Vulnerabilidades de los Sistemas de Información: una revisión

Information System Vulnerabilities: A review.

Yeison Molina Marin[1]*

Luis Guillermo Orozco[2]**

Resumen

La seguridad informática en la actualidad ha pasado a ser una prioridad para las empresas y organizaciones, debido a que la información se ha convertido en un activo valioso y fundamental para su funcionamiento. El objetivo de este artículo, es realizar una revisión del estado del arte y de las metodologías implementadas en el tema de las vulnerabilidades de los sistemas de información estableciendo algunas características tanto de los conceptos de ciberseguridad como análisis de vulnerabilidades a los sistemas de información para luego realizar un corto recorrido sobre algunos tipos de vulnerabilidades como lo son día cero, aplicaciones web y gestores de bases de datos como también de los sistemas de información erp, mecanismos y controles de sistemas de información, seguridad en sitios web, políticas de seguridad, penetration testing y seguridad en TI**.** Finalmente se presenta una conclusión referente a la revisión de los temas anteriores.

Palabras clave:Vulnerabilidades SI, Riesgo, ERP, Día cero, Owasp, Pentesting, Políticas de seguridad.

Abstract

Computer security today has become a priority for companies and organizations, because information has become a valuable and fundamental asset for their operation. The objective of this article is to perform a review of the state of the art and the methodologies implemented in the subject of vulnerabilities in information systems, establishing some characteristics of both the concepts of cybersecurity and analysis of vulnerabilities to information systems and then to take a short tour of some types of vulnerabilities such as zero day, web applications and database managers as well as erp information systems, information systems mechanisms and controls, website security, security policies, penetration testing and IT security. Finally, a conclusion is presented regarding the review of the previous topics.

Keywords: Vulnerability SI, risk, ERP, Zero day, owasp, pentesting, security policies.

---

[1]* Yeison Molina Marin.. Analista de Infraestructura. Tecnológico de Antioquia. yeison.molina.marin@gmail.com.

[2]** Luis Guillermo Orozco. Ingeniero de Sistemas. Tecnológico de Antioquia. lgorozconott19@gmail.com.

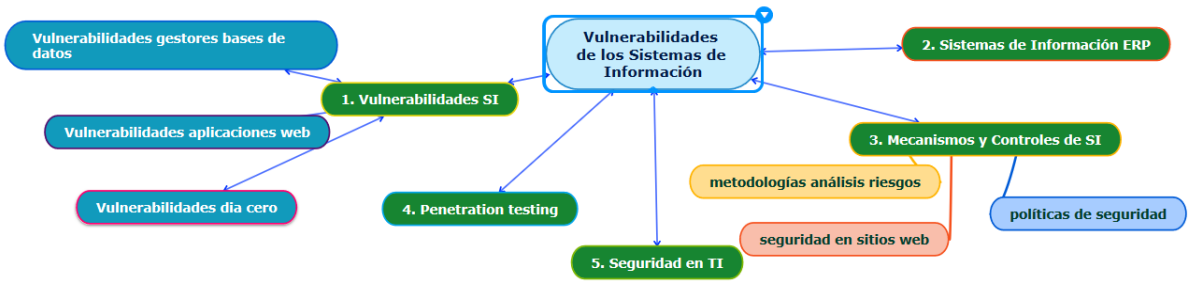
Introducción

La seguridad de la información se refiere a la protección de la confidencialidad, integridad y acceso a la información, “La evidencia sugiere que, independientemente del número de controles técnicos implementados, las organizaciones aún experimentan brechas de seguridad” (Safianu, Twum y Hayfron-Acquah, 2016, p.8). En la actualidad, la información toma un papel fundamental en el adecuado funcionamiento de las empresas y organizaciones, convirtiendo a la información en un activo importante y la seguridad en una inversión necesaria para evitar riesgos en los sistemas de información “Los robos de información o de sistemas, actualmente es el delito con mayor crecimiento a nivel mundial, causando no solamente el desconcertó y enojo por lo sucedido, sino, que causa grandes pérdidas económicas a nivel empresarial.” (Castro, 2011, citado en Arévalo-Cordovilla et al. 2020,p.839). Las vulnerabilidades de los sistemas de información es el resultado de bugs en el diseño del sistema, también puede ser resultado de las limitaciones tecnológicas. En la actualidad existen diferentes tipos de vulnerabilidades que ponen en riesgo los sistemas de información, por ejemplo las vulnerabilidades de día cero, de aplicaciones web y de gestores de bases de datos.

Metodología

Se realizó una búsqueda sistemática del estado del arte en el tema de vulnerabilidades de los sistemas de información y se clasificaron 50 artículos de acuerdo con el tema y se identificaron diferentes metodologías relacionadas con las vulnerabilidades de los sistemas información. En el siguiente mapa conceptual se exponen las principales metodologías identificadas en la revisión del estado del arte. Se aborda cada una de ellas en las siguientes subsecciones y se realiza la delimitación del problema.

Figura 1 - Mapa conceptual que describe el estado del arte de las vulnerabilidades de los sistemas de información.



Fuente: Propia de los autores

Ciberseguridad

Este concepto implica un conjunto de herramientas, políticas, conceptos de seguridad, controles de seguridad, directrices y toda aquella práctica que se utilice para proteger la seguridad de la información, los activos de la organización y de los usuarios. La ciberseguridad es importante porque garantiza que se cumplan y mantengan las propiedades de seguridad al momento de presentarse riesgos en el ciberentorno. Según (José y Montealegre, 2016, p.16) “Las propiedades de seguridad incluyen una o más de las siguientes características: Disponibilidad, integridad que puede incluir la autenticidad y el

no repudio y la confidencialidad". Las anteriores tres propiedades se conocen como los pilares de la información, los cuales se caracterizan por mantener un sistema seguro y fiable, siendo este el objetivo de la ciberseguridad. Como lo menciona International Organization for Standardization en el 2014, la norma ISO/IEC 27000:2014 define a la seguridad de la información como la preservación de la confidencialidad, integridad y disponibilidad de la información (José y Montealegre, 2016,p.17)

Dentro del contexto de la ciberseguridad, existen diferentes prácticas para analizar los riesgos que tienen los sistemas de información, el análisis de vulnerabilidades es una de ellas. A continuación, se realiza una revisión sobre las características del análisis de vulnerabilidades a un Sistema de información como lo son los ERP "*Enterprise Resource Planning".*

Análisis de Vulnerabilidades

En la actualidad existen diferentes tipos de vulnerabilidades que ponen en riesgo los sistemas de información, por ejemplo las vulnerabilidades de día cero, de aplicaciones web y de gestores de bases de datos entre otros, a continuación se hace una breve descripción de las características de algunas de estas vulnerabilidades.

1. Vulnerabilidades Sistemas de información (SI)

En la actualidad las empresas almacenan de forma electrónica grandes cantidades de información, la manera en la que las mismas organizaciones se comunican y traspasan información en vías de internet puede resultar peligroso y obtener como resultado la exposición de datos.

La vulnerabilidad es el resultado de bugs en el diseño del sistema, también puede ser resultado de las limitaciones tecnológicas. "En los Sistemas de Información (SI), la vulnerabilidad es conocida como aquella debilidad de cualquier tipo que compromete la seguridad del sistema informático" (Arévalo-Cordovilla et al. 2020,p.837)

Arévalo-Cordovilla et al. 2020, mencionan que "En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones" p.836. Siendo los sistemas de información un activo fundamental de las organizaciones resulta como prioridad el cuidar y proteger la información de cualquier riesgo informático que se pueda presentar. Hoy en día el robo de información o de sistemas está calificado como un delito mayor generando pérdidas económicas a nivel empresarial en gran medida. Según (Arévalo-Cordovilla et al. 2020, p.839) las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

> Diseño:debilidad en el diseño de protocolos utilizados en las redes, políticas de seguridad deficientes e inexistentes. Implementación: errores de programación, existencia de "puertas traseras" en los sistemas informáticos, descuido de los fabricantes. Uso: mala configuración de los sistemas informáticos, desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, disponibilidad de herramientas que facilitan los ataques, y la limitación gubernamental de tecnologías de seguridad.

Los sistemas de información de una organización pueden ser vulnerables como resultado del factor humano, por más que una empresa compre las mejores tecnologías o soluciones de seguridad en software o en hardware la empresa aún puede ser vulnerable debido a factores como personal poco capacitado, desconocimiento de herramientas y falta de experiencia en el campo.

1.1 Vulnerabilidades día cero

La vulnerabilidad de día cero es una brecha en la seguridad del software o hardware, es un tipo de vulnerabilidad que acaba de ser descubierta y que se presenta de forma desconocida para los sistemas de detección de intrusos, existen pocos métodos de defensa para detectar este tipo de ataques. Según (Guisao y Toro, 2014):

> La detección temprana de vulnerabilidades día cero le permite a las organizaciones tomar acciones de divulgación, informando a entidades y fabricantes, lo cual permitiría contar con tiempos de respuesta rápidos y con acciones que favorezcan a otros posibles afectados; así se evita el daño en los servicios y se mitiga el impacto. p.67

Actualmente existe una metodología para detectar y analizar vulnerabilidades de día cero, esta implica el uso de anzuelos "...la cual consiste en combinar las ventajas de un anzuelo sombra (shadow-honeypot) y una detección de sistemas anómalos, con el fin de prevenir peticiones maliciosas y proteger las aplicaciones"(Guisao y Toro, 2014, p.65)

Guisao y Toro, 2014 también mencionan que :

> Debido a la gran cantidad de ataques, amenazas y vulnerabilidades que enfrenta día a día cada organización, es válido el uso de granjas de servidores y equipos como engaño (honeypots) que presenten vulnerabilidades manejables para validar cada ataque y estar al tanto de las acciones desplegadas; de esta manera los ataques no se concretan en los servidores principales.p.67

1.2 Vulnerabilidades de Aplicaciones Web

Según (Agarwal and Hussain 2018; Bajovic 2017; Jhaveri et al. 2017 citados en González y Montesino, 2018, p.53) "Uno de los principales blancos de ciberataques son las aplicaciones web". "Estas son la base para la informatización de la sociedad moderna. Las organizaciones y personas interactúan fundamentalmente en el ciberespacio a través de aplicaciones web, mediante navegadores, aplicaciones nativas y dispositivos móviles" (Bhandari et al. 2017; Wei and Wolf 2017, citados en González y Montesino, 2018, p.53).

Existen diversas metodologías y guías para la realización de pruebas que permitan revelar en los sistemas de información dando a conocer las vulnerabilidades de las aplicaciones web, una de ella es OWASP top 10.

La Guía de Pruebas de OWASP es la más adecuada para ser tomada como base en una prueba de penetración en aplicaciones web. (OWASP por sus siglas en inglés) es el proyecto abierto de seguridad en aplicaciones web que emite el top 10 de las vulnerabilidades más graves de aplicaciones web. "El objetivo principal es educar a las organizaciones que hacen uso de las TICs sobre las consecuencias de las vulnerabilidades de seguridad en aplicaciones web más importantes"(Landau, 2013, citado en Arias et al. 2015, p.7)

Un mecanismo de seguridad en aplicaciones web es el uso de certificados de seguridad digitales SSL/TSL para establecer un canal cifrado entre el usuario y la aplicación. Segun (Cueva Hurtado y Alvarado Sarango, 2017) concluyeron que:

> Para tener una conexión segura con los certificados digitales SSL/TLS se deben cumplir con ciertas características claves que son: primero utilizar el algoritmo SHA-2 e ignorar algoritmos

> de cifrado obsoletos, segundo la robustez del cifrado no tiene que ser menor a 2048 bits, como tercera característica se tiene que utilizar el certificado estándar X.509, como cuarta característica se debe utilizar las versiones más actuales de los certificados digitales que son SSL/TLS V 1.2. p. 284

En el mercado existen diferentes herramientas para agilizar la revisión y corrección de fallas y vulnerabilidades de las aplicaciones web. La elección de la herramienta adecuada es una tarea importante, ya que su efectividad dependerá de la vulnerabilidad de la aplicación en el entorno de producción. "Estas herramientas de acuerdo con sus capacidades y características pueden ser herramientas de prueba de caja blanca o caja negra" (Muñoz,Armas y Villalba, 2018, p.2).

1.3 Vulnerabilidades Gestores Bases de Datos

La seguridad de las bases de datos es una constante preocupación, muchas veces la seguridad se ve afectada por la configuración de los procesos de conexión. La instalación de un Sistema Gestor de Base de Datos (SGBD) es un procedimiento que requiere configurar un conjunto de parámetros, algunos de ellos sirven para especificar los diferentes procesos que el SGBD utilizará, otros están relacionados con áreas de memoria para realizar las transacciones y soluciones a consultas de las tablas de los modelos de datos y, finalmente, los parámetros requeridos por los procesos de conexiones desde los puntos remotos y locales a la base de datos. (Villalobos Murillo, 2008) Menciona que:

> En la instalación del SGBD, se crean dos usuarios administradores, SYS y SYSTEM, con claves ORACLE y MANAGER, respectivamente. Se recomienda que se cambie la clave una vez realizada la instalación, pero en algunos casos no se hace. El problema es que un atacante con poco conocimiento sobre el SGBD puede instalar herramientas de cliente en su máquina, y lograr descifrar el contenido del archivo de parámetros, así puede intentar conectarse a la base de datos como administrador; si puede acceder el daño sería irreparable, ya que como administrador puede eliminar y cambiar derechos, información y objetos. p.131

2. Sistemas de información ERP

La definición de los sistemas ERP ha tenido una evolución en cuanto a su conceptualización, (Esteves y Pastor en 1999) los definieron como:

> Un sistema compuesto por varios módulos, tales como, recursos humanos, ventas, finanzas y producción, que posibilitan la integración de datos a través de procesos de negocios incrustados. Estos paquetes de software pueden ser configurados para responder a las necesidades específicas de cada organización. (Oltra Badenes, Gil Gómez y Bellver López, 2010,p.65)

En el 2004, Laudon y Laudon, definen a los sistemas de información para la gestión en la empresa de la siguiente manera "sistemas de información que integran los procesos claves del negocio de forma tal que la información pueda fluir libremente entre las diferentes partes de la firma, mejorando con ello la coordinación, la eficiencia y el proceso de toma de decisiones" (Oltra Badenes, Gil Gómez y Bellver López, 2010,p.65). Aberdeen Group, Inc. en el 2004, propone una definición de ERP diferente refiriéndose a un ERP como"la infraestructura de software que, por un lado da soporte a todos los procesos internos de la compañía, y por el otro, apoya a los procesos de negocios externos de la empresa" (Oltra Badenes, Gil Gómez y Bellver López, 2010,p.65)

“Aunque los sistemas ERP se han utilizado y mejorado desde la década de 1970, la tecnología aún está evolucionando y los investigadores aún deben comprender el impacto actual de la implementación del sistema ERP en la alineación organizacional, el aprendizaje, la infraestructura, la subcontratación, la personalización y la ventaja competitiva” (Chung y Snyder, 2004 citado en Mantovani y Iarozinski Neto, 2009, 62). Esto es evidencia de que los modelos organizacionales pueden ayudar a comprender los elementos relevantes en las implementaciones de sistemas ERP y proporcionar mejores estrategias para implementaciones exitosas.

3. Mecanismos y Controles de SI

La gestión de la seguridad se ha convertido en una tarea importante para las empresas debido a que el riesgo tecnológico inicia en el constante incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. La seguridad de la información implica reglamentos y diversas políticas de privacidad y protección de los datos. Según Chang, 2013, “Gestionar la seguridad de la información requiere establecer políticas, medidas de control y de monitoreo al SI” (Solano, García y Bernal, 2016, p.83). Barki y Hartwick, 1989, mencionan que “estos procesos se deben articular a la gestión organizacional mediante actividades de planificación y dirección organizacional de la empresa” (Solano, García y Bernal, 2016, p.83). La ISO 27002, afirma lo siguiente “La implementación de las políticas de seguridad informática deberá suponer la fijación de roles, la coordinación y revisión de procesos técnicos que ayuden a salvaguardar la información”(Solano, García y Bernal, 2016, p.84). Minimizar los riesgos del SI, implica seguimiento, análisis de informes y rendición de cuenta como mecanismos de control.

Según (Montesino, Baluja y Porvén, 2013) “Los controles de seguridad informática a establecer son muchos y muy variados. El estándar ISO/IEC 27001 propone más de 130 controles que están relacionados con aplicaciones, dispositivos tecnológicos, recursos humanos y cuestiones organizativas”p.41 “Los controles de seguridad informática necesitan ser adecuadamente establecidos, implementados, operados, monitorizados, revisados, mantenidos y mejorados; para mantener un sistema de seguridad informática efectivo a lo largo del tiempo” (Montesino, Baluja y Porvén, 2013, p.41). La gran cantidad y variedad de controles que es necesario implementar, en un entorno donde la tecnología evoluciona a una gran velocidad, hace que la gestión de la seguridad informática sea un proceso complejo, en el que hay que lograr una adecuada armonía entre tecnología, personas y procedimientos. (Montesino, Baluja y Porvén, 2013), mencionan que:

> La gestión de la seguridad informática es un proceso complejo que implica el establecimiento de un gran número de controles en un entorno dinámico de múltiples amenazas. Para reducir la complejidad y aumentar la efectividad de la gestión de la seguridad de la información es posible automatizar determinadas acciones y controles. La automatización de controles de seguridad informática implica que la operación, monitorización y la revisión de los mismos se realice de forma automática por herramientas de hardware y software, sin intervención humana en esas acciones. p. 54

3.1 Metodologías Análisis de Riesgo

En este entorno empresarial, creciente y complejo es importante que las empresas tomen conciencia de aplicar continuamente una metodología de análisis de riesgo para garantizar el rendimiento de los sistemas y procesos dentro de la organización. De acuerdo con (Tejena-Macía, 2018, p.232)

> Los ataques a los sistemas informáticos han aumentado, como consecuencia a los avances en los servicios y modelos de comunicaciones e información y el auge de las nuevas Tecnologías de la Información y la Comunicación (TIC), el uso continuo y generalizado a nivel global de la Internet; también se han aumentado los ataques a los sistemas informáticos, lo que ha llevado a las empresas a buscar estrategias que les permitan ejecutar análisis que prevengan, controlen y reduzcan los riesgos asociados a la violación o vulnerabilidad de su información.

El análisis de riesgo a nivel empresarial es una excelente herramienta para generar planes de contingencia y continuidad del negocio, debido a que permite a las empresas mitigar el riesgo y garantizar el rendimiento de los sistemas informáticos.(Tejena-Macía, 2018) menciona que:

> Las metodologías de análisis de riesgos ayuda a las organizaciones a tener un mayor control sobre sus activos, su valor y minimizar las amenazas que pueden impactarlas obligándolas a seleccionar medidas de seguridad que garanticen el éxito de sus procesos y una mayor competitividad en el sector que se desenvuelven. p.240

3.2 Seguridad en Sitios Web

El auge que ha tenido en los últimos años el uso de Internet y la necesidad de transmitir información y realizar transacciones a través de la Web derivó en una serie de amenazas y ataques (phishing, malware, virus, spam, etc.) que comprometen el seguridad de la información y recursos computacionales de clientes y empresas. Debido al aumento significativo de amenazas, ataques y vulnerabilidades que afectan a la Web en los últimos años ha resultado el desarrollo e implementación de herramientas y métodos para garantizar medidas de seguridad en la privacidad, confidencialidad e integridad de los datos de usuarios y negocios. Según (Allen, 2001 citado en Mejia y Ramirez, 2016, p.3) “La seguridad en el sitio web se compone de varios aspectos trabajando en conjunto como lo son el programador, el administrador, la configuración del sitio web y las herramientas utilizadas”.

Seguridad en aplicaciones web están orientadas a satisfacer las necesidades de información transmitida vía web de forma precisa, concisa, oportuna, confidencial y segura, garantizando la protección y privacidad de la información durante el intercambio y transmisión de información entre el cliente y el servidor. Segun (Núñez , Sanjuán y García, 2009, p.80) :

> Las estadísticas sobre seguridad en la Web muestran que es una necesidad inmediata el uso de tecnología que de alguna manera ayude a controlar o minimizar estos ataques y garantizar una mayor seguridad en la protección de los datos confidenciales de los usuarios, para ellos existen muchas herramientas de seguridad en la Web que se utilizan para proteger la información del usuario de posibles ataques de código malicioso como el Teclado Virtual, el CAPTCHA, etc.
>
> El problema que encontramos en la Web en la actualidad es que muchos de estos métodos y herramientas de seguridad que se utilizan para garantizar la protección de la información confidencial en cierto grado brindan seguridad en la transmisión de información, pero es posible que no ofrezcan los niveles adecuados de accesibilidad. a una aplicación puede ser utilizada por cualquier persona independientemente de su navegación y por tanto imposible que cualquier persona con algún tipo de discapacidad permanente o temporal no pueda acceder a los contenidos y servicios disponibles en la Web.

3.3 Políticas de Seguridad

La seguridad informática no implica solamente el crear usuarios y contraseñas, se debe implementar políticas que garanticen la seguridad tanto física como lógica de la información. “Se debe asegurar la privacidad de la información y protegerla tanto de daños no intencionados como deliberados” (Hidalgo, Tupiza y Sánchez, 2016, p.1). Según (Fuertes et al., 2011 citado en Tirado Ríos et al.,2017, p.464):

> La comunidad científica ha investigado e implementado mecanismos que permitan disminuir y mitigar estos ataques de seguridad como hurto, modificación, espionaje, interrupción, falsificación, denegación de servicios, etc., empleando tecnologías de virtualización, cuya aplicación permite disminuir el riesgo a equipos y redes en producción, precautelando la información y servicios de las organizaciones.

Las políticas de seguridad implican normas, reglas, metodologías o protocolos que velan por la seguridad de la información de una organización y se caracterizan por tener tres componentes los cuales son: la prevención, detección y la actuación.

4. Penetration Testing

“Las pruebas de penetración son el método principal utilizado para garantizar que las vulnerabilidades o debilidades en entornos de red, aplicaciones web y locales sean conocidas y puedan abordarse antes de que se exploten en un ataque real” (Tang, 2014, p.8). Las pruebas de penetración pueden abarcar muchas áreas diferentes, que cubren principalmente redes internas y hosts conectados a internet, aplicaciones web, cortafuegos, redes inalámbricas y dispositivos de red. Tang, 2014 menciona que:

> Una prueba de penetración proporciona una prueba probatoria de cualquier debilidad que los ciberdelincuentes podrían explotar y, además, el impacto potencial que una violación exitosa podría causar a una empresa. Ayuda a las empresas a centrarse en los problemas de seguridad clave que tienen en sus sistemas y políticas de seguridad, y a solucionar cualquier problema inseguro.p.8
>
> El pentesting está diseñado para clasificar y determinar los alcances y las repercusiones de los fallos de seguridad, dando resultados para las empresas en cuanto a poder identificar la información o entornos a los cuales se podrían alcanzar en un ataque, además de evaluar la eficiencia de la defensa con la que cuentan. (Panda Security, 2018 citado en Vanegas Romero,2019,p.2)

5. Seguridad en TI

Cada vez hay más gente que se dedica a intentar explotar las vulnerabilidades de las empresas con el fin de sacar beneficios, debido a estas situaciones las empresas cada vez se van tomando conciencia de que la seguridad informática es una de las cosas más importantes de una empresa. Según (Manchado, 2019, p.63)

> Debido a los numerosos ataques, que sobre todo son sufridos por las empresas, éstas muchas veces dejan sus datos más confidenciales en manos de empresas que están expresamente dedicadas a la seguridad de los Sistemas, y otras, recurren a empresas externas solicitando ayuda para mejorar la seguridad de su propio Sistema.

Conclusiones

Los sistemas de planificación de recursos empresariales ERP, son los sistemas que abarcan toda la información de la empresa tanto de sus usuarios como de sus clientes, de allí radica la importancia de que las empresas adopten medidas en aras de proteger su principal activo, la información. En la actualidad cientos de sistemas de información son vulnerados por ciberdelincuentes, quienes se aprovechan de vulnerabilidades existentes y extraen información relevante, que en la mayoría de los casos es utilizada con fines extorsivos o vendidas a competencias directas de las empresas, de allí radica la importancia de que las organizaciones inviertan recursos en aras de salvaguardar los activos de información.

El establecer controles que permitan que la información esté disponible a quienes tienen permiso para acceder a ella, que se mantenga íntegra desde su origen hacia su destino y que sea conocida solo para quien esté dirigida, son estrategias que cualquier empresa u organización hoy en día debe tener implementadas, el uso de Sistemas de Detección de Intrusos - IDS y Sistemas de Prevención de intrusos – IPS, son herramientas que permiten monitorear toda nuestra infraestructura tecnológica y de redes, generando alertas en caso de que personal no autorizado quiera acceder a nuestra información.

Consideramos que el monitoreo constante de cualquier infraestructura tecnológica, ayuda a que las organizaciones detecten y conozcan las vulnerabilidades a las cuales se ve expuesta su información, el realizar pruebas de penetración Pentesting, son buenas estrategias que ayudan a lograr esto. Es fundamental contar con el personal capacitado en cómo hacerles frente a incidentes, al cierre de brechas, al análisis de vulnerabilidades de los sistemas y establecer medidas que permitan la mitigación de cualquier tipo de ataque o pérdida de información.

Referencias

Arévalo-Cordovilla, & Ordoñez-Sigcho. (2020). *Ciencias de la computación Artículo de investigación*. *6*, 835–846.

Arias, M., & Hernández Saucedo, Ana Laura; Mejía Miranda, J. (2015). Implementation of web application for irrigation systems for agriculture. *Revista Electrónica de Computación, Informática Biomédica y Electrónica*, *4*(1). http://www.revistas.ucr.ac.cr/index.php/intersedes/article/view/939%5Cnhttp://www.revistas.ucr.ac.cr/index.php/intersedes/article/download/939/1000

Badenes, R. F. O., Gómez, H. G., & López, R. B. (2011). Factores diferenciales entre los ERP de software libre (FSw ERP) y los ERP propietarios. *Direccion y Organizacion*, *44*(Olson 2009), 64–73.

Cueva Hurtado, M. E., & Alvarado Sarango, D. J. (2017). Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación. *Enfoque UTE*, *8*(1), 273–286. https://doi.org/10.29019/enfoqueute.v8n1.128

González, H. R., & Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. *Revista Cubana de Ciencias Informáticas*, *12*(4), 52–65.

Guisao, J. S., & Toro Rendon, J. C. (2014). *Introducción Metodología para la detección de vulnerabilidades de redes de datos*. 63–67.

Hidalgo Y., J., Tupiza L, D., & Sánchez Almeida, T. (2016). *Políticas de Seguridad de una Red Multiservicios Corporativa, Utilizando Hacking Ético*. *July*. https://doi.org/10.18687/laccei2016.1.1.251

José, B., & Montealegre, R. (2016). *Medición de madurez de CiberSeguridad en MiPymes colombianas*. https://repositorio.unal.edu.co/handle/unal/57956

Mantovani Fontana, R., & Neto, L. (2009). Erp Systems Implementation in Complex Organizations. *JISTEM Journal of Information Systems and Technology Management*, 61–92. https://doi.org/10.4301/s1807-17752009000100004

Miranda, J. M., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *17*, 1–15. https://doi.org/10.17013/risti.17.1-15

Muñoz, F. R., Armas Vega, E. A., & Villalba, L. J. G. (2018). Analyzing the traffic of penetration testing tools with an IDS. *Journal of Supercomputing*, *74*(12), 6454–6469. https://doi.org/10.1007/s11227-016-1920-7

Rafael Hoyos, M., & Ligo, R. (2019). Bisfosfonatos y los Huesos de Cristal. *Journal of Chemical Information and Modeling*, *53*(9), 38–44.

Rocío Tirado Ríos, N., Janeth Ramos Reyes, D., Leuvany Álvarez Morales, E., & Daniel Carreño Sandoya, S. (2017). Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas. *Revista*, *10*, 462–473. https://core.ac.uk/download/pdf/236644851.pdf

Rolando, E., Valdez, N., Martinez, O. S., Fernández, G. G., Aguilar, L. J., Ml, J., & Lovelle, C. (2009). Security Guidelines for the Development of Accessible Web Applications through the implementation of intelligent systems. *International Journal of Interactive Multimedia and Artificial Intelligence*, *1*(2), 79–86.

Solano, O., Pérez, D., & Bernal, J. (2016). El sistema de información y los mecanismos de seguridad informática en la pyme The information system and computer security mechanisms in the SMEs. *Punto de Vista*, *7*, 21.

Tang, A. (2014). A guide to penetration testing. *Network Security*, *2014*(8), 8–11. https://doi.org/10.1016/S1353-4858(14)70079-0

Tejena-Macías, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Vanegas Romero, A. (2019). Pentesting, ¿Por qué es importante para las empresas? *Universidad Piloto de Colombia*, 1–5.

Villalobos, J. (2008). Vulnerabilidad De Sistemas Gestores De Bases De Datos. *Uniciencia Vol. 22*, num 1-2. https://www.redalyc.org/articulo.oa?id=475948929016