Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 21/08/2022 | Aceptado: 01/09/2022

Metodología para la gestión de ciberincidentes en las universidades cubanas

Methodology for cyber incidents management in Cuban universities

Yailin Sánchez Borrell [1*] https://orcid.org/0000-0001-9859-1547
Dennis Barrera Pérez [2] https://orcid.org/0000-0002-7434-7459
Yunia Reyes González [3] https://orcid.org/ 0000-0001-7143-7080

[1] Universidad de las Ciencias Informáticas. Carretera a San Antonio, km 2 ½, Reparto Torrens, La Habana. Cuba. ysanchezb@uci.cu.
[2] Universidad de las Ciencias Informáticas. Carretera a San Antonio, km 2 ½, Reparto Torrens, La Habana. Cuba. dbperez@uci.cu.
[3] Universidad de las Ciencias Informáticas. Carretera a San Antonio, km 2 ½, Reparto Torrens, La Habana. Cuba. yrglez@uci.cu.

*Autor para la correspondencia. (ysanchezb@uci.cu)

RESUMEN

En los últimos tiempos ha aumentado el número de ataques informáticos, pues cada día los atacantes 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

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

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 peligrosidad de los mismos. Con ello se pretende crear una metodología que contribuya al proceso de gestión de ciberincidentes en las universidades cubanas, y podrá servir de guía a los especialistas de seguridad informática.

Palabras clave: ciberincidentes; gestión de incidentes; metodología; ataques informáticos.

ABSTRACT

In recent times, the number of computer attacks has increased, as every day attackers refine their techniques 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 dangerousness. This is intended to create a methodology that contributes to the cyber incident management process in Cuban universities, and may serve as a guide for computer security specialists.

Keywords: cyber incidents; incident management; methodology; computer attacks.

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 ataques informáticos. Las universidades son uno de los objetivos preferidos de los atacantes, debido a la gran cantidad de usuarios conectados a internet. Entre los ataques informáticos más comunes se encuentran acceso no autorizado a sitios web, ransomware que exigen rescate, ataques de denegación de servicios, ataques de phishing, 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 ataques informáticos.

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 en la respuesta de los mismos. Poca preparación de los especialistas para gestionar 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 solucionarse.

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 al proceso de gestión de ciberincidentes en las universidades cubanas.

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.

Ciberespacio

El Ciberespacio es el ambiente virtual y dinámico, definido por tecnologías, equipos, procesos y sistemas de información, control y comunicaciones, que interactúan entre sí y con las personas, y en el que la información se crea, procesa, almacena y transmite (Decreto 360, 2019).

Incidentes de seguridad

Un incidente de seguridad se considera a cualquier evento que se produzca de forma accidental o intencional, que afecte o ponga en peligro las tecnologías de la información y la comunicación o los procesos que con ellas se realizan (Decreto 360, 2019).

Ciberincidente

Como caso específico de los incidentes de seguridad, se encuentran los ciberincidentes. Se define un ciberincidente como un incidente relacionado con la seguridad de las Tecnologías de la Información y las Comunicaciones que se producen en el ciberespacio (CCN-CERT, 2020).

Amenaza

Una amenaza se define como la situación o acontecimiento que puede causar daños a los bienes informáticos, sea una persona, un programa maligno o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema (Decreto 360, 2019).

Ataque informático

Un ataque informático se denomina al intento de acceso o acceso a un sistema o una red informática o terminal mediante la explotación de vulnerabilidades existentes en su seguridad (Decreto 360, 2019).

Vulnerabilidad

Una vulnerabilidad se identifica como el punto o aspecto del sistema que muestra debilidad al ser atacado o que puede ser dañada su seguridad; representa los aspectos falibles o atacables en el sistema informático y califica el nivel de riesgo de un sistema (Decreto 360, 2019).

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. Para ello los niveles que se

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

establecen son Muy Alto, Alto, Medio y Bajo (Resolución 105, 2021), y los factores que se pueden considerar son los siguientes:

Tabla 1- Clasificación de los ciberincidentes.

Clasificación	Tipo de ciberincidente	Peligrosidad
Programas malignos	Amenaza persistente	Muy Alto
	Robot informáticos (botnet)	Alto
	Gusanos	Alto
	Secuestro de la información (Ransomware)	Muy Alto
	Troyanos	Alto
	Tráfico con C&C (mando y control)	Alto
	Virus informáticos	Alto
	Programas espías (Spyware)	Alto
Ataques técnicos o intrusión	Denegación de servicios	Alto
	Denegación de servicios distribuidos	Muy Alto
	Ataque por fuerza bruta	Alto
	Explotación de vulnerabilidades	Muy Alto
	Manipulación del DNS	Alto
Compromiso de la información	Borrado o modificación de la información	Alto
	Robo de información	Alto
	Hombre en el medio	Alto
	Ingeniería social	Alto
	Phishing	Medio
Desfiguración de sitios web	Inclusión local o remota de ficheros	Alto
	Inyección de código	Alto
Correos no deseados	Spam	Bajo
	Hoax	Bajo

Fuente: (Resolución 105, 2021).

La gestión de incidentes es el proceso que se realiza con el objetivo de prevenir, detectar y enfrentar los de ciberseguridad y comprende las acciones que se realizan antes, durante y después de su ocurrencia (Decreto 360, 2019).

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

Resultados y discusión

Cada universidad gestiona de forma diferente los ciberincidentes. Con el objetivo de contribuir al proceso de gestión de ciberincidentes, se propone la elaboración de una Metodología para la gestión de ciberincidentes, que contribuya al proceso de gestión de ciberincidentes en las universidades cubanas.

La metodología propuesta cuenta con varias etapas, 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 ciberincidentes:

Fig. 1- Etapas de la gestión de ciberincidentes.

Etapa 1. Prevención y protección: En esta etapa inicial, las universidades deben estar preparadas para enfrentar de la mejor manera posible cualquier evento que pueda ocurrir. Dentro de las acciones que se deben llevar a cabo se encuentra la creación y preparación de un equipo de respuesta a incidentes, donde los mismos deben estar formados por especialistas capaces y preparados para enfrentar cualquier evento que se pueda presentar. Cumplir con las regulaciones de instancias superiores, las mismas incluyen las regulaciones, reglamentos y normas vigentes en el país y fomentar una cultura de ciberseguridad en los usuarios. Además, deben contar con recursos que faciliten la gestión de incidentes, entre los que se encuentran parches de seguridad, discos de instalación de sistemas operativos, así como un conjunto de herramientas para el tratamiento de incidentes, como son sistemas de detección de intrusos, cortafuegos, software antispam, escáner de vulnerabilidades, herramientas para el análisis forense, entre otros.

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

Etapa 2. Detección, evaluación y notificación: En esta etapa, 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 para detectar ciberincidentes se encuentran las siguientes:

1. Reportes de los usuarios de las tecnologías. Estos reportes pueden ser de estudiantes, profesores, trabajadores, especialistas, terceros, OSRI y se pueden recibir mediante correo electrónico, personalmente o por un sistema de gestión de incidentes, si la universidad cuenta con uno.
2. Revisión periódica de las herramientas automáticas. Si se encuentra la presencia de uno de los siguientes indicios, es muy probable que exista un incidente de seguridad:

Tabla 2- Tipos de indicios.

Tipos de indicios	
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 del IDS sobre desbordamiento de buffer	Nuevas cuentas inexplicables

Fuente: (García, 2014).

Para descubrir algunos de los indicios anteriores, generalmente se puede hacer mediante la revisión periódica de los reportes de las herramientas automáticas, dentro de los que se encuentran: cortafuegos, sistemas SIEM, IDS, antivirus, sistemas antispam, filtros de correo, análisis de registros de auditoría (logs), software de control de integridad de archivos, entre otras.

Al comenzar con la evaluación del ciberincidente, se debe determinar si el problema realmente existe, para ello se identifica si se viola alguna política establecida en el reglamento interno de la universidad o en las

regulaciones y decretos existentes en el país relacionado con la gestión de incidentes. Además, se puede utilizar cualquier software de detección disponible y la revisión de los registros de auditoría.

Se preservan las evidencias digitales con fines forenses, para ello se debe identificar cuales deben recogerse para su posterior análisis. Donde generalmente se recogen evidencias de la cache, procesos, memoria, ficheros temporales del sistema, disco, datos relevantes de conexiones remotas y monitoreo, etc. De ellos se debe establecer el orden de la volatilidad de los datos para que no se pierdan.

Se debe clasificar el ciberincidente de acuerdo a las siguientes características:

Tabla 3- Clasificación de los ciberincidentes.

Origen de la amenaza	Externa
Tipo de amenaza	Identificar el tipo de amenaza al que pertenece el ciberincidente detectado, dentro de las que se encuentran, programas malignos, desfiguración de sitios web, ataques técnicos o intrusiones, compromiso de la información y correos no deseados.
Peligrosidad	La peligrosidad refleja el peligro que el ciberincidente representa para las universidades. Para establecer el valor de la peligrosidad se tiene en cuenta lo establecido en la Resolución 105, Tabla 1.
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 incidentes define los niveles de prioridad de acuerdo a sus características.

Fuente: Elaboración propia.

Tabla 4- Niveles de prioridad por ciberincidentes.

Nivel	**Características**
Muy Alta	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

Revista Cubana de Ciencias Informáticas
Vol. 16, No. 4, Octubre-Diciembre, 2022
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 101-113

	ejemplo, todos los incidentes no clasificados con prioridad alta o muy alta, 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.

Fuente: (García, 2014).

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

Tabla 5- Tiempo de respuesta por cada tipo de ciberincidente.

Nivel de peligrosidad	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	

Fuente: Elaboración propia.

Por último, se debe realizar la contención a corto plazo, con el objetivo de limitar el daño del ciberincidente tan pronto como sea posible. Al concluir con las clasificaciones, se recopilan los datos de diferentes fuentes de información, para su posterior análisis.

Una vez analizado el ciberincidente, se debe notificar por correo electrónico a los niveles correspondientes:

1. Informar sobre la ocurrencia del incidente al jefe inmediato superior para obtener autorización para comenzar la investigación, donde se hará lo siguiente:

2. Crear un grupo de trabajo que será el encargado de la investigación. Donde los miembros deben ser personas altamente calificadas y deben contar con la autorización y los permisos necesarios para realizar las tareas asignadas.
3. Definir las responsabilidades de cada miembro del equipo.
4. Designar el miembro principal de la investigación.
5. Informar sobre la ocurrencia del ciberincidente a la OSRI.

Etapa 3. Investigación: Esta etapa se realiza con el objetivo de investigar lo ocurrido. Para ello se debe identificar el vector de ataque que utilizaron los atacantes, esto se logra mediante el análisis de las diferentes fuentes de información. Además, se debe determinar el origen, autor o autores (IP, direcciones de correo), la causa, los dispositivos afectados (redes, sistemas, aplicaciones, host), como ocurrió el ciberincidente (métodos de ataque, vulnerabilidades explotadas), etc.

Etapa 4. Mitigación y recuperación: 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 para que no siga produciendo daño. Además de eliminar las causas del incidente, y regresar el sistema afectado a su funcionamiento normal. Algunas de las medidas más comunes son las siguientes:

1. Identificar y eliminar todo el software utilizado por los atacantes.
2. Recuperar la información de salvas previamente definidas, donde se debe confirmar que las mismas son confiables y están libres de cualquier problema de seguridad.
3. Validar el funcionamiento correcto del sistema y luego realizar una nueva salva.

Etapa 5. Post-ciberincidente: La misma se realiza una vez que el ciberincidente esté controlado y la actividad ha vuelto a la normalidad. En esta etapa se realizará un informe lo más completo posible donde se describa detalladamente las medidas tomadas, la información comprometida, los usuarios y

dispositivos afectados. 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.

Conclusiones

Como resultado de la investigación se concluye lo siguiente:

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

Referencias

Alsmadi, I. The NICE Cyber Security Framework. Cyber Security Intelligence and Analytics. Springer, 2019.

Eric T. Cybersecurity Incident Response. How to Contain, Eradicate, and Recover from Incidents. 2018.

Cert, C. C. N. (2020). Guía de seguridad de las TIC (CCN-STIC-817) Esquema Nacional de Seguridad Gestión de Ciberincidentes. CCN Cert.

Prasad, R., & Rohokale, V. Cyber Security: The Lifeline of Information and Communication Technology. Springer International Publishing, 2020.

Ministerio de Comunicaciones, 2017. Política Integral para el Perfeccionamiento de la Informatización de la

Sociedad en Cuba., vol. 91, pp. 399-404.

Ministerio de Comunicaciones. (2019). Resolución 128 Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación.

Ministerio de Comunicaciones. (2019). Decreto No. 360/2019 Sobre la Seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional.

Ministerio de Comunicaciones. (2021). Resolución 105 Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad.

DBIR Verizon. (2019). 2019 Data Breach Investigations Report.

DBIR Verizon. (2020). 2020 Data Breach Investigations Report.

DBIR Verizon. (2021). 2021 Data Breach Investigations Report.

Universidad Central de Texa. (2018). Education Cybersecurity Report. (2018). SecurityScorecard.

Chapman, J. (2019). How Safe is Your Data? Cyber-security in Higher Education. Higher Education Policy Institute.

Instituto Nacional de Ciberseguridad. (2019). Procedimiento de gestión de ciberincidentes para el sector privado y la ciudadanía.

Instituto Nacional de Ciberseguridad. (2020). Guía Nacional de Notificación y Gestión de Ciberincidentes.

García Pierrat G. Administración de incidentes de Seguridad Informática, 2014.

Patrick Kral. SANS Institute Information Security Reading RoomThe, Incident Handlers Handbook. 2012.

NIST, S. (2012). 800-61, Revision 2. Computer Security Incident Handling Guide.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. NIST Special Publication, 800(61), 1-147.

Conflicto de interés

El autor no tiene conflicto de interés y autoriza la distribución y uso de su artículo.

Contribuciones de los autores

1. Conceptualización: Contribución de todos los autores
2. Curación de datos: Contribución de todos los autores

3. Análisis formal: Contribución de todos los autores
4. Adquisición de fondos: Contribución de todos los autores
5. Investigación: Yailin Sánchez Borrell
6. Metodología: Contribución de todos los autores
7. Administración del proyecto: Contribución de todos los autores
8. Recursos: Contribución de todos los autores
9. Software: Contribución de todos los autores
10. Supervisión: Contribución de todos los autores
11. Validación: Contribución de todos los autores
12. Visualización: Contribución de todos los autores
13. Redacción – borrador original: Yailin Sánchez Borrell
14. Redacción – revisión y edición: Yailin Sánchez Borrell y Dennis Barrera Pérez.