VULNERABILIDAD EN PLATAFORMAS VIRTUALES Y REDES SOCIALES EN ESTUDIANTES DE EDUCACIÓN MEDIA DEL MUNICIPIO DE PASTO: ESTUDIO DE CASO INSTITUCIÓN EDUCATIVA MUNICIPAL CIUDAD DE PASTO AÑO 2023.

(Resúmen Analítico)

VULNERABILITY IN VIRTUAL PLATFORMS AND SOCIAL NETWORKS IN MIDDLE EDUCATION STUDENTS OF THE MUNICIPALITY OF PASTO: CASE STUDY MUNICIPAL EDUCATIONAL INSTITUTION CITY OF PASTO YEAR 2023.

(Analytical Summary)

Autores (*Authors*): BRAVO ROSERO Camilo Andrés
MARTÍNEZ DELGADO David Sebastián
Facultad (*Faculty*): de INGENIERÍA
Programa (*Program*): INGENIERÍA DE SISTEMAS
Asesor (*Support*): PHD. JOSE JAVIER VILLALBA ROMERO
Fecha de terminación del estudio (*End of the research*): JULIO 2024
Modalidad de Investigación (*Kind of research*): Trabajo de Grado

PALABRAS CLAVE

VULNERABILIDAD, MAGERIT, AMENAZA, EDUCACIÓN, CIBERBULLYING, CIBERSEGURIDAD, REDES SOCIALES, INSTITUCIÓN, VIRTUALIDAD.

KEY WORDS

VULNERABILITY, MAGERIT, THREAT, EDUCATION, CYBERBULLYING, CYBERSECURITY, SOCIAL NETWORKS, INSTITUTION, VIRTUALITY.

RESUMEN:

Durante y después de la pandemia Covid 19, se evidenció que el cambio brusco de la modalidad de estudio en las instituciones de la presencialidad a la virtualidad, causó un gran impacto en la educación, los docentes y sobre todo en los estudiantes. Teniendo en cuenta lo anterior la presente investigación se enfoca en determinar, analizar, y contrarrestar la vulnerabilidad a la que pueden estar sometidos los jóvenes al tener total accesibilidad al internet y sobre todo, dentro de éste el acceso ilimitado a las redes sociales, mismas que según la encuesta que realizamos en el año 2023 en la I.E.M. Ciudad de Pasto, con el uso de MAGERIT que es la metodología de seguridad utilizada para conocer los riesgos a

los que se enfrenta un sistema y la norma internacional ISO/TEC 27001 que describe como gestionar la seguridad de la información en una organización, logramos determinar que las redes sociales son las principales causantes de que los jóvenes sean víctimas de ciberdelitos como: ciberbullying, vishing, phishing, ciberacoso, suplantación de identidad, hackeo, entre otros. Una vez recolectada esta información buscamos posibles soluciones aplicables a la comunidad educativa, permitiendo que el plan que organizamos subsane los vacíos que encontramos se presentaban en las salas de informática de la institución, la falta de capacitación de parte de los docentes a los alumnos para evitar ser víctima de estos delitos, que coloquen en riesgo su salud psicológica e incluso física y el rendimiento en las actividades escolares.

***ABSTRACT*:**

During and after the Covid 19 pandemic, it was evident that the abrupt change in the study modality in institutions from in-person to virtuality caused a great impact on education, teachers and, above all, students. Taking into account the above, this research focuses on determining, analyzing, and counteracting the vulnerability to which young people may be subjected by having full accessibility to the Internet and, above all, within it, unlimited access to social networks, which according to the survey we carried out in 2023 at the I.E.M. Ciudad de Pasto, with the use of MAGERIT, which is the security methodology used to know the risks faced by a system, and the international standard ISO/TEC 27001, which describes how to manage information security in an organization, we were able to determine that social networks are the main causes of young people being victims of cybercrimes such as: cyberbullying, vishing, phishing, cyberbullying, identity theft, hacking, among others. Once this information has been collected, we look for possible solutions applicable to the educational community, allowing the plan we organized to remedy the gaps that we found in the institution's computer rooms, the lack of training on the part of the teachers for the students to avoid being a victim of these crimes, which put their psychological and even physical health and performance in school activities at risk.

CONCLUSIONES:

La Institución Educativa Municipal Ciudad de Pasto cuenta con un sistema de gestión bien estructurado dividido en áreas directiva, académica, administrativa-financiera y comunitaria, cada una con procesos definidos para asegurar un funcionamiento eficiente y un ambiente educativo óptimo. El manejo de la información ha sido un pilar fundamental para la IEM, por lo que se hizo necesario evaluar las amenazas y vulnerabilidades que pudieran afectar su infraestructura tecnológica.

Encontramos que la I.E.M. Ciudad de Pasto posee una variedad de activos informáticos que incluyen equipos de hardware, software, redes de comunicación y datos, los cuales están catalogados y clasificados conforme al estándar ISO/IEC 27001. Esto permite una gestión adecuada de dichos activos, asegurando su protección y correcta utilización.

A través del análisis de riesgos basado en la metodología Magerit y la norma ISO/IEC 27001, se identificaron varias amenazas y vulnerabilidades más recurrentes en el proceso de evaluación se dio en las redes informáticas y en el uso de redes sociales por parte de los estudiantes. Entre estas amenazas se encuentran la falta de sistemas antivirus actualizados, el desconocimiento de medidas de seguridad y una alta exposición a ataques cibernéticos. La encuesta realizada a los estudiantes reveló que, aunque existe una conciencia general sobre los riesgos en redes sociales, hay una significativa falta de capacitación específica en ciberseguridad. Además, muchos estudiantes desconocen las políticas de seguridad y las rutas de manejo de incidentes dentro de la institución.

La valoración de los activos indicó que los datos y accesos credenciales son críticos y necesitan una protección robusta. Aunque otros activos no presentan un riesgo tan alto, también requieren medidas adecuadas de seguridad para garantizar la integridad y disponibilidad de la información.

La implementación de la norma ISO/IEC 27001 en el proyecto de vulnerabilidades en redes sociales de la IEM San Juan de Pasto responde a la necesidad de garantizar la seguridad y protección de la información en un entorno digital vulnerable a riesgos y amenazas. Esta norma proporciona un marco sistemático para la gestión de la seguridad de la información, permitiendo identificar, evaluar y mitigar las vulnerabilidades específicas. La adopción de la ISO/IEC 27001 establece políticas y controles efectivos, promueve la concienciación y la formación continua en ciberseguridad, y refuerza la confianza en la gestión de la información de la institución. Este compromiso no solo protege a la comunidad educativa, sino que también posiciona a la IEM como un referente en la adopción de estándares internacionales de seguridad, promoviendo un entorno educativo seguro y resiliente frente a las amenazas cibernéticas.

CONCLUSIONS:

The Ciudad de Pasto Municipal Educational Institution has a well-structured management system divided into management, academic, administrative-financial and community areas, each with defined processes to ensure efficient operation and an optimal educational environment. Information management has been a fundamental pillar for the IEM, which is why it became necessary to evaluate the threats and vulnerabilities that could affect its technological infrastructure.

We found that the I.E.M. Ciudad de Pasto has a variety of computer assets that include hardware equipment, software, communication networks and data, which are cataloged and classified in accordance with the ISO/IEC 27001 standard. This allows adequate management of said assets, ensuring their protection and correct use.

Through the risk analysis based on the Magerit methodology and the ISO/IEC 27001 standard, several most recurrent threats and vulnerabilities were identified in the evaluation process, which occurred in computer networks and in the use of social networks by students. These threats include the lack of updated antivirus systems, ignorance of security measures and high exposure to cyber-attacks. The survey conducted among students revealed that, although there is general awareness about the risks in social networks, there is a significant lack of specific training in cybersecurity. Additionally, many students are unaware of security policies and incident management routes within the institution.

The asset assessment indicated that data and access credentials are critical and need robust protection. Although other assets do not present as high a risk, they also require appropriate security measures to ensure the integrity and availability of information.

The implementation of the ISO/IEC 27001 standard in the social network vulnerabilities project of the IEM San Juan de Pasto responds to the need to guarantee the security and protection of information in a digital environment vulnerable to risks and threats. This standard provides a systematic framework for information security management, allowing specific vulnerabilities to be identified, evaluated and mitigated. The adoption of ISO/IEC 27001 establishes effective policies and controls, promotes awareness and continuous training in cybersecurity, and reinforces confidence in the institution's information management. This commitment not only protects the educational community, but also positions the IEM as a reference in the adoption of international security standards, promoting a safe and resilient educational environment against cyber threats.

RECOMENDACIONES:

Se recomienda que la IEM Ciudad de Pasto divulgue el plan presentado, exponiendo las políticas, estrategias y acciones establecidas para mejorar la seguridad de la información. Esto garantizará que toda la comunidad educativa esté informada y comprometida con las medidas de seguridad. Asimismo, se propone que en la guía se incluya una tabla con estrategias, acciones, tiempos y responsables por cada estrategia, lo cual facilitará el seguimiento y la

implementación efectiva de las medidas de seguridad.

Es fundamental mejorar la seguridad de los equipos informáticos mediante la instalación y el mantenimiento actualizado de sistemas de antivirus y otros programas de seguridad en todos los equipos de la institución. Además, se deben establecer políticas claras para la actualización regular de estos sistemas, asegurando que siempre estén protegidos contra las últimas amenazas.

Para fortalecer la ciberseguridad, se deben implementar programas de formación y talleres periódicos para estudiantes y personal, enfocándose en prácticas de ciberseguridad, el uso seguro de redes sociales y la identificación de amenazas en línea. Estos programas deben incluir la importancia de contraseñas seguras, la autenticación de dos factores y el manejo de información sensible.

Es crucial desarrollar y comunicar efectivamente las políticas de seguridad de la información a toda la comunidad educativa, asegurando que todos los miembros estén informados sobre los procedimientos a seguir en caso de incidentes de seguridad. Además, se debe continuar con la implementación de la norma ISO/IEC 27001 que le permita aplicar las políticas para fortalecer la seguridad de la información, lo cual incluye la gestión de riesgos, la evaluación de vulnerabilidades y la implementación de controles de seguridad de la institución.

Se debe mejorar la infraestructura de redes y equipos, asegurando que la infraestructura de red (LAN y servicios en la nube) esté configurada de manera segura y eficiente. También es importante proporcionar redundancia y medidas de respaldo adecuadas para garantizar la disponibilidad de los servicios.

Es esencial fomentar un ambiente de confianza en el cual los estudiantes se sientan seguros para reportar incidentes de ciberacoso o vulnerabilidad en redes sociales. Para ello, se deben establecer canales de comunicación claros y seguros para la denuncia de estos casos. Además, se recomienda realizar auditorías y evaluaciones regulares de los sistemas de seguridad de la información para asegurarse de que las políticas y controles implementados sean efectivos, utilizando los resultados de estas evaluaciones para realizar mejoras continuas en el sistema de seguridad.

Implementar estas recomendaciones ayudará a la IEM Ciudad de Pasto a fortalecer su infraestructura de seguridad informática, proteger a sus estudiantes y personal de amenazas cibernéticas y asegurar un entorno educativo seguro y eficiente.

RECOMMENDATIONS:

It is recommended that the IEM Ciudad de Pasto disseminate the plan presented,

exposing the policies, strategies and actions established to improve information security. This will ensure that the entire educational community is informed and committed to security measures. Likewise, it is proposed that the guide include a table with strategies, actions, times and those responsible for each strategy, which will facilitate the monitoring and effective implementation of security measures.

It is essential to improve the security of computer equipment by installing and maintaining updated antivirus systems and other security programs on all the institution's equipment. Additionally, clear policies must be established for regularly updating these systems, ensuring that they are always protected against the latest threats.

To strengthen cybersecurity, regular training programs and workshops should be implemented for students and staff, focusing on cybersecurity practices, the safe use of social media, and the identification of online threats. These programs should include the importance of strong passwords, two-factor authentication, and the handling of sensitive information.

It is crucial to develop and effectively communicate information security policies to the entire educational community, ensuring that all members are informed about the procedures to follow in the event of security incidents. In addition, the implementation of the ISO/IEC 27001 standard must continue, allowing it to apply policies to strengthen information security, which includes risk management, vulnerability assessment, and the implementation of information security controls. institution.

Network and equipment infrastructure must be improved, ensuring that the network infrastructure (LAN and cloud services) is configured securely and efficiently. It is also important to provide redundancy and adequate backup measures to ensure service availability.

It is essential to foster an environment of trust in which students feel safe to report incidents of cyberbullying or vulnerability on social networks. To achieve this, clear and secure communication channels must be established to report these cases. Additionally, it is recommended to conduct regular audits and evaluations of information security systems to ensure that the policies and controls in place are effective, using the results of these evaluations to make continuous improvements to the security system.

Implementing these recommendations will help IEM Ciudad de Pasto strengthen its cybersecurity infrastructure, protect its students and staff from cyber threats, and ensure a safe and efficient educational environment.