IV Conferencia Científica Internacional
Universidad de las Ciencias Informáticas

Temática: Gestión de incidentes

Metodología para la gestión de ciberincidentes en las universidades cubanas.

Methodology for cyber incidents management in Cuban universities

Yailin Sánchez Borrell [1*], Dennis Barrera Perez [2], Yunia Reyes González [3]

[1] Universidad de las Ciencias Informáticas, Cuba. ysanchezb@uci.cu

[2] Universidad de las Ciencias Informáticas, Cuba. dbperez@uci.cu

[3] Universidad de las Ciencias Informáticas, Cuba. yrglez@uci.cu

[*] Autor para correspondencia: ysanchezb@uci.cu

Resumen

En los últimos tiempos ha aumentado el número de ciberataques, pues cada día los usuarios malintencionados perfeccionan sus técnicas para lograr sus objetivos. Esto ha traído consigo que el número de ciberincidentes haya crecido de forma exponencial, principalmente en el sector de educación, debido a la gran fuente de conocimientos que poseen. En el presente trabajo se muestran los resultados de un estudio realizado sobre las principales metodologías, documentos y estándares relacionados con la gestión de incidentes en Cuba y el mundo, además de conceptos y valoraciones en los que se basa el tema de investigación. Se explica, además, detalles del proceso de detección, análisis, contención, recuperación, erradicación, respuesta, así como la clasificación y criticidad de los mismos. Con ello se pretende crear una metodología que permita homogenizar el proceso de gestión de ciberincidentes en las universidades cubanas, y podrá servir de guía a los especialistas de seguridad de las universidades cubanas.

Palabras clave: ciberincidentes, gestión de incidentes, metodología, ciberataques informáticos.

Abstract

In recent times, the number of cyberattacks has increased, as malicious users improve their techniques every day to achieve their objectives. This has brought with it that the number of cyber incidents has grown exponentially, mainly in the education sector, due to the large source of knowledge they have. This paper shows the results of a study carried out on the main methodologies, documents and standards related to incident management in Cuba and the world, as well as the concepts and assessments on which the research topic is based. It also explains details of the process of detection, analysis, containment, recovery, eradication, response, as well as their classification and criticality. This is to create a methodology that allows the homogenization of the cyber-incident management process in Cuban universities, and may serve as a guide for security specialists at Cuban universities.
Keywords: *cyber incidents, cyberattacks, methodology.*

Introducción

La constante evolución de las tecnologías ha facilitado la distribución de información, así como la presencia de empresas y entidades en internet. Pero ha traído como inconveniente que los mismos estén expuestos a amenazas constantes por parte de los usuarios malintencionados. Las empresas invierten mucho dinero para aumentar su seguridad y evitar así ser víctimas de ciberataques. Las universidades son uno de los objetivos preferidos de los ciberdelincuentes por la gran cantidad de usuarios conectados a internet, entre los ciberataques más comunes se encuentran acceso no autorizado a sitios web, ransomware que exigen rescate, ataques de denegación de servicios, ataques de phishing y robo de información sensible, entre otros. En Cuba se ha incrementado considerablemente el acceso a internet, como parte del proceso de informatización de la sociedad, por lo que la presencia en internet de los usuarios y las empresas ha crecido, esto ha traído como consecuencia que los mismos estén cada vez más expuestos a ciberataques.

Haciendo una revisión de la gestión de incidentes en el país, se pudo identificar como problema que los mismos se realizan en su mayoría empleando métodos manuales, lo cual provoca demora para la resolución de los mismos. Poca preparación de los especialistas para resolver determinados incidentes, debido a que en ocasiones la fluctuación de especialistas es alta. Además, no se tiene de forma precisa el procedimiento a realizar cuando ocurre un incidente de seguridad, esto trae como consecuencia que en ocasiones los incidentes demoren varios días en responderse.

Por las razones anteriores, muchos de los ciberincidentes que ocurren en las universidades tienen efectividad. Para dar cumplimiento a la problemática planteada, se propone como objetivo general, la elaboración de una metodología para

la gestión de ciberincidentes, que contribuya a homogenizar el proceso de gestión de ciberincidentes en las universidades cubanas.

Materiales y métodos o Metodología computacional

Para la investigación, se utilizó el método Analítico–Sintético, donde se descompuso el problema de investigación en elementos por separado, lo cual permitió el estudio de cada uno de ellos, para luego sintetizarlos en la solución de la propuesta.

Incidentes de seguridad

Los incidentes de seguridad son eventos que pueden indicar que los sistemas de seguridad de una entidad han sido comprometidos.

Como caso específico de los incidentes de seguridad, se encuentran los ciberincidentes. (CCN-CERT, 2020), define que un ciberincidente es una acción desarrollada a través del uso de redes de ordenadores u otros medios, que se traducen en un efecto real o potencialmente adverso sobre un sistema de información y/o la información que trata o los servicios que presta. Por su parte (GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES, 2020) define un ciberincidente como todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

Clasificación de los ciberincidentes

Para un mejor entendimiento, análisis, contención y erradicación de los ciberincidentes, es necesario contar con clasificaciones, debido a que todos no poseen las mismas características. Los factores que se pueden considerar a la hora de establecer criterios de clasificación son, entre otros (GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES, 2020):

Contenido dañino: Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas. Virus, Gusanos, Troyanos, Ransomware, Botnet.

Disponibilidad: Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas. Denegación [Distribuida] del Servicio Dos/DDoS.

Obtención de información: Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de identificación de vulnerabilidades. Phishing, Ingeniería social, Identificación de activos y vulnerabilidades (escaneo).

Intrusiones: Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización. Cross-Site Request Forgery (CSRF), Falsificación de petición entre sitios cruzados, Defacement (desfiguración), Cross Site Scripting (XSS), Inyección SQL, Ataque de fuerza bruta e Inyección de Ficheros Remota.

Compromiso de la información: Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública. Acceso no autorizado a información, Modificación no autorizada de información y Exfiltración de información.

Contenido abusivo: Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos. Spam (Correo Basura)

Gestión de incidentes

La gestión de incidentes es el proceso que comprende todas las estrategias y actividades que se deben llevar a cabo para supervisar el ciclo de vida del incidente, desde su apertura hasta su cierre y tiene como objetivo mitigar el posible impacto de los incidentes (Rivas, 2019).

Resultados y discusión

Cada universidad gestiona de forma diferente los ciberincidentes. Con el objetivo de homogenizar el proceso de gestión de ciberincidentes, se propone la elaboración de una Metodología para la gestión de ciberincidentes, que contribuya a homogenizar este proceso en las unversidades cubanas.

La metodología propuesta para la gestión de ciberincidentes cuenta con varias fases, donde se recogen las tareas a realizar cuando ocurre un tipo de ciberincidente y la forma de detectarlo, analizarlo, contenerlo y erradicarlo.

En la siguiente figura se muestran las etapas del proceso de gestión de incidentes:

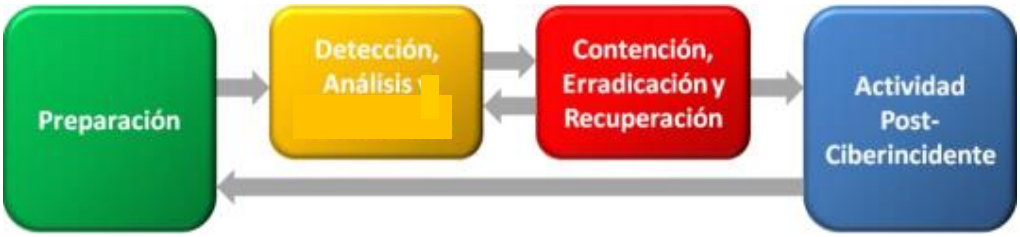

Figura 1: Fases de la gestión de ciberincidentes.

Etapa 1. Preparación: En esta etapa inicial, las universidades deben estar preparadas para enfrentar de la mejor manera posible cualquier evento que pueda ocurrir. Donde se permite proteger los bienes que puedan verse comprometidos, cumplir con las regulaciones de instancias superiores; prevenir el uso de su sistema en el ataque a otro sistema, y minimizar una potencial exposición negativa sobre la organización (Gonzalo, 2013).

Dentro de las acciones que deben llevar a cabo las universidades se encuentran la creación y preparación de un equipo de respuesta a incidentes, donde lo mismos deben ser formados por especialistas capaces y deben estar preparados para enfrentar cualquier evento que se pueda presentar. Cumplir con las regulaciones de instancias superiores: Las mismas incluyen reglamento interno de la universidad, las regulaciones y normas vigentes en el país.

Para el análisis de los incidentes, los especialistas deben contar con recursos que faciliten la gestión de incidentes, entre los que se encuentran los siguientes:

Parches de seguridad, Discos de Sistemas Operativos y aplicaciones, Imágenes de salva. Medios de almacenamiento ligero, Políticas de seguridad, así como un conjunto de herramientas para el tratamiento de incidentes, como son Sistemas de detección de intrusos, Cortafuegos, Software antispam, Escáner de vulnerabilidades, Firewall de aplicaciones web, Herramientas para realizar pruebas de penetración, entre otros.

Etapa 2. Detección: Las universidades deben estar preparadas para detectar cualquier evento que pueda ocurrir. Para ello deben aplicar medidas de detección que pueden ser manuales o automáticas, con el propósito de descubrir indicios que puedan mostrar la presencia de ciberincidentes en sus redes.

Dentro de las formas de detección se encuentran los reportes de los usuarios de las tecnologías de la universidad. Estos reportes pueden ser de estudiantes, profesores, trabajadores, especialistas, OSRI y se pueden recibir por las siguientes vías:

- Correo electrónico
- Personalmente
- Teléfono
- Por un sistema de gestión de incidentes, si la universidad cuenta con uno.

Otra de las vías para detectar indicios de incidentes, es mediante el análisis de las fuentes de información.

Tabla 1. Fuentes de información.

Pruebas sospechosas.	Detección de un troyano en una PC.
Negación de servicios.	Surgimiento de anomalías.

Acceso lento a Internet.	Empeoramiento del rendimiento.
Intentos de escritura en el sistema.	Modificación o borrado de datos.
Aparición de nuevos ficheros.	Cambio de longitud de ficheros y datos.
Caída del sistema.	Bloqueo de cuenta por intentos de acceso fallidos.
Aviso de IDS sobre desbordamiento de buffer	Nuevas cuentas inexplicables.

Para descubrir algunos de los indicios anteriores, generalmente se pueden identificar por la revisión periódica de los reportes de las herramientas automáticas:

Tabla 2. Reportes de herramientas automáticas.

Las alertas que generan los sistemas SIEM.	Las alertas que generan los sistemas de detección de intrusos IDS.
Las alertas que generan los sistemas antivirus.	Los filtros de correo.
Las alertas que generan los sistemas antispam.	Analizar los registros de auditoría (logs).
Sistemas de administración de red (NMS)	SW de control de integridad de archivos.
Información pública.	

Etapa 3. Análisis: El análisis del incidente, se realiza con el objetivo de investigar lo ocurrido, determinar que originó el incidente, así como los usuarios y dispositivos afectados.

Al comenzar con el análisis del incidente, se debe clasificar con las clasificaciones definidas a continuación.

Tabla 3. Relación de clasificaciones de los ciberincidentes.

Origen de la amenaza	En este trabajo se decidió analizar los ciberincidentes.
Tipo de amenaza	Identificar el tipo de amenaza al que pertenece el ciberincidente detectado, dentro de las que se encuentran, código dañino, disponibilidad, intrusiones, obtención de información, compromiso de la información, fraude y contenido abusivo.
Criticidad	La criticidad refleja el peligro que el ciberincidente representa para las unversidades. Para establecer el valor de la criticidad en esta investigación se definieron 4 niveles, en los cuales se recogen los tipos de ciberincidentes que puedan ocurrir en las universidades (Tabla 4).
Prioridad	Para establecer la prioridad de los ciberincidentes se definen diferentes niveles, y luego se le asigna la prioridad a cada uno de ellos. Cada equipo de respuesta a incidente define los niveles de prioridad de acuerdo a sus características (Tabla 5).

Tabla 4: Relación de los ciberincidentes por los niveles de criticidad. (GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES, 2020).

Valor	Criticidad de los ciberincidentes
Muy Alto	Distribución de malware, configuración de malware, robo, sabotaje, interrupciones.
Alto	Sistema infectado, servidor C&C, compromiso de aplicaciones, compromiso de cuentas con privilegios, ataque desconocido, DoS, DDoS, acceso no autorizado a información, modificación no autorizada de información, pérdida de datos, phishing.
Medio	ingeniería social, explotación de vulnerabilidades conocidas, intento de acceso con vulneración de credenciales, desconfiguración, uso no autorizado de recursos, suplantación, amplificador DDoS, servicios con acceso potencial no deseado, revelación de información, sistema vulnerable.
Bajo	Spam, escaneo de redes (scanning), otros.

Tabla 5: Niveles de prioridad por ciberincidentes.

Nivel	Características
Muy Alta	Una emergencia es un incidente cuya resolución no admite demora, como es el caso de todos los que supongan peligro para vidas humanas, para la seguridad nacional o para la infraestructura de Internet.
Alta prioridad	Un incidente de alta prioridad es aquél cuyas características requieren que sea atendido antes que otros, aunque sea detectado posteriormente, como aquellos en que exista infiltración de una cuenta privilegiada o negación de servicio o que requieran acción inmediata debido a su rapidez y ámbito de difusión.
Prioridad media	Por defecto, los incidentes se atienden por orden de llegada, mientras no requiera atención uno de prioridad superior, por ejemplo, todos los incidentes no clasificados como alta prioridad o emergencia, donde el atacante haya ganado acceso a un sistema informático ajeno. También se incluye la exploración insistente de redes.
Baja prioridad	Los incidentes de baja prioridad se atienden por orden de llegada, mientras no requiera atención uno de prioridad superior. Por ejemplo, incidentes aislados en grado de tentativa, donde el atacante no ha conseguido su propósito y no es probable que lo consiga.

Tiempo de respuesta estimado de cada incidente: Para la atención de los ciberincidentes, se estabecieron tiempos máximos, con el objetivo de atender los mismos de acuerdo a su criticidad y prioridad. La siguiente tabla muestra un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso. La siguiente tabla es

un resumen del tiempo de atención según el nivel de impacto y prioridad de atención de un ciberincidente de seguridad.

Tabla 6: Tiempo de respuesta por cada tipo de ciberincidente.

Nivel de criticidad	Prioridad	Tiempo de atención
Muy Alto	Muy alta	Menor o igual a 24 horas
Alto	Alta	24 a 48 horas
Medio	Media	3 a 10 días
Bajo	Baja	

Al concluir con las clasificaciones, se debe informar sobre la ocurrencia del incidente al director encargado de la seguridad informática y los servicios telemáticos para obtener autorización para comenzar la investigación.

1. Se crea un grupo de trabajo que será el encargado de la investigación.
2. Se definen las responsabilidades de cada miembro del equipo.
3. Se designa el miembro principal de la investigación.

Para la investigación, se debe tener en cuenta lo siguiente:

- Obtener datos y realizar correlación de eventos: Los datos se deben recopilar de diferentes fuentes, hacer copia bit a bit y conservar los mismos.
- Identificar el vector de ataque: Los incidentes pueden ocurrir de disimiles maneras, las universidades deben estar preparadas para enfrentar y manejar todos los que puedan presentarse. Se debe identificar el vector de ataque que utilizaron los ciberdelincuentes para materializar la amenaza que desencadenó el ciberincidente. Este vector ayuda a identificar el tipo de incidente, el alcance y los sistemas afectados.
- Identificar el origen del ataque, los dispositivos y sistemas afectados: Para identificar los usuarios y dispositivos afectados, se debe investigar en las fuentes de información.

Una vez que se haya analizado el incidente, se debe notificar por correo electrónico a las entidades y autoridades apropiadas. La información que se brinde debe ser completa y comprobada, explícita, entendible, oportuna, veraz y objetiva:

- Al director encargado de la seguridad informática, redes y servicios telemáticos.
- Al rector de la universidad.
- A los administradores de redes.
- A los administradores de los sistemas en el caso que proceda.

- A la OSRI para informarle de la ocurrencia del incidente en la universidad. En dicho reporte se debe especificar el organismo al que pertenece, el tipo de incidente, la prioridad, el sistema operativo, fecha y hora, así como las medidas adoptadas para mitigar el mismo y los dispositivos comprometidos.

Etapa 4. Contención: En esta etapa se toman las medidas necesarias para limitar la extensión del incidente, con el fin de detener el impacto que pudiera tener el mismo en la organización para que no siga produciendo daño. Además, se recopilan las evidencias para su posterior análisis forense.

Etapa 5. Erradicación: Una vez que el incidente ha sido contenido es necesario eliminar los problemas que ha causado. Las medidas de erradicación dependen del tipo de incidente presentado, y tienen como objetivo eliminar las causas del incidente y todo rastro de los daños. Algunas de las medidas más comunes de erradicación son las siguientes:

1. Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
2. Identificar y eliminar todo el software utilizado por los atacantes.
3. Recuperación de la última copia de seguridad limpia.
4. Identificar servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.

Etapa 6. Recuperación: Al eliminarse las causas del incidente, se debe regresar el sistema afectado a su funcionamiento normal. Esta fase permite evaluar el daño ocurrido y determinar la información que se ha perdido.

- Se devuelven los sistemas a su normal funcionamiento.
- Fortalecimiento de los mecanismos de seguridad del perímetro y otros.
- Recuperar la información de salvas previamente definidas, donde se debe confirmar que las mimas son confiables y están libres de cualquier problema de seguridad.
- Mitigar las vulnerabilidades explotadas.
- Se debe validar el funcionamiento correcto del sistema y luego realizar una nueva salva.

Etapa 7. Post-ciberincidente: La misma se realiza una vez que el ciberincidente este controlado y la actividad ha vuelto a la normalidad. Donde se debe analizar las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de

lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda volver a repetir, además de mejorar los procedimientos.

Por último, se realizará un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.

Conclusiones

Como resultado de la investigación se concluye lo siguiente:

- La metodología propuesta permite una adecuada gestión de los incidentes de seguridad. Donde se definen las actividades a realizar en las fases que componen el ciclo de vida de la metodología, el mismo es flexible y puede ser adaptado al ambiente de cualquier universidad del país.
- Las herramientas y actividades se utilizaron en la gestión de incidentes y se adaptaron al entorno universitario.
- El uso de la metodología propuesta permitió ordenar considerablemente el proceso de gestión de incidentes en las universidades cubanas comparado con lo que se hacía anteriormente.

Referencias

1. IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses. (s. f.-a). Recuperado 22 de marzo de 2020, de https://www.prnewswire.com/news-releases/ibm-study-hidden-costs-of-data-breaches-increase-expenses-for-businesses-300679124.html
2. Pierrat, G. G. (2013). Administración de incidentes de Seguridad Informática, Oficina de Seguridad para las Redes Informáticas (OSRI).
3. Hernández Sampieri, R; Fernández-Collado, C. y Baptista Lucio, P. (2006). Metodología de la Investigación. Cuarta Edición. México DF: Mc Graw Hill. ISBN 970-10-5753-8.
4. What's the Cost of a Data Breach in 2019? | Digital Guardian. (s. f.). Recuperado 19 de marzo de 2020, de https://digitalguardian.com/blog/whats-cost-data-breach-2019
5. Alsmadi, I. (2019). The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics
6. Patrick Kral. (2012). SANS Institute Information Security Reading RoomThe, Incident Handlers Handbook. Recuperado de https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
7. «NATO CIICS Federation: A project of the Multinational Cyber Defence Capability Development Programme». [En línea]. Disponible en: https://www.ncia.nato.int/NewsRoom/Pages/151023-NATO-CIICS-Federation.aspx. Seguridad de TI y Gestión de Seguridad Corporativa», OTRS. [En línea]. Disponible en: https://otrs.com/es/soluciones/seguridad-corporativa/.

8. ISO/IEC 27035 Security incident management. (2016). Recuperado de https://www.iso27001security.com/html/27035.html
9. CCN-CERT, (2016). Guía de Seguridad de las TIC, CCN-STIC 817, ESQUEMA NACIONAL DE SEGURIDAD GESTIÓN DE CIBERINCIDENTES. [archivo PDF]. Recuperado de https://www.ccn-cert.cni.es/en/pdf/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/2025-ccn-stic-817-national-security-framework-cyber-incident management/file.html
10. Guía Nacional de Notificación y Gestión de Ciberincidentes. (2020). [archivo PDF]. Recuperado de http://www.interior.gob.es/documents/10180/9771228/Gu%C3%ADa+Nacional+de+Notificaci%C3%B3n+y+Gesti%C3%B3n+de+Ciberincidentes.pdf
11. Prasad, R., & Rohokale, V. (2020). Cyber Security: The Lifeline of Information and Communication Technology. Springer.
12. Articles-5482_G21_Gestion_Incidentes.pdf. (2016). Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
13. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1-147.
14. ISACA. (2019). State of Cyber 2019, Part 2: Current Trends in Attacks. https://www.isaca.org/bookstore/state-of-cybersecurity-2019/whpsc192
15. Informatización de la sociedad. (2017). Informatización de la sociedad en Cuba |Presidencia de Cuba. https://www.presidencia.gob.cu/es/estado-cubano/programas-priorizados/informatizacion-de-la-sociedad-en-cuba/
16. Ministerio de Comunicaciones. (2019). Resolución 128 de 2019 de Ministerio de Comunicaciones. La Habana: Gaceta Oficial de la República de Cuba.
17. Ministerio del Interior. (2019). Decreto No. 360/2019 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional
18. Ministerio de Comunicaciones. (2017). Política integral para el perfeccionamiento de la informatización de la sociedad en Cuba. La Habana
19. Rivas G. Gestión de incidentes: ¿Por qué es un proceso vital para tu empresa? (2019). Recuperado de https://www.gb-advisors.com/es/gestion-de-incidentes/