Journal **TechInnovation**
Volumen 2, Número 2, 2023
Universidad Estatal del Sur de Manabí
ISSN-e: 2953-6472

ARTÍCULO ORIGINAL

Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001

Data vulnerability in information systems based on ISO 27001

https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

Recibido: 11-08-2023 **Aceptado:** 11-10-2023 **Publicado:** 01-12-2023

Geanfrank Isaias Cruz Lucas[1*]
https://orcid.org/0000-0002-0881-6499

Evelyn Lissette Figueroa Rodríguez[2]
https://orcid.org/0000-0001-9216-6718

Nathaly Isabel Cruz Lucas[3]
https://orcid.org/0009-0002-7096-9936

Wagner Manuel Abad Parrales[4]
https://orcid.org/0000-0002-6094-6813

1. Ingeniero en formación Carrera de Tecnologías de la Información Facultad Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
2. Ingeniero en formación Carrera de Tecnologías de la Información Facultad Ciencias Técnicas; Universidad Estatal del Sur de Manabí Jipijapa, Ecuador.
3. Ingeniero en formación Carrera de Economía Facultad Ciencias Sociales, Derecho y Bienestar; Universidad Laica Eloy Alfaro de Manabí; Jipijapa, Ecuador.
4. Ingeniero en Computación y Redes; Docente de la Carrera Tecnologías de la Información Facultad Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa; Ecuador.

Volumen: 2
Número: 2
Año: 2023
Paginación: 54-59
URL: https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/52
***Correspondencia autor:** cruz-geanfranko339@unesum.edu.ec;

RESUMEN

La norma ISO 27001 es un estándar internacional para la gestión de la seguridad de la información (SI). Establece un marco para implementar, mantener y mejorar la seguridad de la información en una organización. La vulnerabilidad de datos se refiere a las debilidades o brechas en el sistema de información que pueden ser explotadas por un atacante con el fin de acceder, modificar o destruir información confidencial. La norma ISO 27001 establece un proceso de gestión de seguridad de la información que incluye la identificación de vulnerabilidades de seguridad, la evaluación de riesgos, la implementación de medidas de seguridad y la monitorización continua para detectar y corregir problemas. Uno de los principales objetivos de la norma ISO 27001 es garantizar la confidencialidad, integridad y disponibilidad de los datos de la organización. Para ello, se requiere la implementación de medidas de seguridad adecuadas, tales como la grabación de datos, la autenticación y autorización de usuarios, la protección contra malware, la protección de redes y la gestión de incidentes. Además, la norma ISO 27001 también establece requisitos para la gestión de incidentes de seguridad, incluyendo la detección, el análisis y la respuesta a incidentes. Esto es esencial para garantizar que se puedan tomar medidas rápidas y efectivas en caso de una brecha de seguridad. En resumen, la vulnerabilidad de datos en los sistemas de información es un problema importante que la norma ISO 27001 aborda mediante un enfoque integral para la gestión de la seguridad de la información.

Palabras clave: amenaza; malware; vulnerabilidad; virus.

ABSTRACT

ISO 27001 is an international standard for information security (IS) management. Establishes a framework for implementing, maintaining, and improving information security in an organization. Data vulnerability refers to weaknesses or gaps in the information system that can be exploited by an attacker in order to access, modify, or destroy confidential information. The ISO 27001 standard establishes an information security management process that includes the identification of security vulnerabilities, risk assessment, implementation of security measures and continuous monitoring to detect and correct problems. One of the main objectives of the ISO 27001 standard is to guarantee the confidentiality, integrity and availability of the organization's data. For this, the implementation of adequate security measures is required, such as data recording, user authentication and authorization, protection against malware, network protection and incident management. In addition, ISO 27001 also establishes requirements for security incident management, including incident detection, analysis, and response. This is essential to ensure that quick and effective action can be taken in the event of a security breach. In summary, data vulnerability in information systems is a major problem that ISO 27001 addresses through a comprehensive approach to information security management.

Keywords: malware; threats; vulnerability; virus.

Introducción

La seguridad de la información es esencial en un mundo cada vez más digital, donde la información es valiosa y su pérdida o robo puede tener consecuencias graves para individuos, empresas y organizaciones gubernamentales. La norma ISO 27001 es un estándar internacional para la gestión de la seguridad de la información que proporciona un marco para la implementación de medidas de seguridad en un sistema de información (Kitsios et al., 2023). Esta norma se enfoca en la gestión de riesgos y la protección de datos, ayudando a garantizar la seguridad de los datos y la confidencialidad, integridad y disponibilidad de la información.

La vulnerabilidad de la seguridad informática se trata de una debilidad o fallo en un sistema de información que abre la puerta para que un atacante o situación no prevista pueda comprometer la integridad, disponibilidad o confidencialidad de los datos.

La página web Isbel (2021), nos dice que las vulnerabilidades tienen diferentes orígenes, como errores de configuración, fallas en el diseño o en procedimientos. Una amenaza es una acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Las principales vulnerabilidades que pueden presentar los sistemas pueden ser de tipo hardware, software, de redes o humanas, las cuales es importante tenerlas en cuenta y monitorearlas con frecuencia para evitar poner en peligro los datos almacenados allí y prevenir amenazas o ciberataques que pueden afectar no solo la operatividad de alguna empresa y organización , sino también su economía, reputación e incluso, su continuidad (Jiménez, 2022).

Por tal razón se puede decir que la vulnerabilidad de los datos se refiere a la posibilidad de que un sistema de información sufra un ataque o una brecha de seguridad, lo que podría resultar en la pérdida, robo o exposición no autorizada de información confidencial.

Desarrollo

La vulnerabilidad de los datos, la norma ISO 27001 establece un enfoque en la gestión de riesgos para la seguridad de la información (Culot et al., 2021). Esto incluye la identificación y evaluación de los riesgos para la confidencialidad, integridad y disponibilidad de la información, así como la implementación de medidas de seguridad para mitigar esos riesgos.

Una de las principales herramientas para la identificación y mitigación de vulnerabilidades de seguridad en un sistema de información es el análisis de riesgos, el cual es un proceso continuo de evaluación y mejora de la seguridad. A través de este proceso, las organizaciones pueden identificar las vulnerabilidades en sus sistemas e implementar medidas para mitigar esos riesgos.

Además, la norma ISO 27001 también establece la necesidad de un plan de continuidad del negocio (BCP) y un plan de gestión de incidentes (IRP) para garantizar que las organizaciones estén preparadas para hacer frente a incidentes de seguridad y minimizar su impacto. Estos planes deben incluir procedimientos para detectar, responder y recuperarse de incidentes de seguridad, incluyendo la protección y recuperación de datos.

La vulnerabilidad de los datos. - es una debilidad en la seguridad de los sistemas informáticos que permite a los atacantes acceder, modificar o destruir información almacenada o transmitida de forma no autorizada. Puede ser causada por una variedad de factores como fallos en el diseño del software, configuraciones inadecuadas, errores humanos o ataques cibernéticos. Es importante que las organizaciones identifiquen y mitiguen las vulnerabilidades de seguridad en sus sistemas para proteger los datos y prevenir incidentes de seguridad (Poma & Vargas, 2019).

¿Qué es la norma ISO 27001?

Es un estándar internacional para la gestión de la seguridad de la información (ISMS) que proporciona un marco para proteger la confidencialidad, integridad y disponibilidad de la información en una organización (ISOTools Excellence Colombia, 2023). Establece los requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) mediante la identificación y mitigación de riesgos, implementación de medidas de seguridad y manejo de incidentes. La implementación es voluntaria, pero puede ser útil para cumplir con regulaciones y aumentar la confianza de los clientes y accionistas en cuanto a la seguridad de los datos.

Los ataques cibernéticos son cada vez más comunes y sofisticados, y pueden tener consecuencias graves para las organizaciones que son víctimas de ellos. Por ejemplo, una brecha de seguridad puede resultar en la exposición de información personal, lo que podría tener consecuencias legales y financieras para la organización. Además, una brecha de seguridad puede dañar la reputación de una empresa y perder la confianza de los clientes (Bello, 2019).

La norma ISO 27001 proporciona una guía para identificar y mitigar estas vulnerabilidades. En primer lugar, la norma establece un marco para la gestión de riesgos, que incluye la identificación de los riesgos, la evaluación de la probabilidad y el impacto de estos riesgos, y la implementación de medidas para mitigar o eliminar estos riesgos (Cruz Lucas, Delgado Tejena, et al., 2022). En segundo lugar, la norma establece un marco para la protección de datos, que incluye la implementación de medidas de seguridad física y lógica, la gestión de acceso a la información y la gestión de incidentes de seguridad.

La implementación de la norma ISO 27001 también requiere un enfoque sistemático y continuo para la mejora de la seguridad de la información. Esto incluye la revisión regular de las políticas y procedimientos de seguridad, la realización de pruebas de penetración y la formación continua de los empleados en temas de seguridad de la información.

Además de ayudar a garantizar la seguridad de los datos, la implementación de la norma ISO 27001.

Metodología

La presente investigación cuenta con tres métodos principales como lo son: el análisis-síntesis, bibliográfico-documental e histórico-lógico.

El método análisis-síntesis, se aplicó mediante la identificación y evaluación de riesgos, la síntesis de las principales vulnerabilidades y la propuesta de medidas para mitigarlas, y la evaluación continua del plan implementado.

El método bibliográfico-documental se utilizó en la recopilación, selección, lectura, anotación, organización y elaboración de un informe a partir de fuentes relevantes y actuales.

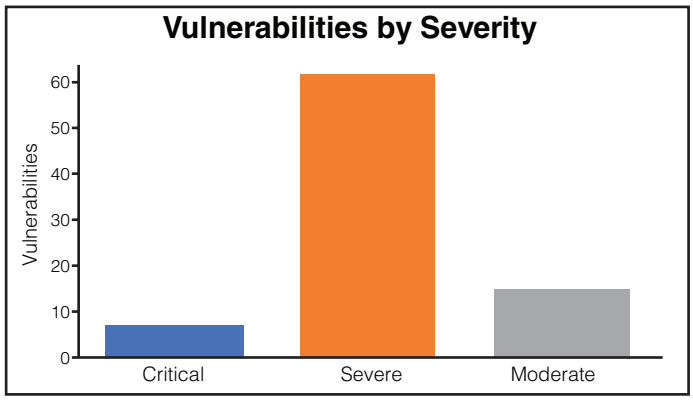
El método histórico-lógico permitió investigar la historia de la norma ISO 27001 y cómo ha evolucionado a lo largo del tiempo, como se aborda las vulnerabilidades de datos, como se realiza la identificación de errores, todo en conjunto para de esta manera proponer posibles soluciones para mejorar la seguridad de la información en relación a la norma ISO 27001.

Resultados

En el estudio realizado por la autora Bonilla (2017) muestra un análisis de las vulnerabilidades de base de datos y las incidencias en la seguridad de la información de la Empresa Automekano Cía. Ltda., de la Ciudad de Ambato. Y nos dice que representa una auditoría de seguridad realizada por NeXpose de Rapid7, la misma que revela que no hay suficientes datos históricos para

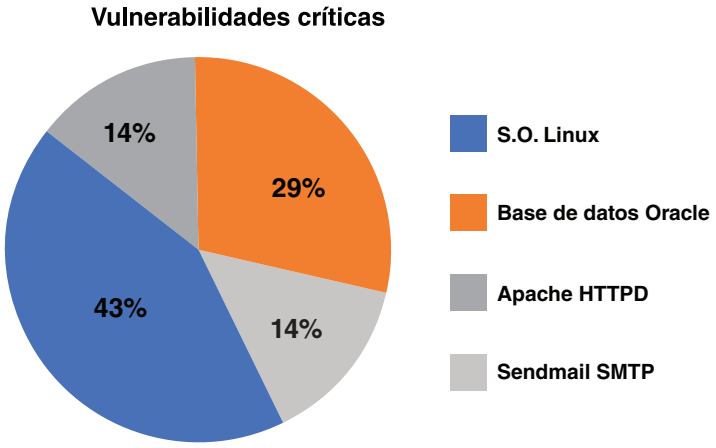
mostrar la tendencia de riesgo puesto que la auditoría se llevó a cabo en un sistema que se encuentra activo.

Figura 1. Vulnerabilidades encontradas



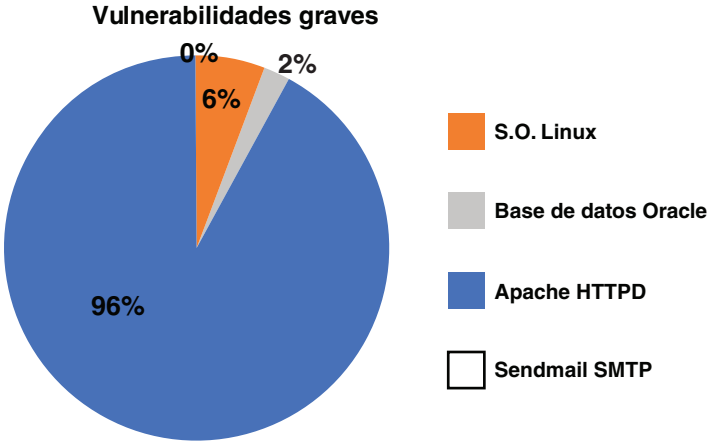
Existen 83 vulnerabilidades encontradas durante la exploración las mismas que se detallan a continuación:

Figura 2. Vulnerabilidades críticas



7 resultaron vulnerabilidades críticas: Las vulnerabilidades críticas requieren inmediata atención, estas hacen que sea relativamente fácil para los atacantes explotar una vulnerabilidad crítica y pueden proporcionarles el control total de los sistemas afectados.

Figura 3. Vulnerabilidades graves



61 vulnerabilidades fueron graves: Las vulnerabilidades graves son a menudo más difíciles de explotar y no pueden proporcionar el mismo acceso a los sistemas afectados.

17 vulnerabilidades moderadas descubiertas: Estas a menudo proporcionan información a los atacantes que pueden ayudar en el montaje ataques posteriores en la red (Cruz Lucas, Galarza Espinoza, et al., 2022).

Las vulnerabilidades críticas y graves fueron tratadas en la presente investigación, a pesar de que las vulnerabilidades moderadas también pudieron averse fijarse de manera oportuna, pero no fueron urgente en ese momento como las otras vulnerabilidades; ya que eran vulnerabilidades que los posibles atacantes podían realizar posterior a la red de comunicaciones (Bonilla, 2017).

Conclusiones

En conclusión, la norma ISO 27001 es un marco importante para la gestión de la seguridad de la información que ayuda a las organizaciones a reducir la vulnerabilidad de los datos en los sistemas de información. La implementación de esta norma proporciona una metodología para identificar y mitigar los riesgos de seguridad, proteger los datos, manejar incidentes de seguridad y mejorar continuamente la seguridad de la información. Además, ayuda a cumplir con regulaciones y requisitos legales relacionados con la seguridad de la información. Por lo tanto, es esencial que las organizaciones consideren la implementación de la norma ISO 27001 como parte de su estrategia de seguridad de la información.

Bibliografía

Bello, E. (29 de Noviembre de 2019). IEBS. https://www.iebschool.com/blog/ciberseguridad-ataques-tecnologia/

Bonilla, C. A. (2017). Elaboración de una metodología de detección y mitigación de vulnerabilidades de base de datos y su incidencia en la seguridad de la información de la empresa Automekano cía. Ltda., de la ciudad de Ambato. Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Dirección de Posgrado. Maestría en Gestión de Bases de Datos II Versión. Retrieved 17 de Diciembre de 2022, from http://repositorio.uta.edu.ec/bitstream/123456789/24534/1/Tesis_t1200mbd.pdf

Cruz Lucas, G. I., Delgado Tejena, L. E., Ponce Solorzano, B. R., & Marcillo Merino, M. J. (2022). Riesgos de seguridad de los datos en la web. Journal TechInnovation, 1(2). https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.43-49

Cruz Lucas, G. I., Galarza Espinoza, R. E., Delgado De La Cruz, R. S., & Marcillo Merino, M. J. (2022). Aplicación de protocolos SSL y TSL para él envió de información. Journal TechInnovation, 1(2). https://doi.org/10.47230/journal.techinnovation.v1.n2.2022.4-9

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In TQM Journal (Vol. 33, Issue 7). https://doi.org/10.1108/TQM-09-2020-0202

isbel. (5 de Septiembre de 2021). Seguridad de la información, vulnerabilidades y riesgos: algunas definiciones. Retrieved 17 de Diciembre de 2022, from https://isbel.com/seguridad-de-la-informacion-vulnerabilidades-riesgos/

Jiménez, M. M. (03 de Abril de 2022). Operani. Retrieved 17 de Diciembre de 2022, from https://www.piranirisk.com/es/blog/vulnerabilidades-en-seguridad-de-la-informacion

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability (Switzerland), 15(7). https://doi.org/10.3390/su15075828

ISOTools Excellence Colombia. (27 de Enero de 2023). Plataforma tecnológica para la gestión de la excelencia. https://co.isotools.us/plataforma-tecnologica-para-la-gestion-de-los-centros/

Poma, A., & Vargas, R. (2019). Problematic in cybersecurity as protection of computer system and social networks in Peru and the World. SCIÉNDO, 22(4). https://doi.org/10.17268/sciendo.2019.034

Cómo citar: Cruz Lucas, G. I., Figueroa Rodríguez, E. L., Cruz Lucas, N. I., & Abad Parrales, W. M. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. Journal TechInnovation, 2(2), 54–59. Recuperado a partir de https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/52