informáticos de acuerdo a la región en la que se establezca (Roldán 2011):

- CERT o CERT/CC (Computer Emergency Response Team): esta abreviatura se utiliza en Estados Unidos.
- CSIRT (Computer Security Incident Response Team): esta abreviatura se utiliza en Europa.
- IRT (Incident Response Team): esta abreviatura se utiliza en equipos pequeños que se encuentran dentro de una organización.
- CIRT (Computer Incident Response Team): esta abreviatura se utiliza principalmente en Australia, Alemania, Japón, Noruega y Estados Unidos.
- SERT (Security Emergency Response Team): esta abreviatura se utiliza en África principalmente.

Los tipos de CSIRT son definidos en base al propósito del enfoque que tendrán y el tipo de sector que cubrirá. Por lo tanto, los CSIRT tienen dos clasificaciones: en base a los nueve dominios que se han identificado y a su vez pueden ser clasificados en cinco modelos organizacionales.

A continuación se listan los 9 dominios y una descripción del sector al que prestan los servicios:

1. *Sector académico*: prestan servicios a centros académicos y educativos.
2. *Sector comercial*: prestan servicios a clientes que pagan por éstos.
3. *Sector de la protección de la información vital y de la información y las estructuras vitales (CIP/CIIP):* prestan servicios a empresas de TI y a ciudadanos.
4. *Interno*: presentan servicio únicamente a la organización que pertenecen.
5. *Sector Público*: prestan servicio a agencias públicas y ciudadanos.
6. *Sector militar*: prestan servicios a instituciones militares y entidades externas a estas.
7. *Nacional:* prestan servicios a un país, se considera un punto de contacto de seguridad, suelen ser intermediarios.
8. *Sector pequeña y mediana empresa (PYME):* presta servicios a empresas, su personal o un grupo de usuarios similar.
9. *De soporte:* prestan servicios a productos específicos para propietarios de productos.

Los diferentes servicios identificados que pueden ofrecer los CSIRT se clasifican en reactivos, proactivos, manejo de instancias y gestión de calidad de seguridad como a continuación se describen en la Figura 4 algunos servicios otorgados por algunos propósitos (ENISA 2006)(Roldán 2011) (Eduardo Carozo Blusmztein 2012):

3.4. Modelos organizacionales

La clasificación de los CSIRT los ayuda a mantenerse comunicados para poder responder, a los incidentes de seguridad informática que se les presenten, existen 5 clasificaciones en base al modelo organizacional que se muestran en la figura 5, estos mantienen una estructura eficiente para poder dar solución a los incidentes. Dependiendo del modelo que se elija podrán brindar diferentes servicios, en diferente calidad y a diferente nivel, también se tomará en cuenta la experiencia y madurez del equipo que variara dependiendo de las metas que se proponga la organización (Roldán 2011) (Eduardo Carozo Blusmztein 2012)

Figura 4 – Lista de los diferentes Servicios por sectores.

- *Equipo de Seguridad: e*s la organización que se da de hecho cuando no existe un CSIRT constituido. No hay una asignación formal de responsabilidades respecto a los incidentes de seguridad. El personal existente, usualmente de TI, maneja los eventos de seguridad como parte de su actividad habitual.
- *Modelo Distribuido: e*s una estructura central pequeña (al menos un gerente de seguridad) supervisa y coordina al personal del equipo distribuido en la organización. El personal del equipo distribuido es personal previamente existente en la organización. Se le asignan explícitamente responsabilidades relativas a seguridad, a las que se dedica parcial o totalmente. Este modelo se adecúa bien a organizaciones grandes en las que un equipo centralizado puede ser insuficiente.
- *Modelo Centralizado: c*onsta de un equipo centralizado de personal a tiempo completo que toma la responsabilidad sobre la seguridad en toda la organización.
- *Modelo Combinado: e*s una combinación entre el modelo distribuido y la centralizada con una estructura centralizada pequeña, con personal capacitado que toma decisiones que les han sido designadas.
- *Modelo Coordinador:* es un equipo centralizado que coordina y facilita el manejo de incidentes de seguridad. Por lo general atiende a una comunidad objetivo formada por organizaciones externas múltiples y diversas.

Una vez constituido el modelo organizacional del CSIRT, se procede a la elección del organigrama que tendrá internamente, dependiendo de los intereses que tenga la organización puede ser elegido dentro de las opciones siguientes(Roldán 2011) (Eduardo Carozo Blusmztein 2012):

Figura 5 – Clasificación de los CSIRT en base a los modelos organizacionales

- *Organigrama funcional*: Consiste en la unificación de las actividades comunes empezando con los niveles más bajos hasta los altos niveles gerenciales y directivos. Este organigrama permite que el conocimiento y las habilidades humanas se fortalezcan, otorgando una mejor eficiencia, que resulta a su vez, más coordinada y controlada para hacer frente a los retos.
- Organigrama basado en el producto: Esta clase de organigrama se estructura considerando lo producido tanto en bienes como servicios; en amplias compañías esta forma de organización posibilita el manejo de unidades y subunidades que las mismas requieren para su funcionamiento.
- Organigrama basado en los clientes: La organización para establecer los tipos de clientes que se busca adquirir, por medio de una base en donde se establece los problemas y necesidades comunes de éstos y la designación de especialistas para resolverlos, puede emplearse de igual manera a la división y subdivisión del personal. La estructura del personal constituiría una utilidad al especificar las funciones requeridas para la demanda de los distintos clientes.
- Organigrama híbrido: Esta estructura puede formarse utilizando diversos criterios de productos-función y producto-geografía. Al posibilitar múltiples enfoques, esta organización es la empleada por aquellas empresas que poseen el control de varios productos o mercados. Debido a que este organigrama permite combinar funciones y divisiones de productos y oficinas las organizaciones pueden advertir con mayor claridad y rapidez las fortalezas y debilidades de cada una.

- Organigrama Matricial: Este organigrama combina la estructura horizontal y vertical, es utilizada al compartir recursos entre líneas de trabajo, cuando los resultados son cruciales y cuando el entorno de la organización es complejo y con cambios frecuentes. Esta estructura mejora la incertidumbre no obstante funcionan mejor en organizaciones medianas.
- El modelo incrustado: Este tipo de modelo es utilizado al crear un CSIRT dentro de una organización que ya existe previamente. Una vez constituido el CSIRT, se designa un jefe encargado de las actividades y del equipo de trabajo, que agrupará a los técnicos que sean requeridos para la resolución de incidentes o actividades propias del CSIRT. El jefe cuenta con la cooperación de la organización existente.
- El modelo universitario: Con este modelo las instituciones de investigación y las académicas que integran una misma universidad pero que se encuentran ubicadas en distintas regiones del país, se organizan por medio de un CSIRT central que coordina a dichas organizaciones, las cuales, en su mayoría, son independientes y cuentan con un CSIRT propio.

3.5. Modelos, marcos de trabajo y estándares

Para robustecer la creación del CSIRT existen modelos, marcos de trabajo y estándares que apoyan a la creación mantenimiento y la gestión de la organización en diferente puntos clave del manejo de riesgos. Estos se encuentran resumidos en la Figura 6.

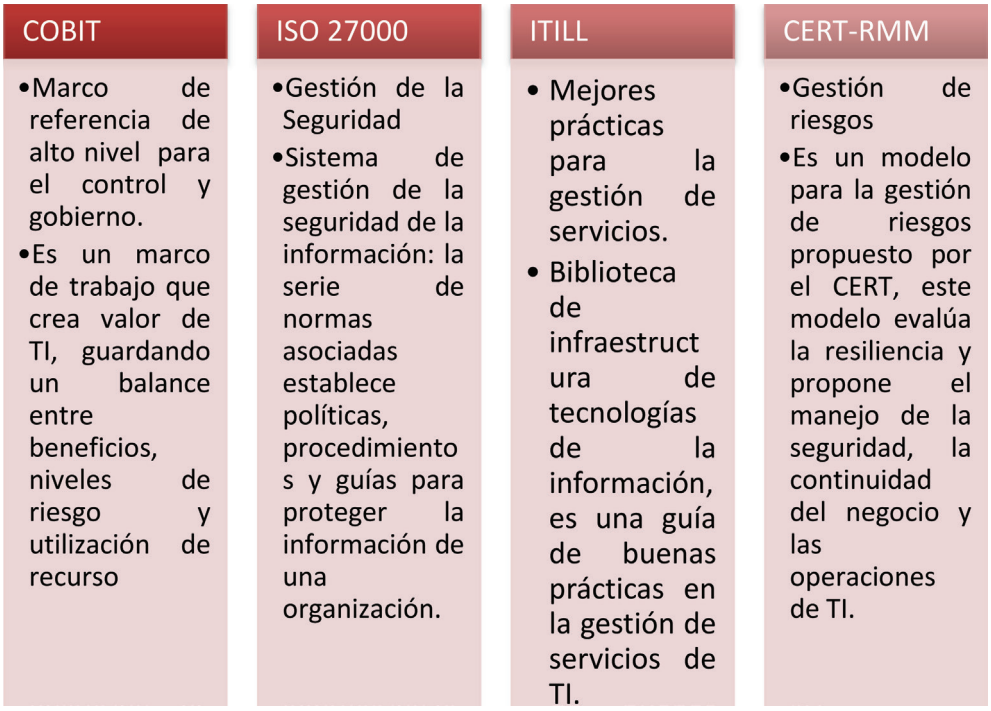

Figura 6 – Modelos, marcos y estándares del manejo de riesgos

El manejo de incidencias es una tarea sensible, para asegurarnos del correcto manejo de la información se puede apoyar con el uso de marcos de trabajo, estándares y modelos que minimicen el factor de riesgo y el grado de criticidad en los incidentes registrados. Se eligieron COBIT, ITIL, CERT-RMM e ISO 27000 por su grado de integración adaptable que puede ser desarrollado en el CSIRT (Caralli et al. 2010).

4. Conclusiones y trabajos futuros

Las organizaciones necesitan una estabilidad y mayor grado de protección enfocada a la seguridad informática para proteger y minimizar las amenazas a su información. Aun cuando existen diferentes maneras de proteger sus datos el principal problema es la desinformación que tienen las organizaciones para la toma de decisiones, por lo tanto, se identifica la necesidad de desarrollar un modelo que permita aplicar buenas prácticas para establecer la seguridad en equipos de seguridad informática proporcione información eficaz y eficiente sobre recomendaciones, estrategias y planes para tener un nivel de seguridad alto en su información.

En este trabajo se han logrado, establecer el estado del arte identificando elementos básicos que deben ser tener en cuenta para el establecimiento de un CSIRT. Además, se ha identificado la necesidad de proveer apoyo a las organizaciones para implementar equipos de seguridad que cubra con sus necesidades, por lo tanto, como trabajo futuro se está desarrollando un propuesta que comprende la creación del método que apoye a las organizaciones en la selección y establecimiento de un equipo de seguridad que cubra sus necesidades y gestione su evolución para brindar servicios especializados. Esta propuesta incluye el desarrollo de una herramienta que agilice la creación o evolución del equipo de seguridad.

Referencias

Caralli, Richard A., Julia H. Allen, Pamela D. Curtis, David W. White, and Lisa R. Young. 2010. *CERT ® Resilience Management Model*. Retrieved (http://www.cert.org/resilience/download/CERT-RMM_v1.0.pdf).

Eduardo Carozo Blusmztein. 2012. *Proyecto AMPARO Manual : Gestión de Incidentes de Seguridad Informática*.

ENISA. 2006. "CSIRT Setting up Guide in Spanish." 90. Retrieved July 15, 2014 (http://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide-in-spanish).

Kitchenham, Barbara. 2004. "Procedures for Performing Systematic Reviews." *Keele, UK, Keele University* 33:28. Retrieved (http://csnotes.upm.edu.my/kelasmaya/pgkm20910.nsf/0/715071a8011d4c2f482577a700386d3a/$FILE/10.1.1.122.3308[1].pdf\nhttp://tests-zingarelli.googlecode.com/svn-history/r336/trunk/2-Disciplinas/MetodPesquisa/kitchenham_2004.pdf).

Kitchenham, Barbara and S. Charters. 2007. "Guidelines for Performing Systematic Literature Reviews in Software Engineering." *Engineering* 2:1051.

MAIWALD, ERIC. 2004. *FUNDAMENTOS DE SEGURIDAD DE REDES - Margen Libros*. edited by MCGRAW-HILL / INTERAMERICANA DE MEXICO. Retrieved February 9, 2015 (http://mx.casadellibro.com/libro-fundamentos-de-seguridad-de-redes/9789701046241/997462).

Mian, Paula, Tayana Conte, Ana Natali, Jorge Biolchini, and Guilherme Travassos. 2007. "A Systematic Review Process for Software Engineering." *Empirical Software Engineering* 32:1–6. Retrieved (http://portal.acm.org/citation.cfm?id=1241572.1241584).

Roldán, Félix Sanz. 2011. "GUÍA DE CREACIÓN DE UN CERT / CSIRT." 60. Retrieved July 15, 2014 (https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf).

Tashi, Igli and Solange Ghernaouti-Hélie. 2009. "A Security Management Assurance Model to Holistically Assess the Information Security Posture." *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009* 756–61.

Anexos

Selección de artículos primarios

Ahmad, R. A., & Hashim, M. S. (2011). Computer Emergency Response Team (OIC-CERT).

Flegel, U., Hoffmann, J., & Meier, M. (2010). Cooperation enablement for centralistic early warning systems. *Proceedings of the 2010 ACM Symposium on Applied Computing*, 2001–2008. doi:10.1145/1774088.1774509

Glass, K., & Colbaugh, R. (2011). Web analytics for security informatics. *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011*, 214–219. doi:10.1109/EISIC.2011.66

Goncalves, J. M., & Fernandes, F. (2009). The impact of information security on Latin America. *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*.

Grobauer, B., & Schreck, T. (2010). Towards Incident Handling in the Cloud: Challenges and Approaches. *ACM Workshop on Cloud Computing Security Workshop (CCSW)*, 77–85. doi:10.1145/1866835.1866850

Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a CSIRT. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*, 2–7. doi:10.1109/ISSA.2010.5588307

Haller, J., Merrell, S., Butkovic, M., & Willke, B. (2010). Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, 40. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA536721

Khurana, H., Basney, J., Bakht, M., Freemon, M., Welch, V., & Butler, R. (2009). Palantir : A Framework for Collaborative Incident Response and Investigation. *Proceedings of the 8th Symposium on Identity and Trust on the Internet*, 38–51. doi:10.1145/1527017.1527023

Lee, C. S., Lee, G. M., & Rhee, W. S. (2013). Standardization and challenges of smart ubiquitous networks in ITU-T. *IEEE Communications Magazine*, *51*(10), 102–110. doi:10.1109/MCOM.2013.6619572

Mazzini, S., Puri, S., & Vardanega, T. (2009). An MDE methodology for the development of high-integrity real-time systems. *2009 Design, Automation & Test in Europe Conference & Exhibition*. doi:10.1109/DATE.2009.5090837

Messnarz, R., Ekert, D., Reiner, M., & Sicilia, M. A. (2012). Europe wide industry certification using standard procedures based on ISO 17024. *Proceedings - 2012 Technologies Applied to Electronics Teaching, TAEE 2012*, 342–347. doi:10.1109/TAEE.2012.6235462

Metzger, S., Hommel, W., & Reiser, H. (2011). Integrated security incident management - Concepts and real-world experiences. *Proceedings - 6th International Conference on IT Security Incident Management and IT Forensics, IMF 2011*, 107–121. doi:10.1109/IMF.2011.15

Mouton, J., & Ellefsen, I. (2013). The Identification of Information Sources to aid with Critical Information Infrastructure Protection.

Penedo, D. (2006). Technical infrastructure of a CSIRT. *International Conference on Internet Surveillance and Protection, ICISP'06*, *00*(c). doi:10.1109/ICISP.2006.32

Pereira, R., & Silva, M. M. Da. (2013). IT Compliance Management Process Modeling Based on Best Practices Reference Models and Qualitative Data. *2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops*, 178–187. doi:10.1109/EDOCW.2013.27

Reyes, G. L. (2013). MODELO BASICO PARA LA INTEGRACION DEL GRUPO CSIRT HONDURAS EN. *Revista H-TICs*, *1*(1). Retrieved from Descargar este archivo PDF - Instituto de Investigaciones ...

Rogers, L. R. (2006). The CERT Survivability and Information Assurance Curriculum: Building Enterprise Networks on a Firm Educational Foundation. *2006 IEEE Information Assurance Workshop*, 61–68. doi:10.1109/IAW.2006.1652078

Tashi, I., & Ghernaouti-Hélie, S. (2009). A security management assurance model to holistically assess the information security posture. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 756–761. doi:10.1109/ARES.2009.28

Trebolle, D., Go, X, & Mez, T. (2010). Reliability Options in Distribution Planning Using Distributed Generation. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, *8*(5), 557–564. doi:10.1109/TLA.2010.5623509

When, R., & What, W. (2013). FIRST Site Visit Requirements and Assessment.