REVISTA MÁRGENES. VOLUMEN 11 NÚMERO 3. AÑO SEPTIEMBRE-DICIEMBRE 2023

ARTÍCULO DE INVESTIGACIÓN ORIGINAL

UNIVERSIDAD DE SANCTI SPÍRITUS
José Martí Pérez
MÁRGENES
Revista multitemática de desarrollo local y sostenibilidad
ISSN: 2664-2190
RNPS: 2460

Fecha de presentación: 25/4/2023 Fecha de aceptación: 24/7/2023 Fecha de publicación: 25/9/2023

¿Cómo citar este artículo?

Mahmoud Díaz, S., Jiménez Puerto, C, L. y Companioni Martínez, J. (2023). Sistema de gestión de incidentes de seguridad informática en la universidad de Sancti Spíritus. *Revista Márgenes,* *11*(3), 57-68. https://revistas.uniss.edu.cu/index.php/margenes/article/view/1721

TÍTULO: SISTEMA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA EN LAUNIVERSIDAD DE SANCTI SPÍRITUS

TILTE: CYBERSECURITY INCIDENT MANAGEMENT SYSTEM AT THE UNIVERSITY OFSANCTI SPIRITUS

Autores:

Est. Somar Mahmoud Díaz[1]

E-mail: somarmahmouddiaz@gmail.com

https://orcid.org/0009-0005-5070-1029

Dr. C. Carlos Lázaro Jiménez Puerto[2]

E-mail: puerto@uniss.edu.cu

https://orcid.org/0000-0002-3075-8504

M. Sc. Julio Companioni Martínez[2]

E-mail: jcmartinez@uniss.edu.cu

https://orcid.org/0000-0001-7412-7758

[1]Estudiante extranjero de la República Árabe de Siria, Facultad de Ciencias Técnicas y Económicas. Sancti Spíritus, Cuba.
[2]Universidad de Sancti Spíritus "José Martí Pérez", Departamento de Ingeniería Informática, Facultad de Ciencias Técnicas y Económicas. Sancti Spíritus, Cuba.

RESUMEN

Introducción: Hoy, la información constituye un asunto importante para personas u organizaciones, por lo tanto, su protección se ha convertido en una prioridad, que aún no cuenta con una fórmula única que pueda garantizarla totalmente. En este sentido, se hace necesario el uso de herramientas que brinden ayuda a los especialistas en seguridad de la información para la gestión de los incidentes.

Objetivo: Identificar las metodologías y herramientas para desarrollar un sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus "José Martí Pérez".

Métodos: Desde un punto de vista científico se asumen como métodos la observación científica, el análisis de documentos, la encuesta y la entrevista, dando lugar a una propuesta susceptible de verificación y validación científica.

Resultados: Implementación de un sistema informático que gestiona los incidentes de ciberseguridad; adicionalmente cuenta con una base de datos que contiene incidentes y reportes. Asimismo, se desarrolló, un módulo para la detección de vulnerabilidades de un sitio web.

Conclusiones: La puesta en funcionamiento del sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus "José Martí Pérez", se valora de positiva como apoyo para la gestión, el registro y control del avance de cada incidente, reporte o informe en un solo repositorio.

Palabras Claves: ciberseguridad; gestión; incidentes; reportes.

ABSTRACT

Introduction: Nowadays, information is a very important asset for people or organizations; therefore, protecting it has become a priority for everyone, though there is not a unique formula to guarantee it. Thus, it is necessary to use tools helping information security specialists to manage incidents.

Objective: To identify the methodologies and tools to develop a cybersecurity incident management system at the University of Sancti Spíritus "José Martí Pérez".

Methods: From a scientific point of view, the methods assumed are scientific observation, document analysis, survey and interview, giving rise to a proposal susceptible of scientific verification and validation.

Results: A computer software system that manages cybersecurity incidents was implemented. Additionally, it has a database that contains incidents and reports. Likewise, a module for detecting vulnerabilities in websites was developed.

Conclusions: The implementation of a cybersecurity incident management system at the University of Sancti Spíritus "José Martí Pérez" is valued as positive for supporting the management, recording and control of the progress of each incident or report in a single repository.

Keywords: cybersecurity; incidents; management; reports.

INTRODUCCIÓN

Desde 1950 comenzaron a desarrollarse las redes computacionales, lo que posibilitó el surgimiento de las primeras redes informáticas y módems, desde ese momento se comenzó a hablar de seguridad informática. En el 1960 la seguridad informática comenzó a tomar la forma que se le conoce en la actualidad.

Al tener en cuenta lo anterior, se puede separar esta disciplina en dos partes: antes y después de la invención del Internet. Antes del Internet, la única forma de dañar un dispositivo era acceder físicamente a él, por lo tanto, el delito era considerado como “allanamiento de morada” y no ciberataque (Mata Barranco, 2016). Después de la

invención del Internet a finales de los 60 fue cuando nace el ciberespacio, lo que significó un nuevo entorno y una nueva posibilidad para los ciberdelincuentes.

A medida que las empresas comenzaron a utilizar la web, controlar el acceso a los datos en los sistemas se convirtió en un punto importante de preocupación a mediados finales de la década de 1960. Entre las primeras medidas para proteger la información se incluye el procesamiento de periodos, donde se separaban las actividades por partes, y los usuarios podían manipular la información en un tiempo determinado, establecido por los expertos de Ciberseguridad.

Es indudable que la seguridad de los sistemas informáticos de cualquier organización se ha convertido en uno de los pilares más sostenibles y vulnerables, y se hace imprescindible la búsqueda de los mecanismos para fortalecerla. El plan de la seguridad se convierte en una herramienta fundamental en el tratamiento de la información, en la explotación de los recursos tecnológicos, y en el desarrollo de nuevas aplicaciones y tecnologías para la implementación de sistemas más avanzados a escala internacional (Vera-Baceta et al., 2022).

En la actualidad, la seguridad informática no es solo un tema importante para las grandes empresas, sino también para las universidades. Con la creciente cantidad de información personal almacenada en dispositivos digitales y la transmisión de información a través de redes, esta, se ha convertido en un tema crítico para la protección de la privacidad y la integridad de los datos (Solís Tejedor et al., 2023). Por esta razón, cada vez más personas toman medidas para proteger sus sistemas y datos de las amenazas cibernéticas.

Cuba no es la excepción, el avance de la seguridad informática se ha notado y ha cobrado más auge en los últimos años a partir del proceso de informatización de la sociedad cubana, el surgimiento de la Universidad de Ciencias Informáticas (UCI) en 2003 y la apertura en esta de programas orientados a la seguridad informática (ciclo corto y carrera universitaria).

La Universidad “José Martí Pérez” de Sancti Spíritus (Uniss), cuenta con un grupo de seguridad informática, subordinado al rector, para mantener el control y la seguridad de los datos personales y profesionales de todas las estructuras de la organización. El grupo de seguridad informática de la Universidad de Sancti Spíritus “José Martí Pérez” en el desarrollo de sus actividades, se han identificado algunas problemáticas prácticas:

1. Todo el trabajo que se realiza en el departamento no está automatizado sino se encuentra la mayor parte en formato duro.
2. Existe una única planilla para los reportes de incidentes donde se tiene que sobrescribir cada vez que ocurra un incidente y se encuentra en Word.
3. No existe una base de datos que almacene todos los incidentes ocurridos y los que irán a ocurrir en algún futuro, en cambio se guardan en una carpeta.
4. La falta de cultura y conocimiento sobre la seguridad informática en toda la universidad.

Por lo tanto, el departamento quiere a través de la gestión, planeación y planificación brindar tanto los servicios de seguridad para todas las entidades de la organización, como expandir la cultura de la seguridad informática en la misma.

Las demandas sociales actuales exigen de la universidad un proceso de gestión de la seguridad informática consciente, basado en un proyecto flexible y competente, que prometa cobertura suficiente y satisfaga las necesidades de la organización, y resuelva las carencias y necesidades de sus profesionales, de ahí se deriva el objetivo de esta investigación: Identificar las metodologías y herramientas para desarrollar un sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus “José Martí Pérez” (Uniss).

DESARROLLO

Actualmente las comunicaciones y relaciones sociales se dan a través de los diversos dispositivos electrónicos dentro de un entorno virtual; lo cual, si bien acorta distancias y permite tener acceso a una cantidad infinita de contenido en solo segundos, al mismo

tiempo representa un grave riesgo para la seguridad de los ciudadanos y una constante amenaza a sus derechos humanos (Tapia Hernández et al., 2021).

Las organizaciones tratan de proteger los activos cibernéticos e implementar medidas y programas de ciberseguridad, pero a pesar de este esfuerzo continuo, es inevitable que se presenten las violaciones de la ciberseguridad y se materialicen ataques cibernéticos (Sabillón y Cano, 2019).

Tener un control, una administración y una gestión de los incidentes de seguridad informática es un pilar clave que debe tener cada organización (Bodin et al., 2018), y es ahí donde cae toda la importancia del software que se trata en este artículo.

Importancia del Software:

Cada incidente de ciberseguridad que ocurra en la Universidad de Sancti Spíritus "José Martí Pérez" (Uniss), se tiene que archivar por varios motivos entre ellos es para tener más precaución en un futuro y para proceder con los reglamentos y cuestiones necesarias al caso, por lo tanto, se necesita de una herramienta para la gestión de los incidentes en dicha institución ya que el departamento de seguridad informática de la Uniss cuenta con especialistas en la disciplina pero carece de una herramienta para la gestión de los incidentes. Como se ha mencionado anteriormente se cuenta con una plantilla en Word donde se procesan los incidentes y se sobrescriben cada vez que ocurra uno nuevo.

La importancia del sistema de gestión de los incidentes de seguridad informática es en la organización y la administración de los incidentes, ya que de eso dependen muchas informaciones tanto institucionales como personales de los empleados y estudiantes de la misma.

Características del Software:

El sistema contará con los siguientes apartados:

Un apartado para la gestión y administración de los tipos de reportes que se le realizan a los incidentes, entre ellos se encuentran los reportes de tipo Cucert y los reportes de

tipo incidente violación, donde se podrán tanto crear y modificar, como mostrar y eliminar algún reporte del tipo deseado. También contará con la posibilidad de exportar a PDF algún reporte deseado para así imprimirlo y archivarlo en formato duro después de haber sido procesado.

Habrá un apartado donde se gestionen los informes de visitas realizadas o que se realizarán a las distintas áreas de la organización, que al igual que los reportes se podrán exportar a PDF para su procesamiento. Un apartado de la administración de los usuarios del sistema son los administradores, así como los usuarios de la universidad.

Contará con un servicio RCS donde se estarán publicando noticias sobre la seguridad informática para así expandir la cultura de la misma entre las entidades de la organización.

Tendrá un apartado para la detección de vulnerabilidades de un sitio web dado su enlace. Ese apartado es una de las herramientas más importantes del sistema ya que ocurren muy a menudo ataques categorizados como (Phishing) o pesca donde se envía un enlace por vía de correo electrónico que contiene algún software malicioso o malware que termina causando daño al receptor del correo. Con dicha herramienta se podrá saber si el enlace enviado es legítimo o no.

Sistemas y Software similares:

En la universidad de ciencias médicas de Holguín se ha realizado un sistema de gestión de la información asociada con la seguridad informática de la misma. El sistema cuenta con herramientas similares para la gestión de los incidentes que ocurren en la universidad. La Uniss propone un sistema con varias diferencias en la estructura, el sistema que se desarrollará en la misma, cuenta con herramientas más avanzadas y más asociadas a seguridad que el sistema de la universidad de ciencias médicas de Holguín, como es el caso del detector de vulnerabilidades y el servicio RCS para las noticias más recientes de la disciplina.

En la universidad de ciencias médicas de Holguín se tratan otros tipos de incidentes y reportes asociados a la seguridad informática distintos a los incidentes y reportes que se conocieran en el sistema de la Uniss.

MATERIALES Y MÉTODOS

La metodología empleada permite obtener una propuesta flexible como alternativa de solución, susceptible a comprobación científica; se emplearon los siguientes métodos de la investigación científica.

Del nivel teórico:

• Análisis histórico-lógico, que permitió el estudio del modo en que han evolucionado los estándares y normas para la gestión de la seguridad informática.

• Analítico-sintético, posibilitó el estudio de los principales sistemas de gestión de seguridad informática, así como las tendencias en la gestión de incidentes y detección de vulnerabilidades.

Del nivel empírico:

• Observación, guió el estudio del estado del arte, permitiendo realizar un análisis sistémico, selectivo y objetivo de los principales sistemas que en la actualidad puede realizar la gestión de la seguridad informática.

• Entrevista no estructurada, se aplicó con la intención de obtener información referente a los procesos de gestión de incidentes y detección de vulnerabilidades, así como criterios de expertos en el tema.

RESULTADOS Y DISCUSIÓN

El procesamiento de los resultados obtenidos con la aplicación de los métodos descritos, permitió identificar las metodologías y herramientas para desarrollar el sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus “José Martí Pérez” (Uniss).

A la hora de desarrollar este sistema hay que tener en cuenta algunos elementos que forman parte del mismo desarrollo, en este caso de los *frameworks* que pueden ser

utilizados en la parte “interfaz” a la que se dedica el *frontend*, al contrario que el *backend* que se basa en el interior del código (Pérez Ibarra et al., 2021). Las particularidades se presentan a continuación.

Tecnologías para el desarrollo de Frontend (Interfaz de usuario):

Angular:

Según los desarrolladores de Angular, “Angular es un *framework* para aplicaciones web desarrollado en *TypeScript*, de código abierto, mantenido por Google, que se utiliza para crear y mantener aplicaciones web de una sola página”.

HTML 5:

HTML (Lenguaje de Marcas de Hipertexto) es el lenguaje con el que se define el contenido de las páginas web. Básicamente se trata de un conjunto de etiquetas que sirven para definir el texto y otros elementos que compondrán una página web, como imágenes, listas y vídeos.

CSS:

CSS (Hojas de Estilo en Cascada) es un lenguaje de diseño gráfico para definir y crear la presentación de un documento estructurado escrito en un lenguaje de marcado.

Boostrap:

Bootstrap es una biblioteca multiplataforma o conjunto de herramientas de código abierto para diseño de sitios y aplicaciones web.

Tecnologías para el desarrollo del Backend (Funciones y Funcionalidades):

API:

API (Interfaz de programación de aplicaciones) se refiere a cualquier software con una función distinta. La interfaz puede considerarse como un contrato de servicio entre dos aplicaciones.

Python:

Python es un lenguaje de programación ampliamente utilizado en las aplicaciones web, el desarrollo de software, la ciencia de datos y el machine learning (ML). Los

desarrolladores utilizan Python porque es eficiente y fácil de aprender, además de que se puede ejecutar en muchas plataformas diferentes.

Django:

Django es un *framework* del lenguaje Python que puede utilizar para desarrollar aplicaciones web de forma rápida y eficiente.

Herramientas para la base de datos:

El gestor de datos es un sistema de software invisible para el usuario final, compuesto por un lenguaje de definición de datos, un lenguaje de manipulación y de consulta, que puede trabajar a distintos niveles.

PostgreSQL:

PostreSQL es un sistema de gestión de bases de datos relacional orientado a objetos y de código abierto, publicado bajo la licencia PostgreSQL similar a la BSD (Distribución de software Berkeley) o la MIT (Instituto de Tecnología de Massachusetts).

CONCLUSIONES

- El análisis de los mecanismos para la gestión de incidentes de ciberseguridad tanto nacionales como internacionales evidenció la necesidad de implementar una solución a la medida del Grupo que atiende la función en la Universidad de Sancti Spíritus “José Martí Pérez”, porque las soluciones encontradas no satisfacen por sí solas las necesidades del presente trabajo de diploma. Además, permitió identificar nuevos requisitos.
- Los resultados del procesamiento de métodos del nivel empírico permitieron identificar las metodologías y herramientas para desarrollar el Sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus “José Martí Pérez” (Uniss).
- La vinculación entre las tecnologías para el desarrollo de Frontend, el Backend y las herramientas para la base de datos permitió dar inicio a la implementación

del Sistema para la gestión de los incidentes de ciberseguridad de la Universidad de Sancti Spíritus “José Martí Pérez” (Uniss).

REFERENCIAS BIBLIOGRÁFICAS

Bodin, L. D., Gordon, L. A. & Loeb, M. P. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Poly, 37*(6), 527-544. https://www.sciencedirect.com/science/article/abs/pii/S0278425418302382

Mata Barranco, N. J. de la (2016). Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito. *Cuadernos de Política Criminal*, (118), 43-86. https://dialnet.unirojas.es/servlex/articulo?codigo=6078276

Pérez Ibarra, S. G., Quispe, J. R., Mullicundo, F. F. y Lamas, D. A. (2021). *Herramientas y tecnologías para el desarrollo web desde el FrontEnd al BackEnd*. [Conferencia]. XXIII Workshop de Investigadores en Ciencias de la Computación, La Rioja, Chilecito, Argentina. http://sedici.unpl.edu.ar/handle/10915/120476

Sabillón, R. y Cano, J. J. (2019). Auditorías en ciberseguridad: Un modelo de aplicación general para empresas y naciones. *Revista Ibérica* de Sistemas *e Tecnologías de Informacao,* (32), 33-48. https://doi.org/10.17013/risti.32.33-48

Solís Tejedor, B. G., Valderrama Castrellón, H., Tejedor De León, E. y Vásquez de Ayala, D. (2023). Seguridad de los Sistemas Informáticos Universitarios: Retos Pendientes. *Revista Especializada de Ingeniería y Ciencias de la Tierra: REICIT, 2*(2), 113-142. https://revistas.up.ac.pa/index.php/REICIT/article/view/3585/3104

Tapia Hernández, E. F., Ruiz Canizales, R. y Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Revista Misión Jurídica, 14*(20), 142-158. https://www.revistamisionjuridica.com/la-importancia-de-la-ciberseguridad-y-los-derechos-humanos-en-el-entorno-virtual/

Vera-Baceta, M. Á., Navarro Carretero, G. y Gómez-Hernández, J. A. (2022). Riesgos de la aceleración digital: una mirada desde el Marco DIGCOMP2.2 y los

derechos digitales de la ciudadanía. *Anuario ThinkEPI*, *16*(1). https://dialnet.unirojas.es/servlex/articulo?codigo=8546677&orden=0&info=link

Conflicto de intereses:
Los autores declaran no tener conflictos de intereses.

Contribución de los autores:
S.M.D.: Diseño de la investigación, recolección de datos, análisis de los resultados, redacción del borrador del artículo.
C.L.J.P.: Orientación científica y metodológica. Revisión crítica de su contenido y aprobación final.
J.C.M.: Redacción del borrador delartículo. Revisión crítica de su contenido y aprobación final.