




Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información

Computer security protocols applied in the information technology career laboratories


 <https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.79-84>

Recibido: 15-01-2023 **Aceptado:** 16-04-2023 **Publicado:** 01-06-2023


Johan Enrique Intriago García^{1*}

 <https://orcid.org/0000-0003-0463-4193>


Jonathan Steven Quimis Castro²

 <https://orcid.org/0000-0002-9302-177X>

Cristopher Alexander Choez García³

 <https://orcid.org/0000-0002-3005-6561>

Mario Javier Marcillo Merino⁴

 <https://orcid.org/0000-0001-5818-367X>

1. Estudiante de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
2. Estudiante de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
3. Estudiantes de Tecnologías de la Información, Facultad de Ciencias Técnicas; Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.
4. Máster en Docencia Universitaria e Investigación Educativa; Ingeniero en Sistemas; Docente de la Universidad Estatal del Sur de Manabí; Jipijapa, Ecuador.

Volumen: 2

Número: 1

Año: 2023

Paginación: 79-84

URL: <https://revistas.unesum.edu.ec/JTI/index.php/JTI/article/view/40>

***Correspondencia autor:** intriago-johan7791@unesum.edu.ec

RESUMEN

El presente artículo científico tiene como finalidad garantizar la integridad, confidencialidad y disponibilidad de la información y los recursos utilizados en los laboratorios de la carrera de Tecnologías de la Información, haciendo un análisis de las formas en que se emplean dichos protocolos. Esto se hizo con el fin de proteger los datos y sistemas de posibles amenazas internas y externas, y asegurar la continuidad de las actividades académicas y de investigación. En ese entonces, se consideraba muy importante el uso y aplicación de estos protocolos, y gracias a la investigación realizada, se encontró con la presencia de los protocolos de seguridad físicos, que tenían medidas para proteger el acceso no autorizado a la información a través de la implementación de sistemas de seguridad como cámaras de seguridad, sistemas de alarma, controles de acceso y cerraduras. Sin embargo, se identificaron algunas oportunidades de mejora en cuanto a la protección de la información ante eventos como incendios, inundaciones, terremotos, entre otros. También se detectaron algunas debilidades en los protocolos de seguridad lógicos, a pesar de que la mayoría de los laboratorios tenían medidas de seguridad adecuadas para proteger la información a través de la implementación de firewalls, antivirus, actualizaciones de software, entre otras. Se descubrió que había algunas vulnerabilidades en cuanto a la gestión de contraseñas, el control de acceso a los sistemas y la formación del personal en seguridad informática. A pesar de que se encontraron muchos protocolos, se concluyó que algunos de los laboratorios presentaban ciertas vulnerabilidades.

Palabras clave: control; disponibilidad; firewalls; protocolos; seguridad.

ABSTRACT

The purpose of this scientific article is to guarantee the integrity, confidentiality and availability of the information and resources used in the laboratories of the Information Technology career, making an analysis of the ways in which said protocols are used. This was done in order to protect data and systems from possible internal and external threats, and to ensure the continuity of academic and research activities. At that time, the use and application of these protocols was considered very important, and thanks to the investigation carried out, the presence of physical security protocols was found, which had measures to protect unauthorized access to information through the implementation of security systems such as security cameras, alarm systems, access controls and locks. However, some opportunities for improvement were identified in terms of information protection against events such as fires, floods, earthquakes, among others. Some weaknesses in the logical security protocols were also detected, despite the fact that most of the laboratories had adequate security measures to protect the information through the implementation of firewalls, antivirus, software updates, among others. Some vulnerabilities were found to exist in password management, system access control, and IT security training for staff. Despite the fact that many protocols were found, it was concluded that some of the laboratories had certain vulnerabilities.

Keywords: availability; control; firewalls; protocols; security.



Creative Commons Attribution 4.0
International (CC BY 4.0)

Introducción

La seguridad de la información es un tema de gran importancia en la sociedad actual, donde la tecnología juega un papel fundamental en la vida cotidiana. Las instituciones educativas, como la Universidad Estatal del Sur de Manabí (UNESUM), manejan una gran cantidad de información confidencial, incluyendo datos de los estudiantes, investigaciones científicas y documentos institucionales.

La información confidencial puede estar expuesta a diferentes riesgos, como robo, daño o pérdida, lo que podría resultar en un gran impacto en la privacidad y seguridad de los individuos y la institución. Es por eso que es fundamental establecer protocolos de seguridad de la información físicos y lógicos en los laboratorios de la carrera Tecnología de la Información de la UNESUM.

Los protocolos de seguridad de la información físicos se enfocan en la protección de la información almacenada en los equipos y dispositivos físicos, como computadoras, servidores y dispositivos de almacenamiento. La implementación de medidas de seguridad físicas ayuda a prevenir el acceso no autorizado, la pérdida o daño físico de los equipos y la información almacenada (Marqués, 2022).

Entre las medidas de seguridad físicas que se pueden implementar se encuentran el control de acceso, que permite restringir el acceso a los laboratorios y otros espacios que contengan información confidencial solo a personas autorizadas; la instalación de cámaras de seguridad y alarmas, que ayudan a monitorear y prevenir el robo y la intrusión; la colocación de candados en los armarios y cajones para proteger los dispositivos de almacenamiento y otros equipos y la realización de inspecciones periódicas para asegurarse de que los equipos y cables estén en buen estado y no presenten riesgos de seguridad.

Por otro lado, los protocolos de seguridad lógicos se enfocan en la protección de la información almacenada en sistemas informáticos y redes. Las medidas de seguridad lógicas incluyen la protección contra virus y malware, el control de acceso a los sistemas informáticos y la implementación de firewalls y sistemas de encriptación. Además, se deben establecer contraseñas seguras y actualizarlas periódicamente para evitar el acceso no autorizado (Grupo, 2023).

Es importante destacar que los protocolos de seguridad de la información no se limitan a medidas técnicas. También es necesario establecer políticas y procedimientos de seguridad para los usuarios, incluyendo la promoción de buenas prácticas de seguridad, la concientización sobre los riesgos de seguridad y la implementación de un programa de capacitación para los usuarios sobre las medidas de seguridad físicas y lógicas que se deben seguir.

La implementación de protocolos de seguridad de la información físicos y lógicos en los laboratorios de la carrera de Tecnologías de la Información de la UNESUM es de vital importancia para garantizar la protección de la información confidencial y la continuidad de las actividades académicas e investigativas de la universidad. La implementación de estos protocolos debe ser una prioridad para la universidad, y deben ser revisados y actualizados periódicamente para garantizar su efectividad en un entorno en constante evolución (Marqués, 2022).

Protocolos de seguridad de la información.

Los protocolos de seguridad de la información son un conjunto de medidas, políticas y procedimientos diseñados para proteger la información confidencial de una organización. Estos protocolos se enfocan en la prevención de la exposición, alteración, pérdida o destrucción de información importante, incluyendo datos de clientes, información financiera, propiedad intelectual

y cualquier otra información sensible (Toledo, 2022).

Los protocolos de seguridad de la información pueden ser físicos o lógicos. Los protocolos físicos se enfocan en la protección de los dispositivos de almacenamiento y equipos físicos, como computadoras, servidores y dispositivos de almacenamiento. Los protocolos lógicos, por otro lado, se enfocan en la protección de la información almacenada en sistemas informáticos y redes.

Entre las medidas de seguridad físicas se incluyen el control de acceso, la instalación de cámaras de seguridad y alarmas, la colocación de candados en armarios y cajones, y la realización de inspecciones periódicas. Los protocolos de seguridad lógicos, por su parte, incluyen la implementación de software de seguridad, la protección contra virus y malware, el control de acceso a los sistemas informáticos y la implementación de firewalls y sistemas de encriptación (empresa, 2023).

Es importante destacar que la implementación de protocolos de seguridad de la información no solo se enfoca en medidas técnicas. También es necesario establecer políticas y procedimientos de seguridad para los usuarios, incluyendo la promoción de buenas prácticas de seguridad, la concientización sobre los riesgos de seguridad y la implementación de programas de capacitación para los usuarios.

Los protocolos de seguridad de la información son una parte esencial de la protección de la información confidencial de una organización. La implementación de estos protocolos ayuda a garantizar la privacidad y seguridad de la información, así como la continuidad de las actividades de la organización (Atico34, 2022).

Características de los protocolos de seguridad de la información

Los protocolos de seguridad de la información deben ser diseñados y desarrollados para garantizar la protección de la información confidencial de una organización. Algunas de las características de los protocolos de seguridad de la información incluyen:

- **Integralidad:** los protocolos deben cubrir todos los aspectos de la seguridad de la información, incluyendo medidas técnicas, políticas y procedimientos.
- **Personalización:** los protocolos deben ser personalizados para las necesidades específicas de la organización, considerando su tamaño, estructura, industria y tipo de información que manejan.
- **Flexibilidad:** los protocolos deben ser flexibles para poder adaptarse a los cambios tecnológicos, de la industria y a las necesidades de la organización.
- **Claridad:** los protocolos deben ser claros y fáciles de entender para todos los miembros de la organización. Esto incluye el uso de lenguaje sencillo y la clarificación de los roles y responsabilidades de cada persona en el manejo de la información.
- **Actualización continua:** los protocolos deben ser actualizados de manera constante para garantizar que estén en línea con las últimas amenazas y vulnerabilidades de seguridad.
- **Conciencia de la cultura organizacional:** los protocolos deben ser desarrollados con una comprensión profunda de la cultura organizacional. Esto incluye considerar la actitud de los empleados hacia la seguridad de la información y diseñar políticas y procedimientos que sean aceptables para ellos.
- **Enfoque en la privacidad:** los protocolos deben estar enfocados en garantizar la privacidad de los datos y la información de la organización.

Entonces decimos que los protocolos de seguridad de la información deben ser integrales, personalizados, flexibles, claros, actualizados continuamente, considerar la cultura organizacional, enfocarse en la privacidad de los datos y estar diseñados para garantizar la protección de la información confidencial de la organización (Bustamante, 2022).

Metodología

La metodología utilizada para la investigación de los protocolos de seguridad física y lógica de la UNESUM, considerando la revisión bibliográfica y el análisis de campo, puede clasificarse como una metodología de investigación mixta y descriptiva. En concreto, se realizó una revisión bibliográfica para recopilar información y conocimientos teóricos previos sobre los protocolos de seguridad física y lógica. Luego, se llevó a cabo un análisis de campo para recopilar datos empíricos y observaciones en los laboratorios de la UNESUM sobre los protocolos de seguridad implementados. La combinación de ambos métodos permitió obtener una visión más amplia y completa sobre los protocolos de seguridad física y lógica de la UNESUM, lo que permitió describir y analizar tanto los aspectos teóricos como prácticos de los protocolos implementados.

Resultados y Discusión

Los resultados obtenidos en la evaluación de los Protocolos de Seguridad de la Información Físicos y Lógicos en los laboratorios de la carrera Tecnologías de la Información de la UNESUM muestran que, en general, los laboratorios tienen medidas de seguridad adecuadas para proteger la información que manejan. Sin embargo, también se identificaron algunas debilidades y oportunidades de mejora que se deben considerar.

En cuanto a los protocolos de seguridad físicos, se encontró que los laboratorios tienen

medidas para proteger el acceso no autorizado a la información a través de la implementación de sistemas de seguridad como cámaras de seguridad, sistemas de alarma, controles de acceso y cerraduras. Sin embargo, se identificaron algunas oportunidades de mejora en cuanto a la protección de la información ante eventos como incendios, inundaciones, terremotos, entre otros. Se sugiere la implementación de medidas adicionales como la instalación de sistemas de detección de humo, extintores, sistemas de protección contra inundaciones, entre otros.

Del mismo modo los protocolos de seguridad lógicos, se encontró que la mayoría de los laboratorios tienen medidas de seguridad adecuadas para proteger la información a través de la implementación de firewalls, antivirus, actualizaciones de software, entre otras. Sin embargo, también se identificaron algunas debilidades en cuanto a la gestión de contraseñas, el control de acceso a los sistemas y la formación del personal en seguridad informática. Se recomienda la implementación de medidas adicionales para mejorar la seguridad de la información, como la formación del personal en seguridad informática, la implementación de políticas de seguridad de contraseñas y la revisión periódica de los permisos de acceso a los sistemas.

En general, se concluye que los laboratorios de la UNESUM tienen medidas de seguridad adecuadas para proteger la información que manejan. Sin embargo, se deben implementar algunas medidas adicionales para mejorar la protección de la información ante eventos imprevistos y reforzar la seguridad lógica. Se recomienda la implementación de políticas de seguridad de la información y la formación del personal para mejorar la conciencia y la cultura de seguridad en los laboratorios (REYES, 2018).

También se sugiere la revisión periódica de los protocolos de seguridad y su actualización para adaptarse a los cambios tecnológicos y las nuevas amenazas a la seguridad.

Conclusiones

En conclusión, los Protocolos de Seguridad de la Información Físicos y Lógicos en los Laboratorios de la carrera Tecnologías de la Información de la UNESUM son fundamentales para proteger la información que se maneja en estos espacios y garantizar la integridad, confidencialidad y disponibilidad de la misma.

Los resultados obtenidos en la evaluación de los protocolos de seguridad muestran que los laboratorios tienen medidas de seguridad adecuadas, pero también se han identificado debilidades y oportunidades de mejora que deben ser consideradas para mejorar la protección de la información.

Es importante destacar que la seguridad de la información es una responsabilidad compartida entre todos los usuarios de los laboratorios y no solo de los responsables de seguridad. Por lo tanto, es fundamental que se promueva una cultura de seguridad en los laboratorios y se fomente la formación continua del personal en temas de seguridad de la información.

Además, se debe tener en cuenta que los protocolos de seguridad deben ser revisados y actualizados periódicamente para adaptarse a los cambios tecnológicos y las nuevas amenazas a la seguridad. También se recomienda que se establezcan políticas de seguridad de la información claras y que se realicen auditorías periódicas para verificar el cumplimiento de los protocolos.

Es importante destacar que la seguridad de la información no solo se limita a los protocolos físicos y lógicos, sino que también incluye aspectos relacionados con la gestión de riesgos, la continuidad del negocio y la privacidad de los datos. Por lo tanto, es fundamental que los protocolos de seguridad se integren en una estrategia global de seguridad de la información para garantizar una protección integral.

Entonces los Protocolos de Seguridad de la Información Físicos y Lógicos en los Laboratorios de la UNESUM son fundamentales para garantizar la protección de la información que se maneja en estos espacios. Se recomienda implementar medidas adicionales para mejorar la protección de la información y promover una cultura de seguridad en los laboratorios. También es fundamental revisar y actualizar periódicamente los protocolos de seguridad y establecer una estrategia global de seguridad de la información para garantizar una protección integral.

Bibliografía

- Atico34, G. (2022). protecciondatos. Obtenido de <https://protecciondatos-lopd.com/empresas/protocolos-seguridad-informatica/#:~:text=Los%20protocolos%20de%20seguridad%20inform%C3%A1tica%20son%20las%20reglas%20o%20normas,la%20informaci%C3%B3n%2C%20manipularla%20o%20destruirla>.
- Bustamante, M. (2022). mbaonlineceupe. Obtenido de <https://mbaonlineceupe.com/cuales-son-las-caracteristicas-basicas-de-seguridad-de-la-informacion/>
- empresa. (19 de enero de 2023). datos101. Obtenido de <https://www.datos101.com/blog/medidas-de-seguridad-informatica/>
- Grupo. (2023). ayudaleyprotecciondatos. Obtenido de <https://ayudaleyprotecciondatos.es/2020/12/30/seguridad-logica/#:~:text=El%20t%C3%A9rmino%20Seguridad%20l%C3%B3gica%20se,el%20firewall%2C%20enrutadores%20y%20conmutadores>.
- Marqués, D. F. (2022). clinic-cloud. Obtenido de <https://clinic-cloud.com/blog/protocolos-de-seguridad-de-la-informacion/>
- REYES, D. J. (2018). repositorio. Obtenido de <http://repositorio.unesum.edu.ec/bitstream/53000/1474/1/UNESUM-ECU-REDES-2017-06.pdf>
- Toledo, R. (2022). grupocibernos. Obtenido de <https://www.grupocibernos.com/blog/cuales-son-los-protocolos-a-seguir-de-seguridad-informatica>

Cómo citar: Intriago García, J. E., Quimis Castro, J. S., Choez García, C. A., & Marcillo Merino, M. J. (2023). Protocolos de seguridad informática aplicados en los laboratorios de la carrera tecnologías de la información. *Journal TechInnovation*, 2(1), 79–84. <https://doi.org/10.47230/Journal.TechInnovation.v2.n1.2023.79-84>