SISTEMAS CENTRALIZADOS. PAUTAS PARA LOGRAR UNA CORRECTA SEGURIDAD INFORMÁTICA

CENTRALIZED SYSTEMS. GUIDELINES TO ACHIVE A CORRECT INFORMATIC SECURITY

Yudi Guilarte Garcés. guilartegy@hotmail.com. Universidad de Moa, Holguín. Cuba
ORCID: https//.orcid.org/0000-0003-3572-2858

Fecha de recepción: 30 de abril de 2024

Fecha de aceptación: 30 de mayo de 2024

RESUMEN

Se realizó un estudio que determinó una serie de elementos, conceptos, y consideraciones que constituyen la base para la protección y seguridad informática. Fueron empleados métodos tales como histórico-lógico y el de análisis -síntesis. Estos elementos forman parte del procedimiento para establecer herramientas de seguridad altamente confiables, definir mecanismos y asegurar políticas de prevención que garanticen la seguridad requerida por los sistemas centralizados; permiten aumentar la fiabilidad, simplificar el proceso de búsqueda de datos, mejorar la correlación de directivas, evitar ataques de día cero, reducir el número de falsos positivos, entre otras vulnerabilidades a la que se ven expuestos estos conjuntos.

PALABRAS CLAVES: sistemas centralizados; seguridad informática; vulnerabilidades

ABSTRACT

A study to determine a series of elements, concepts and considerations to the proper protection and safety of information technology was put into practice by means of the use of methods such as: logical-historical and analysis- synthesis. These elements are part of the procedure to establish highly reliable security tools, to define mechanisms ans assure preventive policies to garantee the necessary security of centraliced systems, to simplify data seach, to better up correlation of directives, to

avoid day zero attacks, to reduce the amount of false positive, among other vulnerabilities these sets are exposed to.

KEYWORDS: centraliced systems; cybersecurity; vulnerabilities

INTRODUCCIÓN

La seguridad de un equipo se puede definir como el conjunto de controles que se ponen en marcha para proporcionar confidencialidad, integridad y disponibilidad de todos los componentes (datos, software, hardware y firmware) de un sistema informático Ramírez (2015). Por sistema informático entiéndase un conjunto de elementos (software, hardware, aplicaciones, almacenamiento y comunicación) trabajando interconectados para lograr un objetivo común Berdik et al. (2021, 58). La interconexión de sistemas informáticos puede tornarse difícil debido a incompatibilidades. A veces estas dificultades ocurren a nivel de hardware, mientras que en otras ocasiones se dan entre programas informáticos que no son compatibles entre sí (Vides, 2012).

Por su parte la seguridad informática es la disciplina que con base en políticas y normas internas (externas) de la empresa se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático. Esta información se protege contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos Urbina (2016). En la actualidad la seguridad de los sistemas informáticos ha adquirido gran auge, esto, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles; y es que la posibilidad de interconectarse a través de redes ha abierto nuevos horizontes que permiten explorar más allá de las fronteras de la organización.

Esta situación ha llevado a la aparición de nuevas amenazas en los sistemas computarizados y de información Vogelman (2007). Son precisamente los sistemas de información uno de los componentes más amenazados y relevantes del entorno actual de negocios, ello en parte a que solo estos sistemas ofrecen grandes oportunidades de éxito para las empresas, esto, dado que cuentan con la capacidad

de reunir, procesar, distribuir y compartir datos de manera oportuna e integrada (Abrego et al., 2017).

Se destaca que, de no ser detectadas a tiempo, las amenazas experimentadas por un sistema centralizado causarían daños severos a la información, pudiendo ello influir el futuro de la entidad atacada Gómez F. (2021, 2). Y claro está que, al dañarse pierde valor la información. Al decir valor de la información, se refiere a cuan peligroso es enviar la información grabada en la tarjeta de crédito a través de Internet para hacer una compra en una red gigantesca donde viajan no solo los 16 dígitos de una tarjeta, sino millones de datos, gráficas, vídeos y voz, Vogelman (2007).

Sin lugar a dudas refieren los sistemas centralizados conjuntos bajo constante amenazas y vulnerabilidades. Cuando la centralización se realiza correctamente no sólo se pueden simplificar tareas administrativas, mejorar la seguridad y la gestión de datos, permite ahorrar dinero a un usuario/propietario que busca integridad, privacidad, efectividad y eficiencia de los recursos informáticos que emplea; puede acceder a la información que desea, y hacerlo de manera correcta y oportuna (Gómez, 2022).

La seguridad de los sistemas de información ha crecido en los últimos años en proporción a su extensión e importancia, se convierte en un factor clave en el desarrollo económico y social de las empresas, organizaciones y gobiernos. En la sociedad de la información, los datos se pueden encontrar en todos los ámbitos y en todas partes (Molina, 2015).

Las computadoras son una manera conveniente para recolectarlos y organizarlos; esto aumenta la eficiencia en el tratamiento de dicha información, reduce los costos y mejora en gran medida la calidad de cualquier servicio prestado. Sin embargo, sin un nivel adecuado de seguridad el valor de tales servicios se ve disminuido.

Al desarrollar nuevos sistemas informáticos se especializan de igual manera los hackers para atacarlos, por lo que los administradores deben implementar mecanismos y/o técnicas que permitan asegurar la integridad y evitar la posible pérdida de los datos que se transfieren en el sistema de información entendiéndose

como tal al conjunto de datos y recursos físicos, lógicos y humanos que permiten almacenar y circular la información que contiene (Agé et al., 2011).

En este sentido baste destacar la importancia de implementar adecuadas estrategias de seguridad, ello permitiría no solo minimizar los riesgos físicos (lógicos) a los que está expuesto un equipo (sistema) donde no se han definido controles que proporcionen confidencialidad, integridad y disponibilidad de sus componentes; estrechará la brecha entre la percepción y la realidad (Ramírez, 2015). Sean pues, estas políticas, así como la implementación de adecuadas herramientas de control de riesgos elementos claves de la presente investigación. Se realizó un estudio que determinó una serie de elementos, conceptos, y consideraciones que constituyen la base para la protección y seguridad informática. Los métodos que sustentaron la investigación fueron: histórico-lógico y el de análisis -síntesis, análisis documental. Estos elementos forman parte del procedimiento para establecer herramientas de seguridad altamente confiables, definir mecanismos y asegurar políticas de prevención que garanticen la seguridad requerida por los sistemas centralizados

DESARROLLO

Sistemas centralizados

Los sistemas centralizados de seguridad informática se definen como un conjunto de elementos organizados que cumplen un objetivo esencial en el mundo de la interconexión de las redes; tal objetivo está centrado esencialmente en preservar la información del usuario. Los sistemas centralizados representan aspectos controlables, gestionables y fáciles de manejar, ello, dada su relativa homogeneidad y escasa dispersión geográfica.

Según Padilla (2021), los sistemas centralizados por demás son seguros, pues no deben elegir entre ser consistentes o estar disponibles; De igual modo no resulta difícil capturar el estado global de un sistema centralizado. Las mayores ventajas de un sistema centralizado radican en ser accesible, homogéneo, administrable, y de consistente seguridad

Riesgos, amenazas, y vulnerabilidades a los que está expuesto un sistema centralizado

Una vulnerabilidad en la tecnología de la información es un defecto en el código o diseño que crea un potencial punto de ataque de seguridad por un extremo o red López (2010). Se puede definir también como las debilidades que se presentan en un sistema operativo (de información o software) que permiten a un atacante violar la confidencialidad e integridad de los datos; peor aún, la disponibilidad, control de acceso y consistencia del sistema Abomhara & Køien (2015).

La existencia de las vulnerabilidades da paso a que existan amenazas externas o internas. El proceso de evaluación de amenazas constituye el mayor problema en la protección de los datos o información, porque la fuente de vulnerabilidad y amedrentamiento en un sistema de información puede estar oculta hasta que comienza el ataque, lo que genera controles de seguridad insuficientes que generan un nivel alto de riesgo para la organización (Kamenskih et al., 2020).

Las principales amenazas de seguridad están asociadas a: *Interrupción* (cuando un objeto del sistema se pierde puede suceder que pase a estado de no disponible), *Interceptación* (cuando los usuarios acceden a información no autorizada), y la *Modificación* (cuando personas no autorizadas realizan cambios y no presentan los registros en la base de datos; por tanto, para minimizar la disponibilidad de amenazas y vulnerabilidades en las organizaciones, es necesario que realicen una adecuada evaluación de riesgos y establezcan controles para la configuración de procesos; también equipos hardware, aplicaciones y sistemas operativos. Esta evaluación debe ser realizada por un profesional en seguridad, y es que solo las vulnerabilidades a las que suelen estar expuestos los sistemas (computación o información) pueden perjudicar un activo o un control de proceso.

Un adecuado análisis de riesgo en un sistema centralizado requiere entender cuáles recursos de la red se necesitan proteger, de quién y cómo podemos protegerlo Vogelman (2007). Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo, pues, no todos son vulnerables a las mismas

amenazas. Entre las vulnerabilidades más comunes a las que se exponen estos sistemas están:

- ✓ Negación de servicio
- ✓ Cracking de passwords
- ✓ e-mail bombing (spamming)
- ✓ Bypass de dispositivos

Ataques a los que está expuesto un sistema centralizado

Un ataque informático consiste en aprovechar alguna debilidad en el software, en el hardware, o incluso en los usuarios que forman parte del sistema provocando un efecto negativo en la seguridad de los mismos que posteriormente afectará a los activos de la organización Mieres (2009). Existen ataques informáticos que amenazan la seguridad a los sistemas cuya funcionalidad es el intercambio de información, es decir, cuando existe una comunicación desde el emisor hacia el receptor a través de una red de comunicación.

En este sentido, los ataques pueden ser categorizados de la siguiente manera: interrupción, intercepción, modificación y fabricación (Maciá, 2007). Una forma de clasificar los ataques informáticos según X.800 del RFC 2828 son ataques activos y ataques pasivos. Los ataques activos implican una modificación al flujo de los datos o la creación de flujos falsos, mientras que los ataques pasivos son conexiones para monitorear e interceptar la transmisión de los datos.

Uno de los ataques activos de interrupción es la Denegación de Servicio (DoS) que es un intento por parte de un atacante para agotar los recursos disponibles de la red, impidiendo a los usuarios el acceso a la aplicación o servicio US-CERT (1997). Una variante de este tipo son los ataques distribuidos de denegación de Servicio (DDoS) los mismos que tiene lugar cuando muchos equipos están infectados en forma simultánea por el código malicioso y se coordinan bajo el control de un solo atacante con el fin de establecer comunicaciones hacia los servicios que ofrece el sistema de la víctima.

A continuación, se muestra una lista de los tipos más comunes de ataque:

- ✓ Desbordamiento del buffer
- ✓ Codigo shell
- ✓ Puerta tresera
- ✓ Escaneo de puertos
- ✓ Sniffing
- ✓ Keylogging
- ✓ Supplantation de identidad
- ✓ Troyanos
- ✓ Denegación de servicios

Sistemas centralizados. Recursos que deben ser protegidos ante una amenaza a la seguridad

Toda estrategia de seguridad en su composición debe lograr altos niveles de:

Hardware: es la parte física o tangible del equipo, como la tarjeta de memoria del sistema, la unidad de disco, procesadores, teclados, terminales, computadoras personales, impresoras, unidades de disco, cableado de la red, routers, bridges, entre otros.

Firmware: es el software permanente que ejecuta los procesos de la computadora y es en su mayoría invisible al usuario, como las funciones de puesta en marcha que hacen que los elementos del hardware funcionen juntos.

Software: es la programación que ofrece servicios al usuario y al administrador. El sistema operativo, el procesador de textos, programas fuente, programas objeto, programas de diagnóstico, los juegos de ordenador y el navegador de Internet son ejemplos de softwares que se encuentran comúnmente en un ordenador.

Datos: en ejecución, almacenados en línea, archivados fuera de línea, back -up, bases de datos, en tránsito sobre medios de comunicación.

Personas: personal encargado de operar los sistemas.

Documentación: documentos sobre programas, hardware, sistemas, y procedimientos administrativos locales.

Accesorios: hace referencia al papel, los formularios, las cintas, y la información grabada en el computador.

Niveles a considerar para lograr una adecuada seguridad

Para lograr una adecuada seguridad informática es necesario que todo sistema cumpla con los siguientes principios.

Efectividad. Procura lograr que la información requerida para desarrollar cualquier tarea en la empresa sea adecuada y necesaria; proporcionándola de manera accesible, oportuna, correcta, y consistente.

Eficiencia. Sugiere que, la información sea generada y procesada utilizando de manera óptima los recursos que tiene la empresa destinados a este fin.

Confidencialidad. Se define como la propiedad de la información que busca asegurar que la misma es accedida únicamente por el personal autorizado.

Integridad. Busca proteger la información contra la modificación sin el permiso del dueño. La información a ser protegida, incluye no sólo la que está almacenada directamente en los sistemas de cómputo, sino, que también se deben considerar elementos menos obvios como respaldos, documentación, registros de contabilidad del sistema, tránsito en una red, etc.

Autenticidad. Garantiza que quien dice ser "X ", sea realmente "X " y no "Y".

No repudio. Ni el origen ni el destino en un mensaje deben poder negar la transmisión, o lo que es lo mismo, quien envía el mensaje puede probar que, en efecto, su mensaje fue enviado y viceversa.

Disponibilidad de los recursos. Se refiere al acceso oportuno por parte del usuario a la información que se encuentra en el Sistema. La disponibilidad también se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de algún problema.

Control de acceso a los recursos. Consiste en controlar quién utiliza el sistema o cualquiera de los recursos que este ofrece y cómo lo hace.

Consistencia. Asegura que el sistema siempre se comporte de la forma esperada.

Auditoría. Abarca los mecanismos para poder determinar qué es lo que sucede en el sistema, esto es, qué hace cada usuario y los tiempos y fechas de dichas acciones.

Una correcta gestión de la seguridad debe buscar, establecer (mantener) programas, controles y políticas que tengan como finalidad conservar la confidencialidad integridad y disponibilidad de la información, si alguna de estas características falla no se está ante nada seguro (Galindo et al., 2016).

Al tiempo de garantizar una adecuada seguridad informática es indispensable implementar políticas basadas en metodologías de seguridad (entiéndase Coras, Octave, Ebios, NIST SP 800:30, Magerit, Cramm, entre otras) capaces de determinar, analizar, evaluar y clasificar los riesgos, pudiendo así evitar ataques que pongan en riesgo la información (Llerena et al., 2020).

Una adecuada política de seguridad interna requiere de una oportuna descripción de los recursos que se desean proteger. Esta política debe orientar acerca de las decisiones que se adoptan en relación con la seguridad, ofrecer explicaciones comprensibles acerca de las mismas, al crear expectativas en la organización; todo ello debe ser abordado con un lenguaje común, libre de tecnicismos y términos legales que impidan una clara comprensión de las políticas; solo entonces conseguirán implantarse.

Es así que, las políticas de seguridad interna deben responder a intereses y necesidades organizacionales que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos, y a reconocer en los mecanismos de seguridad informática factores que facilitan la normalización y materialización de los compromisos adquiridos con dicha organización. Deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales tales como: crecimiento (rotación)

de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios.

Mecanismos de seguridad

- ✓ Mecanismos de prevención: Son los que duplican la seguridad cuando se realiza una tarea para prevenir el robo de información. Ejemplo: El uso de cifrado en la trasmisión de datos porque evita que un atacante escuche las conexiones de un sistema de red Gutiérrez et al. (2018).
- ✓ Mecanismo de detección: Permite detectar a tiempo las vulnerabilidades de seguridad que se puedan presentar: Ejemplo: El programa de auditoría de Cadavid, 2018.
- ✓ Mecanismos de recuperación: Son aquellos que se utilizan cuando sufren violación en el sistema donde se logra detectar que está surgiendo un problema. Ejemplo: Cuando se implementan las copias de seguridad o el uso de hardware adicional (Patiño et al., 2017).

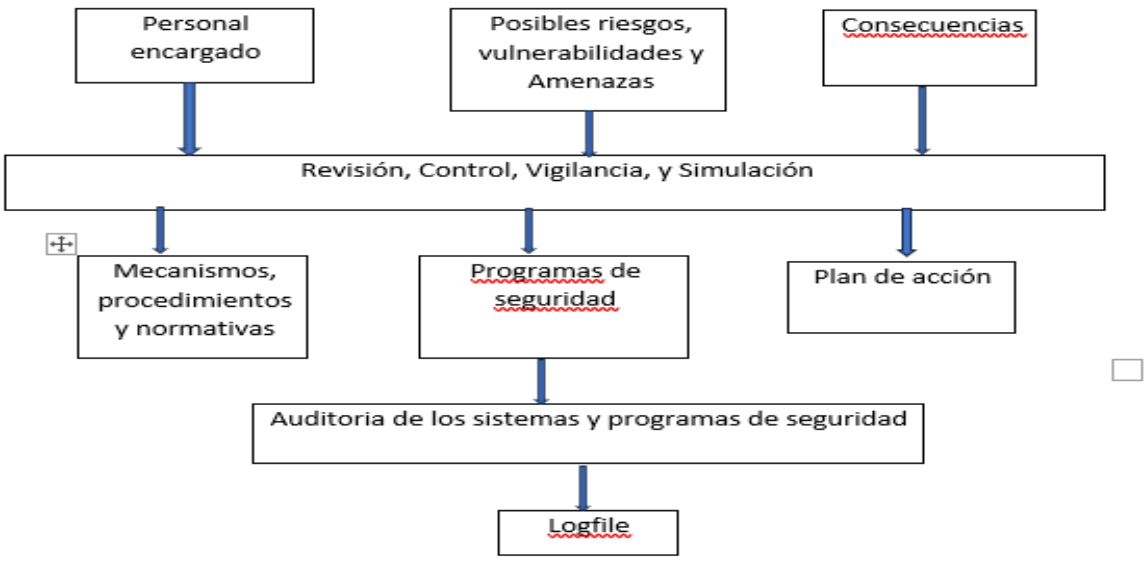

Fig. 1. Diagrama para el análisis de un sistema de seguridad (Adaptado de Vogelman M. 2007)

Los criterios de seguridad establecidos simplifican el proceso de búsqueda de datos y mejora la seguridad informática de millones de usuarios que cada día se conectan a redes ofrecidas por universidades, aeropuertos, cafeterías, hoteles y empresas que

carecen de la seguridad, con una herramienta adecuada de control de riesgos aumenta la correlación de directivas, evita los ataques de día cero y otras vulnerabilidades aprovechadas por miles de predadores informáticos (Hackers) que cada vez desarrollan nuevas técnicas; adecuadas políticas de seguridad elevan la confidencialidad, integridad y disponibilidad de la información administrada por actores (especialistas de seguridad, administradores de red, entre otros) en su mayoría escasamente preparado en el manejo de herramientas con elevados requisitos de software/hardware.

CONCLUSIONES

Para garantizar una seguridad informática adecuada en entornos centralizados es esencial establecer políticas de acceso estrictas, mantener todos los sistemas y softwares actualizados; además, es crucial realizar copias de seguridad regulares de los datos y almacenarlas en ubicaciones seguras. Finalmente, es fundamental educar a los empleados sobre las mejores prácticas de seguridad y cómo identificar posibles amenazas para crear una cultura de seguridad y protección.

REFERENCIAS BIBLIOGRÁFICAS

Abomhara, M. & Køien, G. (2015) *Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks.* J. Cyber Secur. https://doi.org/10.13052/jcsm2245-1439.414.

Abrego, A.; Sánchez, T. & Medina, Quintero (2017). *Influencia de los sistemas de información en los resultados organizacionales*. Contaduría y Administración. p. 303–320. https://doi.org/10.1016/j.cya.2016.07.005

A*gé*, M.; Baudru, S.; Crocfer, R., Ebel, F.; Hennecart, J.; Lasson, S. & PUCHE, D. (2011). *Seguridad Informática*, Ethical Hacking, Ediciones ENI. ISBN: 978-2-7460-6811-7. p. 17.

Berdik, D., Otoum, S., Schmidt, N., Porter, D. & Jararweh, Y. (2021). A *Survey on Blockchain for Information Systems Management and Security* [online]. Information Processing & Management, 58(1), 102397. https://doi.org/10.1016/j.ipm.2020.10239

Cadavid, R. (2018). *Hallazgos de vulnerabilidades en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías SAS.* Universidad nacional abierta y a distancia, Guadalajara de Buga (Colombia). https://repository.unad.edu.co/bitstream/handle/10596/17412/94477303.pdf?sequence

Galindo, C.; Mena, A.; santizo, W.; Mendoza, S & García, M. (2016). *Seguridad de la Información*. Guatemala. Editorial Universidad de San Carlos de Guatemala (Guatemala).

Gómez, F.; Colon, E.; Bermeo; Xavier, Oscar; (2022). *Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim*. Ecuadorian Science Journal (Ecuador). p 1-9. ISSN-e: 2602-8077 https://journals.gdeon.org/index.php/esj/article/view/181

Gutiérrez, G. (2018). Gestión de seguridad de la información en las organizaciones. Investigación e Innovación [en línea]. https://www.researchgate.net/publication/343167096

Kamenskih, A; (2020): *The Development of Method for Evaluation of Information Security Threats in Critical Systems*. Proc. 2020 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. EIConRus 2020. 333–336. https://doi.org/10.1109/EIConRus49466.2020.9038960

Llerena, I.; Barcia, Ayala & Ayala Carabajo (2020): Faculty Training through Crowdlearning for Emerging Online Education [online]. IEEE ANDESCON. https://doi.org/10.1109/ANDESCON50619.2020.9272103

López, P. A. (2010). *Seguridad informática*. Editex. ISBN: 139788497716574.

Maciá, G. (2007). *Ataques de Denegación de Servicio a Baja Tasa contra Servidores*, Tesis Doctoral, Departamento de Teoría de la Señal, Telemática y Comunicaciones, Universidad de Granada (España) https://digibug.ugr.es/bitstream/handle/10481/1543/16714763.pdf?

Mieres, J. (2009) *Ataques Informáticos. Debilidades de seguridad comúnmente explotada.* https://www.evilfingers.com/publications/white_AR/01

Molina, Lorena; Furfaro, Angelo; Malena, Giovanna & Parise Andrea (2015). *Ataques Distribuidos de Denegación de Servicios: modelación y simulación con eventos discretos. Universidad Nacional de Chimborazo (Ecuador)* https://www.researchgate.net/publication/280877593

Padilla, V.; (2021). *Introducción Sistemas Distribuidos.* Universidad Nacional Experimental de Guayana (Guyana) [en línea]. https://moodle.uneg.edu.ve/pluginfile.php/34236/mod_page/content/52/Introduccion.pdf

Patiño, S.; *(2017). Evaluación de seguridad informática basada en ICREA e ISO27001. Universidad Ciencia y Tecnología (Ecuador) [en linea].* https://www.researchgate.net/publication/325191433

R*amírez,* F. (2015). *¿Podremos alcanzar la seguridad informática?* https://www.estamosenlinea.com.ve/2015/04/01/podremos-alcanzar-la-seguridad-informatica

Urbina, G. B. (2016). *Introducción a la seguridad informática*. Grupo editorial PATRIA

V*ides*, Marta Susana (2012). *Diseño e implementación de un sistema centralizado de reportes en un centro de soporte operativo para una empresa comercializadora de combustible.* Tesis de grado (Magister en Administración Industrial y de Empresas de Servicios), Ciudad de Guatemala (Guatemala).

Villacís, G. & Morocho, R. (2017). *Vulnerabilidades y amenazas a los servicios web de la intranet de la universidad técnica de Babahoyo*. 3c Tecnología: glosas de innovación aplicadas a la pyme. p. 53-66. Universidad técnica de Babahoyo (Ecuador).

Vogelman M., Estela Evangelina (2007). Seguridad de sistemas distribuidos. Trabajo de Adscripción, Georgetown (Guyana).