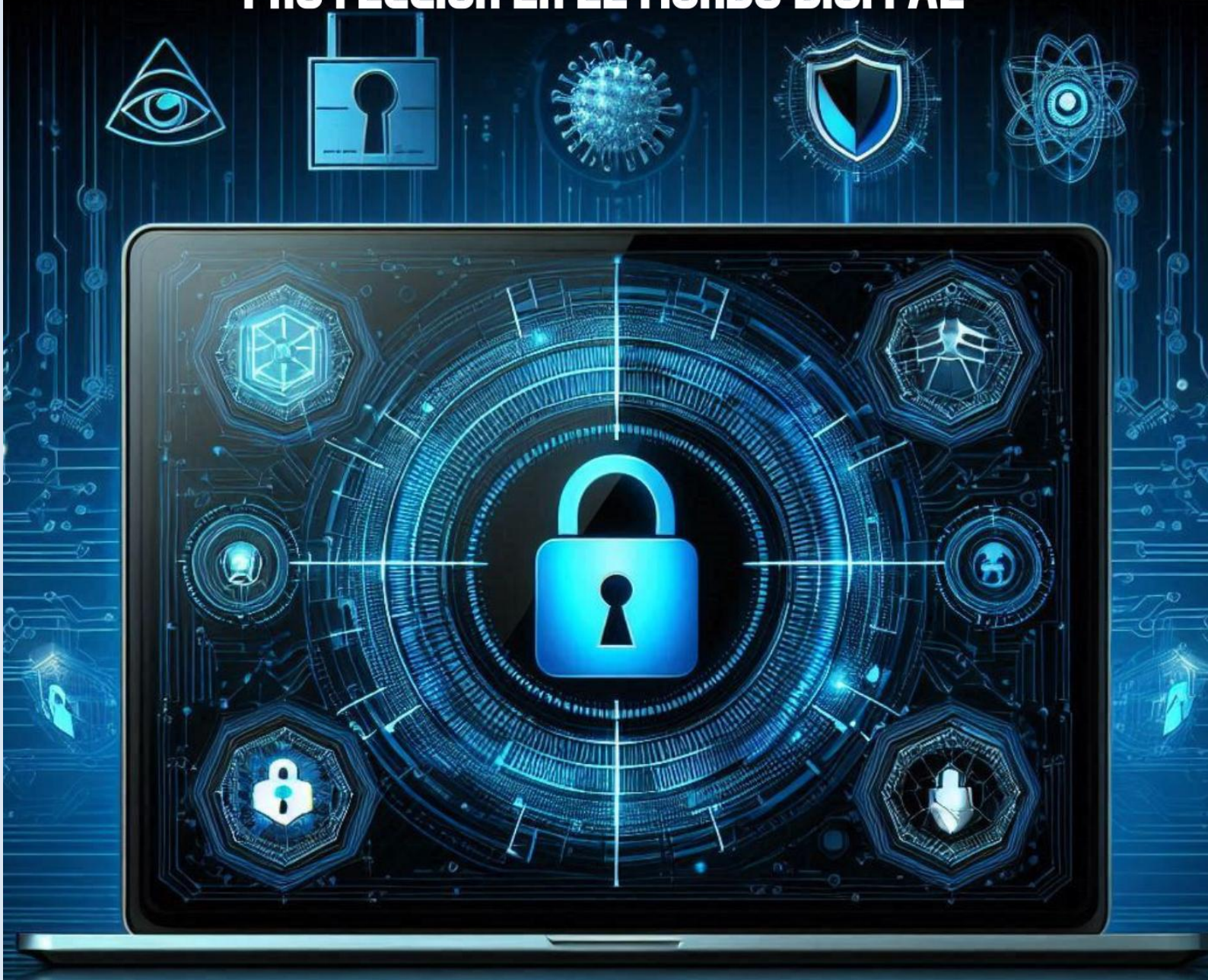
CIBERSEGURIDAD

UN ENFOQUE INTERDISCIPLINARIO PARA LA PROTECCIÓN EN EL MUNDO DIGITAL



Sello Editorial CITSA

Compiladores

José Antonio Romero Palmera
Vita María Calzolaio Cristofano

José Antonio Romero Palmera &Vita María Calzolaio Cristofano
Compiladores

Ciberseguridad:

Un enfoque interdisciplinario para la protección del mundo digital

https://doi.org/10.61286/edcitsa.vi.64

Sello Editorial CITSA

Maracay, estado Aragua, Venezuela 2024

Catalogación en Fuente

José Antonio Romero Palmera..

Ciberseguridad: Un enfoque interdisciplinario para la protección del mundo digital. 1ª ed. – Maracay: Sello Editorial CITSA, 2024.
Recursos en línea (85 páginas); 7 il. ; 21 x 29,7 cm.
ISBN: 978-980-8050-00-4
- Teoría de la comunicación y el control Cibernética . Libros de texto. I. José Antonio Romero Palmera., II. Vita María Calzolaio Cristofano.

CDD 003.5

Sello Editorial CITSA

Centro de Investigación en Tecnologías de Salud y Ambiente.

Dirección: Calle el Stadium Nº 3-A, Las Brisas, La Pedrera, Parroquia Las Delicias, Maracay estado Aragua, Venezuela.

Email: citsa@investigaciondetecnologias.com
Web: www.investigaciondetecnologias.com

Coordinación Editorial: Dr. José Romero
Revisión y corrección de estilo: Lic.Esp. Carmen Julia Silva Sánchez
Diseño de cubierta: CITSA
Composición y puesta en línea: Dra. Mirta Isabel Camacho Rivas.
Depósito Legal en la Biblioteca Nacional de Venezuela según el Número AR2024000390.

Índice

Prólogo

La ciberseguridad se ha convertido en un tema de vital importancia en la era digital, donde la interconexión de sistemas y la dependencia de tecnologías avanzadas han creado un entorno propicio para la vulnerabilidad. Este libro, titulado "**Ciberseguridad: un enfoque interdisciplinario para la protección del mundo digital**", busca abordar este fenómeno desde múltiples perspectivas, integrando conocimientos y prácticas de diversas disciplinas que son esenciales para comprender y enfrentar los retos actuales en el ámbito de la seguridad cibernética. En un mundo donde los datos son considerados el nuevo petróleo, la ciberseguridad no solo es una necesidad técnica, sino también una cuestión estratégica que afecta a empresas, gobiernos y ciudadanos por igual.

Los desafíos en ciberseguridad son numerosos y complejos. Las amenazas como ransomware, phishing y ataques DDoS están en constante evolución, lo que requiere que las organizaciones se adapten rápidamente a un panorama cambiante. Además, el aumento del trabajo remoto ha ampliado la superficie de ataque, haciendo que las empresas sean más vulnerables a incidentes de seguridad. Las pequeñas y medianas empresas (PYMES) son especialmente susceptibles debido a recursos limitados para invertir en medidas de protección adecuadas.

Un aspecto fundamental de la ciberseguridad es su naturaleza interdisciplinaria. La protección efectiva de los activos digitales no puede lograrse únicamente a través de soluciones tecnológicas; también es crucial considerar aspectos legales y psicológicos. Por ejemplo, la ingeniería social es una técnica utilizada por ciberdelincuentes para manipular a las personas y obtener acceso a información sensible. Esto resalta la necesidad de educar a los usuarios sobre las amenazas potenciales y fomentar una cultura de seguridad dentro de las organizaciones.

La educación continua es esencial para los profesionales en este campo. Dado que las amenazas cibernéticas están en constante evolución, es vital que los expertos se mantengan actualizados sobre las últimas tendencias y técnicas utilizadas por los atacantes. Este libro proporcionará no solo una base teórica sólida, sino también ejemplos prácticos y estudios de caso que ilustran cómo aplicar estos conocimientos en situaciones del mundo real. Al abordar temas como principios básicos de seguridad informática, normativas legales y el impacto del comportamiento humano, buscamos ofrecer una comprensión integral que empodere a los lectores.

Además, se explorarán las implicaciones éticas de la ciberseguridad. A medida que las tecnologías avanzan, surgen preguntas sobre la privacidad, el uso responsable de datos y la vigilancia. La comprensión de estos temas es crucial para desarrollar políticas efectivas que protejan tanto a las organizaciones como a los individuos en un entorno digital cada vez más complejo.

El objetivo principal de "**Ciberseguridad: un enfoque interdisciplinario para la protección del mundo digital**" es ofrecer a los lectores herramientas prácticas y conocimientos aplicables para enfrentar los desafíos actuales. La colaboración entre disciplinas será clave para

construir un futuro digital más seguro, donde tanto individuos como organizaciones puedan prosperar sin temor a ser víctimas de ataques cibernéticos.

En este libro no solo educa sobre las amenazas existentes, sino que también proporciona estrategias para implementar medidas efectivas de protección. A través del estudio y aplicación del contenido presentado aquí, esperamos contribuir a formar una nueva generación de profesionales capaces de enfrentar los desafíos del mundo digital con confianza y competencia. La ciberseguridad es un esfuerzo colectivo que requiere la participación activa de todos los sectores de la sociedad; juntos podemos construir un entorno digital más seguro y resiliente.

José Antonio Romero Palmera ✉ **& Vita María Calzolaio Cristofano** ✉

Compiladores

Introducción

La ciberseguridad se ha convertido en un pilar fundamental en la era digital, donde la interconexión de sistemas y la creciente dependencia de tecnologías avanzadas han expuesto a individuos y organizaciones a un sinfín de amenazas. Este libro, "**Ciberseguridad: un enfoque interdisciplinario para la protección del mundo digital**", se propone explorar los múltiples aspectos de la ciberseguridad, destacando su importancia y relevancia en diversos campos. A medida que los ataques cibernéticos se vuelven más sofisticados y frecuentes, es crucial entender no solo las técnicas de defensa, sino también el contexto en el que estas amenazas emergen.

El primer capítulo se centra en la importancia de la ciberseguridad en la era digital, donde se abordarán los conceptos fundamentales que sustentan esta disciplina. Se explorarán las amenazas más comunes, como el malware, el phishing y los ataques DDoS, que representan riesgos significativos para la confidencialidad, integridad y disponibilidad de la información. La comprensión de estos conceptos es esencial para establecer una base sólida sobre la cual construir estrategias de defensa efectivas.

En los siguientes capítulos, se profundizará en la ciberseguridad aplicada a áreas específicas como la ingeniería civil y la ingeniería de sistemas. Se analizarán los riesgos particulares que enfrenta cada sector y las tecnologías emergentes que pueden ayudar a mitigar estos desafíos. Por ejemplo, en el ámbito de la ingeniería civil, se discutirán las medidas necesarias para proteger infraestructuras críticas contra ciberataques, mientras que en ingeniería de sistemas se examinará cómo fortalecer redes y sistemas informáticos frente a amenazas cibernéticas.

Otro aspecto clave del libro es la educación en ciberseguridad, un tema que se abordará en profundidad en uno de los capítulos. La concienciación y formación son fundamentales para empoderar a los usuarios y reducir el riesgo de ataques exitosos. Se explorarán las barreras que dificultan la adopción de prácticas efectivas en educación y cómo superarlas, así como herramientas y recursos disponibles para enseñar sobre ciberseguridad.

Además, se discutirá el impacto de la ciberseguridad en el ámbito educativo, incluyendo la protección de datos tanto de estudiantes como de docentes. La confidencialidad de esta información es crítica, y se analizarán las tendencias emergentes que afectan este panorama. La integración de prácticas seguras en entornos educativos no solo protege a los individuos, sino que también contribuye a formar una cultura más amplia de seguridad digital.

Finalmente, el libro presentará casos prácticos sobre la metodología MSSI (Metodología para la Seguridad en Sistemas Informáticos) aplicada al proceso de enseñanza-aprendizaje. Se examinarán las ventajas y desafíos al implementar esta metodología en entornos educativos, así como buenas prácticas que puedan servir como referencia para educadores y administradores.

A través de este enfoque interdisciplinario, "**Ciberseguridad: un enfoque interdisciplinario para la protección del mundo digital**" busca ofrecer una visión integral que

no solo informe sobre las amenazas actuales, sino que también proporcione herramientas prácticas para enfrentarlas. La colaboración entre disciplinas será clave para construir un futuro digital más seguro, donde tanto individuos como organizaciones puedan prosperar sin temor a ser víctimas de ataques cibernéticos, como puede suceder en las empresas.

José Antonio Romero Palmera ✉ **& Vita María Calzolaio Cristofano** ✉
Compiladores

Dulio Oseda Gago [1], **Amanda Durán Carhuamaca** [1], **Guido Raúl Larico Uchamaco** [1], **María Cristina Ramos Toledo** [1], **Hussein Anthony Palomino Quispe** [1], **Patricia Paulina Huarancca Contreras** [1] & **José Luis Medina Aliaga** [1]

1. Universidad Nacional de Cañete, Perú

Importancia de la ciberseguridad en la era digital

Este aumento de la conectividad y la dependencia de los sistemas informáticos también ha dado lugar a un incremento en las amenazas cibernéticas (ENISA, 2023). Los delincuentes informáticos y los actores malintencionados han desarrollado métodos cada vez más sofisticados para infiltrarse en estos sistemas y causar daños, como por ejemplo, apropiarse de datos confidenciales, interrumpir servicios esenciales o incluso sabotear infraestructuras vitales.

Estos desafíos se han acentuado con la aceleración de la transformación digital durante la pandemia de COVID-19, que ha impulsado la adopción masiva de soluciones y herramientas remotas y ha expuesto a las organizaciones a riesgos cibernéticos (IBM, 2022). Además, el aumento del trabajo remoto y la adopción de tecnologías emergentes como el Internet de las Cosas (IoT) y la Inteligencia Artificial (IA) han ampliado mucho más la superficie de ataque, creando nuevas vulnerabilidades que los ciberdelincuentes buscan explotar.

Por lo tanto, invertir en medidas de ciberseguridad sólidas y mantener una postura de defensa actualizada se ha vuelto trascendental no solo para proteger datos y sistemas críticos, sino también para salvaguardar la privacidad, la reputación y la prosperidad de individuos, empresas y naciones en el mundo digital (Ponemon Institute, 2022). La ciberseguridad se ha convertido en una piedra angular para garantizar la confianza, la resiliencia y el éxito en la era de la transformación digital, desempeñando un papel esencial en la protección de la infraestructura, la economía y nuestra forma de vida.

Partiendo de un enfoque interdiscilinario, proteger la información se ha convertido en un activo invaluable y la conectividad es una necesidad imperante. Este enfoque demuestra que la ciberseguridad no es solo una cuestión tecnológica, sino que tiene un impacto significativo en múltiples áreas de una organización. Cada una de estas áreas destaca la importancia crítica de la ciberseguridad para proteger el mundo digital y garantizar la resiliencia, la confianza y el éxito a largo plazo. En la tabla 1 se muestra la importancia de la ciberseguridad desde un enfoque interdisciplinario para la protección en el mundo digital.

En esta época digital, la ciberseguridad se ha convertido en una prioridad crítica, tanto a nivel particular como general. Como individuos, es elemental estar informados sobre los desafíos

y riesgos que enfrentamos en un mundo cada vez más interconectado. Todos debemos tomar medidas proactivas para proteger la información, los dispositivos y la privacidad en línea.

Tabla 1. *Importancia de la ciberseguridad desde un enfoque multidisciplinario*

Área	Importancia de la Ciberseguridad
Tecnología	Protección de infraestructura y sistemas IT críticos Detección y respuesta a amenazas cibernéticas Implementación de controles de seguridad robustos
Negocios	Asegurar la continuidad operativa Protección de datos y activos empresariales Mantener la confianza de clientes y socios
Normativa y Cumplimiento	Cumplimiento de regulaciones de ciberseguridad Evitar sanciones y multas por incidentes de seguridad Demostración de prácticas de seguridad adecuadas
Recursos Humanos	Capacitación y concientización del personal sobre ciberseguridad Desarrollo de habilidades y competencias en seguridad digital Promoción de una cultura de seguridad
Legal y Privacidad	Protección de datos personales y derechos de privacidad Gestión de incidentes y respuesta a brechas de seguridad Asesoramiento reglamentario sobre requisitos y obligaciones
Estrategia y Gobernanza	Alineación de la ciberseguridad con los objetivos del negocio Definición de políticas, procesos y responsabilidades Gestión integral de riesgos cibernéticos
Educación	Desarrollo de habilidades y competencias digitales seguras Uso responsable y seguro de la tecnología Proteger la privacidad y los datos personales de los estudiantes Implementación de controles de seguridad para plataformas de aprendizaje en línea Aseguramiento de la disponibilidad y la integridad de los datos académicos

A nivel de sociedad, es importante que se trabaje de manera conjunta para fortalecer la seguridad cibernética. Las organizaciones, los gobiernos y los ciudadanos deben colaborar para desarrollar estrategias y políticas efectivas que permitan hacer frente a las amenazas digitales. Solo a través de un enfoque integral y coordinado se puede salvaguardar la seguridad y prosperidad en el entorno digital. Como individuos y como sociedad, debemos estar informados y tomar medidas para enfrentar los desafíos que nos presenta esta era digital. En la tabla 2 se resumen los aspectos más relevantes sobre la Ciberseguridad.

Tabla 2. *Aspectos relevantes sobre la ciberseguridad*

Aspecto	Descripción
Amenazas Persistentes	Ciberdelincuentes: Buscan explotar vulnerabilidades para obtener acceso no autorizado a datos Malware: Virus, ransomware y otras amenazas Ingeniería Social: Tácticas psicológicas para engañar a las personas
Importancia de la Ciberseguridad	Protección de datos personales Seguridad empresarial Infraestructura crítica
Enfoques de Ciberseguridad	Prevención Detección y respuesta Educación y concienciación
Tendencias Emergentes	Inteligencia artificial y machine learning IoT (Internet de las cosas) Ciberseguridad cuántica

En la tabla 3 se resume los principales aspectos que destacan la importancia estratégica de la ciberseguridad en la era digital, desde la protección de datos hasta la seguridad nacional. Cada uno de estos elementos subraya la necesidad de invertir en medidas de seguridad cibernética sólidas y mantener una postura de defensa actualizada.

Tabla 3. *Aspectos que destacan la ciberseguridad*

Aspecto	Importancia
Protección de Datos	La ciberseguridad es crucial para proteger los datos personales, financieros y empresariales de los ciberataques y el robo de identidad
Resiliencia Operativa	Los sistemas y redes seguros garantizan la continuidad de las operaciones críticas y evitan interrupciones costosas
Confianza del Usuario	Una sólida postura de ciberseguridad genera confianza en los clientes, socios y partes interesadas
Cumplimiento Normativo	El cumplimiento de las regulaciones de ciberseguridad es obligatorio y evita sanciones y multas
Reputación Empresarial	Los incidentes de seguridad pueden dañar gravemente la reputación y la imagen de una organización
Innovación y Competitividad	La ciberseguridad permite adoptar nuevas tecnologías y modelos de negocio de manera segura
Seguridad de la Infraestructura Crítica	La protección de sistemas como energía, transporte y comunicaciones es vital para la estabilidad social y económica
Ciberseguridad Nacional	Los gobiernos deben garantizar la seguridad cibernética para proteger la soberanía y la seguridad nacional

Conceptos fundamentales de la ciberseguridad y amenazas comunes

Los conceptos fundamentales de la ciberseguridad abarcan una serie de principios y definiciones clave que sentaron las bases para el desarrollo y la evolución de este campo. Entre estos conceptos se encuentran la confidencialidad, la integridad y la disponibilidad (también conocido como la "tríada CIA"), que establecen los pilares para garantizar la seguridad de la información (Whitman & Mattord, 2019; Stallings & Brown, 2018), así como autenticación, no repudio y gestión de riesgos (Whitman & Mattord, 2019), definen los principios esenciales que deben guiar los esfuerzos de ciberseguridad.

Además, conceptos como el riesgo, la amenaza, la vulnerabilidad y el control de acceso son fundamentales para comprender los desafíos y las estrategias de mitigación en el entorno cibernético (Pfleeger & Pfleeger, 2015). Finalmente, la ciberseguridad también se basa en principios como la defensa en profundidad, la segmentación y la resiliencia, que permiten a las organizaciones y los individuos desarrollar una postura de seguridad sólida y adaptable (Andress, 2019).

Estos conceptos fundamentales sirven como base para desarrollar e implementar estrategias y controles efectivos de ciberseguridad en las organizaciones. En la tabla 4 se describe cada concepto.

Estos conceptos fundamentales sientan las bases para comprender los principios y las estrategias clave de la ciberseguridad y permiten a las organizaciones y los individuos desarrollar enfoques sólidos y efectivos para proteger sus activos digitales. Además de los conceptos fundamentales, hay otros elementos complementarios importantes que permiten ampliar la visión

de los diferentes componentes que conforman el campo de la ciberseguridad, desde las amenazas hasta los marcos de referencia y las estrategias de capacitación, entre ellos se encuentran:

Tabla 4. *Descripción de conceptos fundamentales en la ciberseguridad*

Concepto Fundamental	Descripción
Confidencialidad	Asegurar que la información solo sea accesible por las entidades autorizadas. Evitar la divulgación no autorizada de datos
Integridad	Garantizar que la información y los sistemas se mantengan precisos, completos y sin alteraciones no autorizadas
Disponibilidad	Asegurar que los usuarios autorizados tengan acceso confiable a la información y los recursos cuando lo necesiten
Autenticación	Verificar la identidad de un usuario, dispositivo o sistema para controlar el acceso a los recursos
No Repudio	Impedir que una entidad pueda negar haber realizado una acción o transacción específica
Gestión de Riesgos	Identificar, analizar y mitigar los riesgos de seguridad a los que están expuestos los sistemas e información
Defensa en Profundidad	Implementar múltiples capas de controles de seguridad para proteger contra diferentes tipos de amenazas
Autenticación	Verificar la identidad de un usuario, dispositivo o sistema antes de otorgar acceso a recursos (Stallings & Brown, 2018).
No Repudio	Principio que impide que un usuario o entidad niegue su participación en una determinada acción o evento (Stallings & Brown, 2018).
Ciber-Resilencia	Capacidad de un sistema, organización o individuo de anticipar, resistir, adaptarse y recuperarse de disrupciones cibernéticas (NIST, 2018).
Defensa en Profundidad	Enfoque de seguridad que combina múltiples capas de controles y mecanismos de protección (Andress, 2019).
Gestión de Riesgos	Proceso sistemático de identificar, analizar y mitigar los riesgos cibernéticos a los que está expuesta una organización (Whitman & Mattord, 2019).

Tipos de Amenazas Cibernéticas: incluyen malware, phishing, ataques de denegación de servicio, accesos no autorizados y filtraciones de datos, entre otros (Andress, 2019).

Controles de Seguridad: mecanismos técnicos, administrativos y físicos implementados para mitigar riesgos, como firewalls, sistemas de detección de intrusos, políticas de seguridad y controles de acceso (Whitman & Mattord, 2019).

Estándares y Marcos de Seguridad: guías y buenas prácticas como ISO/IEC 27001, NIST Cybersecurity Framework y CIS Controls, que proporcionan lineamientos para la implementación de programas de ciberseguridad (ISO, 2013; NIST, 2018; CIS, 2021).

Gobierno y Cumplimiento: leyes, regulaciones y requisitos de cumplimiento relacionados con la protección de datos, privacidad y seguridad de la información (por ejemplo, GDPR, HIPAA, PCI DSS) (Whitman & Mattord, 2019).

Conciencia y Capacitación en Seguridad: programas educativos y de concientización para que usuarios, empleados y organizaciones comprendan y adopten prácticas de ciberseguridad (Cone et al., 2007).

Paralelamente, las organizaciones deben estar preparadas para enfrentar las principales amenazas cibernéticas, como malware, ataques de phishing y denegación de servicio, entre otras

(Andress, 2019).Un enfoque integral que combine estos conceptos fundamentales con la identificación y mitigación de amenazas comunes es decisivo para construir sistemas y entornos digitales seguros y resilientes.

La ciberseguridad es esencial para garantizar una experiencia segura en el uso de la tecnología y proteger nuestra información digital. Además de las amenazas cibernéticas más conocidas como malware, phishing y denegación de servicio, algunas otras amenazas comunes que las organizaciones deben enfrentar incluyen:

Ataques de Ingeniería Social: técnicas que manipulan a las personas para revelar información confidencial o realizar acciones que comprometen la seguridad, como dar clic en enlaces maliciosos (Krombholz et al., 2015).

Violaciones de Datos: accesos no autorizados a sistemas o bases de datos que resultan en la exposición o pérdida de información sensible como datos personales o información financiera (Romanosky, 2016).

Ataques Internos: amenazas provenientes de usuarios autorizados, como empleados deshonestos o negligentes, que pueden causar daños por abuso de privilegios o sabotaje (Nurse et al., 2014).

Vulnerabilidades de Software: debilidades en el diseño o implementación de sistemas y aplicaciones que pueden ser explotadas por atacantes para acceder, modificar o destruir información (Choudhary et al., 2020).

Ransomware: malware que secuestra datos y sistemas, exigiendo un rescate para recuperar el acceso (Liao et al., 2016).

Ataques de Día Cero: exploits que se aprovechan de vulnerabilidades desconocidas o recién descubiertas, antes de que se disponga de una corrección o parche (Bilge & Dumitras, 2012).

La ciberseguridad es una prioridad estratégica clave para cualquier organización en la era digital. Entender los vectores de ataque más prevalentes, como el ransomware, el phishing y las brechas de datos, es fundamental para implementar controles de seguridad adecuados y mantener protegidos los activos digitales. Asimismo, estar atento a las amenazas internas y los ataques de denegación de servicio también es crucial. Al adoptar un enfoque holístico que aborde estos riesgos clave, las organizaciones pueden mejorar significativamente su postura de seguridad y estar mejor preparadas para responder y recuperarse de incidentes. La ciberseguridad sólida es ahora una necesidad empresarial crucial en un mundo cada vez más dependiente de la tecnología. Mantener estos conceptos fundamentales en mente es un paso esencial para proteger a su organización de los crecientes desafíos de seguridad.

Referencias Bibliográficas

Andress, J. (2019). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (3rd ed.). Syngress.

Bilge, L., & Dumitras, T. (2012). *Before we knew it: an empirical study of zero-day attacks in the real world*. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844).

CIS. (2021). CIS Controls v8. Center for Internet Security.

Cisco. (2022). Cisco Annual Internet Report (2018–2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

Choudhary, N., Kesarwani, A., & Mehtre, B. M. (2020). Vulnerability analysis and patch recommendation using CVE dataset. *Journal of King Saud University-Computer and Information Sciences*, 32(1), 99-109.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *Computers & Security*, 26(1), 63-72.

ENISA. (2023). Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

IBM. (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/ADDVQPOX

ISO. (2013). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113-122.

Liao, K., Zhao, Z., Doupe, A., & Ahn, G. J. (2016). *Behind closed doors: measurement and analysis of CryptoLocker ransoms in Bitcoin*. In 2016 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity* (Version 1.1). National Institute of Standards and Technology.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., & Whitty, M. (2014). *Understanding insider threat: A framework for characterising attacks*. In 2014 IEEE Security and Privacy Workshops (pp. 214-228). IEEE.

Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in Computing* (5th ed.). Prentice Hall.

Ponemon Institute. (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/ADDVQPOX

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121-135.

Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (3rd ed.). Pearson.

Whitman, M. E., & Mattord, H. J. (2019). *Principles of Information Security* (6th ed.). Cengage Learning.

Ronald Vilcahuaman Tadeo ✉ 1, **Wilmer Carlos Chavez Pecho** ✉ 1, **David Ramos Piñas** ✉ 2 **& Giancarlo Fernando Meza Terbullino** ✉ 1

1. Universidad Continental, Huancayo Perú - 2.Universidad Peruana Los Andes, Huancayo Perú

En los sectores de la construcción y la ingeniería civil, la seguridad de la información es una de las principales preocupaciones de las empresas u organizaciones públicas o privadas, no es solo un reto, sino una prioridad. Imagina que cada avance tecnológico, cada nueva herramienta integrada en los procesos de edificación y diseño, trae consigo un potencial caballo de Troya que podría desatar ciberataques.

Por eso, es importante incorporar medidas de seguridad cibernéticas robustas, que actúen como escudo protector de los sistemas de ingeniería civil. Hablamos de levantar muros digitales como los firewalls, de cifrar los datos como si fueran tesoros, de autenticar a los usuarios como guardianes del reino y de formar al personal como si fueran centinelas en la cibernética.

No se puede olvidar que la ciberseguridad no solo trasciende la protección de los sistemas informáticos; es también el arte de custodiar la información confidencial de los clientes, los datos de diseño y salvaguardar la confianza pública de las infraestructuras que soportan la vida cotidiana. Es esencial, que cada organización forje políticas claras de seguridad de la información y se comprometa con el cumplimiento cabal de las mismas.

Riesgos de ciberseguridad en la ingeniería civil

En el complejo mundo de la ingeniería civil, donde se erigen puentes y se construyen ciudades, existe un invasor invisible y silencioso: los riesgos de ciberseguridad. Desde el uso indebido de información hasta el acceso no autorizado y la pérdida de datos, los riesgos son tan reales como el acero y el hormigón (Rau & Carneiro, 2019). Imagina un escenario donde un solo clic malintencionado podría poner en peligro un puente entero o comprometer la seguridad de un sistema de agua. Por eso, la ingeniería civil moderna no solo requiere cálculos precisos y materiales de calidad, sino también una armadura digital impenetrable que salvaguarde cada proyecto desde su concepción hasta su realización. La ciberseguridad en la ingeniería civil no es solo una línea de código o un firewall; es la vanguardia que protege el núcleo vital de nuestras sociedades.

Las empresas de construcción tienen acceso a una gran cantidad de información, entre las que destacan la propiedad intelectual, los activos patentados, los planos, las especificaciones

arquitectónicas, así como las cuentas bancarias y financieras de las empresas, convirtiéndola en objetivos atractivos para los ciberdelincuentes.

Es así que, la ciberseguridad como campo especializado, se enfoca en proteger los sistemas informáticos, redes y datos contra amenazas cibernéticas (Galloway & Aravind, 2019a). Si bien la ingeniería civil se centra principalmente en la construcción de infraestructura física, como edificios, puentes y carreteras, hay algunos aspectos en los que la ciberseguridad puede desempeñar un papel importante:

Infraestructura crítica: como redes eléctricas, sistemas de transporte y plantas de tratamiento de agua, dependen cada vez más de tecnologías de la información y la comunicación. Un ingeniero civil que trabaje en estos proyectos debe colaborar con expertos en ciberseguridad para asegurarse de que estos sistemas estén debidamente protegidos contra ciberataques (Karyotis & Kokolakis, 2018).

Edificios inteligentes: estos edificios modernos a menudo cuentan con sistemas de control y automatización integrados, como sistemas de seguridad, iluminación y climatización. Un profesional de la ingeniería civil debe hacer un engranaje con especialistas en ciberseguridad de modo de garantizar que estos sistemas estén protegidos contra accesos no autorizados y ataques (Aloulou & Meddeb, 2018).

Gestión de proyectos: en la planificación y ejecución de proyectos de ingeniería civil, los ingenieros deben tomar en consideración los riesgos cibernéticos relacionados con la gestión de datos, la comunicación y la coordinación del proyecto, trabajando en colaboración estrecha con los expertos en el campo de la seguridad de la información (Lavesson, Söderström & Lundqvist, 2018).

Un ciberataque puede tener consecuencias devastadoras, que van desde la fuga de datos sensibles hasta la interrupción total de las operaciones. Los intrusos digitales podrían obtener acceso a secretos corporativos, datos personales de empleados, como nombres, números de seguridad social y detalles bancarios, lo que podría llevar a un robo de identidad. La imagen de la empresa sufriría un golpe severo, afectando la confianza de clientes y socios. Además, las repercusiones financieras podrían ser enormes, incluyendo el costo de detener la producción, enfrentar demandas legales y reparar los daños causados. No es solo un asalto técnico, sino una amenaza real a la integridad y estabilidad de una organización.

En el dinámico mundo de la construcción, el manejo del riesgo cibernético se convierte en un desafío aún mayor. Este aumenta debido a la mezcla de trabajadores temporales y permanentes de diversas compañías que pueden estar realizando trabajos al mismo tiempo, incrementando las posibilidades de brechas de seguridad. A esto se suma la presión por cumplir con los plazos de entrega, lo que puede hacer que la gestión de la seguridad informática pase a un segundo plano. Para salvaguardar la información vital, es esencial limitar el acceso a los sistemas críticos a un círculo reducido y confiable, y establecer políticas, normas y procedimientos de seguridad estrictos, que todos deben seguir al pie de la letra (Alawadhi & Alawadhi, 2020).

En la actualidad, la industria de la ingeniería civil ha experimentado una creciente dependencia de la tecnología y la digitalización. Con el advenimiento de infraestructuras inteligentes y su interconexión, la ciberseguridad se ha elevado a un aspecto crítico. Es esencial que, mientras se avanza hacia un futuro más conectado, se ponga igual énfasis en proteger los

sistemas contra las amenazas digitales que emergen junto con estas nuevas oportunidades tecnológicas. Dentro de los riesgos más significativos a tomar en consideración destacan:

Riesgo de interrupción de infraestructuras críticas: las infraestructuras críticas, cada vez están más interconectadas y dependen de las tecnologías de la información y la comunicación. Los ataques cibernéticos pueden interrumpir o dañar severamente estas infraestructuras, lo que podría tener consecuencias devastadoras para la sociedad y la economía.

Riesgo de robo o manipulación de datos: el manejo de grandes cantidades de datos, incluidos diseños, planos, informes y datos de los sistemas de control, pueden ser hurtados o manipulados para obtener ventajas competitivas, causar daños o incluso poner en peligro la seguridad de las infraestructuras. (Cui & Wu, 2018).

Riesgo de compromiso de la seguridad de la información confidencial: se manejan datos confidenciales, como contratos, información financiera y datos personales. El acceso no autorizado a esta información puede ocasionar pérdidas económicas, daño a la reputación y riesgos legales.

Riesgo de ataques dirigidos a proveedores y contratistas: involucra múltiples proveedores y contratistas y los ciberdelincuentes pueden atacar a la cadena más débil para obtener acceso a los sistemas y datos de las organizaciones principales, lo que puede llevar a comprometer la seguridad de manera significativa (Huang & Zhang, 2020).

Riesgo de falta de conciencia y capacitación en seguridad cibernética: esta falta entre los profesionales de la ingeniería civil expone a las organizaciones a riesgos de caer en trampas de phishing, utilizar contraseñas débiles o no seguir las mejores prácticas de seguridad, lo que aumenta la vulnerabilidad de los sistemas y datos.

Tomando en consideración los riesgos mencionados, se pueden resumir los tipos más comunes de ataques de seguridad dentro de la ingeniería civil en los siguientes:

Phishing: pretenden engañar a las personas para que suministren información confidencial, como lo son las contraseñas o datos de tarjetas de crédito. Los ingenieros civiles pueden ser objeto de estos ataques a través de correos electrónicos falsificados o sitios web fraudulentos que imitan a organizaciones legítimas (Hadžiosmanović & Čaušević, 2019).

Malware: conocido también como software malicioso, está diseñado para dañar, acceder de manera no autorizada o controlar sistemas informáticos cuando estos archivos infectados son descargados o se visitan sitios web comprometidos que contienen dichos programas (Alazab, Venkatraman & Valli, 2017).

Ransomware: es un tipo de malware que cifra los archivos de una computadora o sistema y exige un rescate para restaurar el acceso a los datos. Si los ingenieros civiles no tienen medidas de seguridad adecuadas, pueden ser víctimas de ataques de ransomware que afecten a su trabajo, como la pérdida de diseños, planos o documentos críticos (Baryamureeba & Tushabe, 2018).

Ataques de inyección de código: implica la inserción de código malicioso en una aplicación o sistema para obtener acceso y llevar a cabo actividades dañinas. Un ataque de inyección de código podría dirigirse a los sistemas de control de infraestructuras críticas,

permitiendo a los atacantes tomar el control de los mismos (Alrawi, Alrawi & Mohammed, 2020).

Amenazas internas: pueden provenir de personas dentro de las propias organizaciones responsables de las infraestructuras críticas. Los empleados descontentos, los contratistas o los proveedores de servicios con acceso a los sistemas pueden representar una amenaza significativa si abusan de sus privilegios de acceso (Choudhary & Verma, 2019).

Vulnerabilidades en software y sistemas operativos: las infraestructuras críticas a menudo dependen de software y sistemas operativos para su funcionamiento. Las vulnerabilidades en estos componentes pueden ser explotadas por los atacantes para comprometer la seguridad de las infraestructuras (Bhattacharya & Chakraborty, 2019).

Ataques de denegación de servicio (DDoS): buscan inundar un sistema o red con tráfico malicioso para sobrecargarlo y hacerlo inaccesible para los usuarios legítimos. En el contexto de la ingeniería civil, esto podría afectar a los sistemas de gestión de proyectos, comunicaciones o incluso sistemas de control de infraestructuras críticas causando la interrupción del servicio de suministros esenciales (Li & Chen, 2018).

Ingeniería social: este ataque se basa en la manipulación psicológica para engañar a las personas y obtener acceso no autorizado a información confidencial o sistemas a través de llamadas telefónicas fraudulentas, correos electrónicos engañosos o incluso interacciones en persona. Esto puede incluir técnicas como el phishing, el spear phishing y la suplantación de identidad (Bada & Bhavsar, 2020).

Cabe destacar que estas amenazas cibernéticas están en constante evolución. Los ciberdelincuentes buscan nuevas formas de atacar las infraestructuras críticas, por lo que es fundamental mantenerse actualizado sobre las últimas tendencias y adoptar medidas de seguridad adecuadas para proteger estas infraestructuras.

La seguridad informática, en la ingeniería civil, se basa en minimizar los riesgos que puedan existir tanto en los accesos como en el uso indebido de la información, usando procedimientos de medidas preventivas para así de esta manera poder protegerse contra los ataques y evitar el reemplazo, la alteración y/o modificación de la información que esta almacenada (Sumba Fajardo, 2022).

Protección de infraestructuras críticas

Al hablar de infraestructuras críticas en el contexto de la ingeniería civil, se hace referencia a aquellas que son activos esenciales para el funcionamiento de una sociedad, como los sistemas de energía, sistemas de transporte, sistemas de suministro de agua y comunicaciones. Estas infraestructuras están cada vez más interconectadas y dependen de tecnologías de la información y la comunicación (TIC) para su operación eficiente. Sin embargo, esta creciente interconexión también aumenta la exposición a los riesgos cibernéticos y las amenazas para la seguridad.

Según el Departamento de Seguridad Nacional de los Estados Unidos, "la infraestructura crítica es el conjunto de sistemas y redes, tanto físicos como virtuales, que son esenciales para el funcionamiento continuo de la economía y la sociedad". La protección de estas infraestructuras

críticas es esencial para garantizar la seguridad y el bienestar de la sociedad (Departamento de Seguridad Nacional de los Estados Unidos, 2013)

En la ingeniería civil, la protección de estas infraestructuras es un tema complejo que requiere una comprensión profunda de los riesgos y amenazas a los que se enfrentan estas estructuras. Asegurar que se implementen medidas de protección cibernética con el fin de resguardarlas es fundamental para garantizar la seguridad, la integridad y el funcionamiento confiable de los sistemas, así como para prevenir el impacto negativo en la sociedad y la economía (Sevillano, 2021; Organización Internacional de Normalización, 2018). Existen varias infraestructuras críticas:

Sistemas de control de tráfico: como los semáforos y los sistemas de gestión del tráfico, son vitales para la seguridad y la eficiencia del transporte. Un ataque cibernético podría interrumpir la operación de estos sistemas, causando congestión, accidentes o incluso el colapso completo del tráfico.

Redes de suministro de agua: son fundamentales para la vida diaria en las ciudades, un ataque cibernético dirigido a estas redes podría comprometer la calidad del agua, interrumpir el suministro o causar daños a las infraestructuras físicas, como las estaciones de bombeo.

Redes eléctricas: éstas son esenciales para el funcionamiento de todas las demás infraestructuras críticas. Su interrupción podría provocar apagones masivos y prolongados, afectando no solo a los hogares y las empresas, sino también a los servicios de emergencia y la infraestructura de comunicaciones.

Puentes y estructuras de transporte: podría poner en peligro la seguridad de las personas que los utilizan y causar daños significativos a la infraestructura.

Sistemas de comunicación: como las redes de telecomunicaciones y los sistemas de radio, son cruciales para las operaciones de emergencia, la coordinación de respuesta a desastres y la comunicación en general, interrumpir estos sistemas, podrían poner en dificultad la coordinación y la respuesta efectiva.

Instalaciones de tratamiento de aguas residuales: son responsables de procesar y eliminar de manera segura los desechos líquidos de las comunidades. Un ataque cibernético podría afectar la operación de estas instalaciones, pudiendo resultar en contaminación del agua y riesgos para la salud pública.

Según informe de Trend Micro (2019), destaca que los ataques a la infraestructura crítica se han convertido en una importante preocupación para los gobiernos y proveedores privados de todo el mundo. La vulnerabilidad de estas estructuras se debe a factores como sistemas anticuados, hardware en desuso, fallos de seguridad intrínsecos, el incremento de dispositivos interconectados, la falta de preparación y conciencia, así como a regulaciones más estricta. Además, la seguridad cibernética no solo se trata de proteger los sistemas informáticos, sino también implica resguardar los datos confidenciales de los clientes y planos de diseño, para ello es crucial implementar políticas de seguridad de la información bien definidas y garantizar su cumplimiento organizacional.

El Instituto de Ingenieros Civiles de los Estados Unidos (2018), señala que la defensa de infraestructuras críticas en la ingeniería civil demanda un esfuerzo conjunto entre ingenieros, especialistas en ciberseguridad, tomadores de decisiones y organismos estatales. La sinergia

entre distintas entidades y agencias gubernamentales asegura la integridad de estas infraestructuras frente a amenazas cibernéticas.

Para garantizar una protección efectiva, se requiere adoptar un conjunto de medidas y estrategias diseñadas para prevenir, identificar, mitigar y recuperarse de los incidentes cibernéticos (Organización de las Naciones Unidas, 2021; Organización Internacional de Normalización, 2018). Entre las consideraciones elementales en la protección de infraestructuras críticas en el campo de la ingeniería civil, destacan::

Evaluación de riesgos: implica identificar las vulnerabilidades y amenazas potenciales antes de que se materialicen, de modo de evaluar el impacto que los ataques cibernéticos podrían tener en la infraestructura y en la sociedad en general.

Diseño seguro: al diseñar nuevas infraestructuras o realizar mejoras en las existentes, hay que considerar la seguridad cibernética desde el principio. Esto lleva a incorporar medidas de seguridad en el diseño de los sistemas, como la segmentación de redes, la autenticación de usuarios, el cifrado de datos y la resistencia a ataques conocidos.

Protección de datos: incluye el cifrado de datos confidenciales, la implementación de políticas de gestión de datos seguras, la realización de copias de seguridad y la recuperación de datos en caso de un ataque cibernético.

Control de acceso: implementar medidas de autenticación fuertes, como la autenticación de dos factores, y limitar el acceso solo a las personas autorizadas.

Monitoreo y detección de amenazas en tiempo real: para identificar y responder rápidamente a los ataques cibernéticos, esto incluye el uso de sistemas de detección de intrusiones, análisis de registros de eventos y sistemas de alerta temprana.

Respuesta y recuperación: lleva a establecer protocolos claros y ensayados para actuar rápidamente en caso de un ataque, mitigar el impacto y restaurar la funcionalidad de las infraestructuras afectadas, para restaurar los sistemas y operaciones con la menor interrupción posible tras un incidente.

Concienciación y capacitación: involucra a todos los actores implicados en la protección de infraestructuras críticas, entre ellos a los profesionales de la ingeniería civil, al personal de operación y mantenimiento, y a los usuarios finales. La educación en seguridad cibernética puede ayudar a prevenir incidentes y mejorar la respuesta en caso de un ataque.

Nuevas tecnologías para prevenir ciberataques a las infraestructuras críticas en la ingeniería civil

En la era digital, salvaguardar las infraestructuras críticas de la ingeniería civil de los ciberataques es decisivo. Por suerte, hay tecnologías innovadoras y métodos avanzados que ofrecen nuevas formas para proteger y mitigar estos riesgos. Entre las tecnologías emergentes que están reforzando la ciberseguridad en este campo se incluyen:

Arquitecturas de sistema modular: permiten que los sistemas de infraestructura crítica se dividan en componentes más pequeños y manejables, lo que hace que sea más fácil detectar y responder a los ciberataques (Hartmann & Broy, 2019).

Seguridad por diseño: se promueve la incorporación de la seguridad desde las etapas iniciales de diseño de las infraestructuras críticas. Esto implica considerar los aspectos de seguridad cibernética desde el principio y diseñar sistemas y redes con una arquitectura segura.

Enfoque de "confianza cero": implica que no se confía en ningún usuario o dispositivo hasta que se haya verificado su identidad y se haya comprobado que es seguro (Hartmann & Broy, 2019).

Sistemas de inspección de infraestructuras basados en fotografías: utilizan tecnología de inteligencia artificial para detectar anomalías en las infraestructuras críticas, lo que puede ayudar a prevenir los ciberataques (Hartmann & Broy, 2019).

Sistemas de protección de red: pueden ayudar a prevenir los ciberataques mediante la detección y el bloqueo de tráfico malicioso (Kaur, Singh & Lamba, 2019).

Colaboración entre organizaciones: la colaboración entre diferentes organizaciones y agencias gubernamentales es esencial para garantizar una respuesta coordinada y efectiva a los posibles ataques (Kaur, Singh & Lamba, 2019).

Colaboración y compartición de información: permite una respuesta más rápida y eficiente ante las amenazas cibernéticas y promueve la adopción de medidas de seguridad efectivas en toda la industria.

Sistemas de autenticación de usuarios: previenen los ciberataques mediante la verificación de la identidad de los usuarios y la comprobación de que tienen permiso para acceder a los sistemas de infraestructura crítica (Cherdantseva, Burnap, Blyth & Eden, 2018).

Sistemas de encriptación de datos: ayudan a prevenir los ciberataques mediante la protección de la información confidencial de los clientes y los datos de diseño

Seguridad defensiva en profundidad: esta estrategia utiliza múltiples capas de defensa para proteger las infraestructuras críticas, puede incluir firewalls, sistemas de detección y prevención de intrusiones, cifrado de datos, entre otros.

Sistemas de capacitación en seguridad cibernética: previenen los ciberataques mediante la educación del personal en las mejores prácticas de seguridad cibernética y puedan así identificar posibles amenazas crítica (Cherdantseva, Burnap, Blyth & Eden, 2018).

La tecnología por sí sola no es suficiente para prevenir los ciberataques a las infraestructuras críticas en la ingeniería civil. Contar con la existencia de políticas de seguridad de la información bien definidas y su estricta aplicación en todos los niveles de la organización es igualmente vital. Además, la protección eficaz de estas infraestructuras requiere una colaboración sin fisuras entre diversas entidades y organismos gubernamentales, asegurando así un frente unido contra las amenazas cibernéticas en el ámbito de la ingeniería civil.

En la actualidad, se están desarrollando y utilizando nuevos modos de protección para prevenir los ciberataques a las infraestructuras críticas en la ingeniería civil. Algunas de estas medidas incluyen:

Internet de las cosas (IoT): permite la conexión y comunicación de dispositivos y sistemas en tiempo real. En el contexto de la ingeniería civil, el IoT se utiliza para monitorear y controlar las infraestructuras críticas, como puentes, túneles y sistemas de suministro de agua. Al

implementar sensores y dispositivos conectados, es posible recopilar datos en tiempo real sobre el estado de la infraestructura y detectar anomalías o posibles amenazas. Esto ayuda a prevenir ciberataques al proporcionar una visibilidad y supervisión mejoradas de los sistemas críticos. De acuerdo a un trabajo realizado por Li et al. (2019), la implementación de tecnologías IoT en infraestructuras críticas ha demostrado ser eficaz para mejorar la detección y respuesta ante posibles amenazas cibernéticas. Además, el informe de la Comisión de Infraestructura Crítica de los Estados Unidos (2018) resalta la importancia de utilizar dispositivos IoT seguros y robustos para garantizar la integridad y confiabilidad de las infraestructuras críticas.

Sistemas de detección y respuesta automatizados (ADRS): utilizan algoritmos y técnicas avanzadas de análisis de datos para detectar y responder automáticamente a las amenazas cibernéticas en tiempo real. Estos sistemas monitorean constantemente las redes y sistemas, identifican patrones de comportamiento sospechosos y generan alertas en caso de actividad maliciosa. Pueden tomar medidas preventivas para detener o mitigar los ataques. Según el informe de la Agencia de Seguridad Cibernética y de Infraestructura (CISA) de los Estados Unidos (2020), los sistemas ADRS son una herramienta efectiva para proteger las infraestructuras críticas contra los ciberataques. Estos sistemas permiten una respuesta más rápida y automatizada, lo que reduce el tiempo de detección y mitigación de los ataques, minimizando así el impacto en la infraestructura.

Blockchain: la tecnología blockchain proporciona una plataforma segura y descentralizada para el almacenamiento y la transmisión de datos. En el contexto, puede utilizarse para garantizar la integridad de los registros y transacciones relacionadas con las infraestructuras críticas. Al utilizar la criptografía y la distribución de nodos, blockchain ofrece un alto nivel de seguridad y transparencia, lo que dificulta la manipulación de datos y asegura la confiabilidad de la información. El estudio de Wang et al. (2018) afirma que, la tecnología blockchain puede desempeñar un papel crucial en la protección de las infraestructuras críticas contra los ciberataques, especialmente en la gestión de identidad y acceso, el seguimiento de cambios en los sistemas y la verificación de la integridad de los datos.

Análisis de big data: implica la recopilación, procesamiento y análisis de grandes volúmenes de datos para obtener información y patrones significativos. El análisis de big data puede ayudar a identificar anomalías, detectar amenazas emergentes y prevenir ataques antes de que ocurran. Al combinar datos de diferentes fuentes, como registros de eventos, tráfico de red y datos de sensores, se pueden obtener insights valiosos para fortalecer la seguridad de las infraestructuras críticas. El informe de la Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de los Estados Unidos (2019) indica que, el análisis de big data desempeña un papel crucial en la identificación temprana de amenazas cibernéticas y la toma de decisiones informadas para proteger las infraestructuras críticas.

Inteligencia Artificial (IA) y Aprendizaje Automático (Machine Learning): son utilizados para analizar y detectar patrones de comportamiento maliciosos en los sistemas de infraestructuras críticas. Estas tecnologías pueden identificar anomalías y actividades sospechosas en tiempo real, lo que permite una respuesta más rápida y eficiente ante posibles ciberataques. Además, pueden mejorar la capacidad de detección de amenazas al adaptarse y aprender de los nuevos ataques y técnicas utilizadas por los ciberdelincuentes (Chui & Manyika, 2017).

Virtualización y contenedores: permiten crear entornos virtualizados para ejecutar aplicaciones y sistemas de forma aislada. Estas tecnologías contribuyen a mejorar la seguridad de las infraestructuras críticas al proporcionar una separación entre los sistemas críticos y las aplicaciones potencialmente inseguras. También facilitan la gestión y el despliegue de sistemas, lo que permite una implementación más rápida de parches y actualizaciones de seguridad (Li, Qian & Li, 2020).

Seguridad definida por software: implica la implementación de políticas y medidas de seguridad a través de software y algoritmos en lugar de depender exclusivamente de hardware dedicado. Esta tecnología permite una mayor flexibilidad y adaptabilidad en la implementación de medidas de seguridad en las infraestructuras críticas de la ingeniería civil. Facilita también la gestión centralizada de la seguridad y la implementación de políticas de seguridad coherentes en todos los sistemas y componentes (Gritzalis, Katos & Stergiopoulos, 2019).

Autenticación multifactor (MFA): es una técnica que requiere múltiples formas de autenticación para acceder a sistemas críticos. En conjunto con la tradicional contraseña, se pueden utilizar factores adicionales como tarjetas inteligentes, tokens de seguridad, huellas dactilares o reconocimiento facial. La MFA proporciona una capa adicional de seguridad, ya que incluso si una credencial es comprometida, el acceso al sistema seguirá siendo difícil de lograr sin los otros factores de autenticación.

Computación en la nube segura: ampliamente adoptada en la ingeniería civil debido a sus ventajas en términos de escalabilidad y flexibilidad. Sin embargo, la seguridad en la nube es una preocupación importante. Por lo tanto, se están desarrollando tecnologías y prácticas de seguridad específicas para garantizar la protección de los datos y sistemas en la nube. Esto incluye el cifrado de datos, la segmentación de redes, la autenticación fuerte y la monitorización continua de la seguridad (Mell & Grance, 2011).

Sistemas de detección y respuesta automatizados (EDR): estos sistemas utilizan algoritmos y técnicas avanzadas de machine learning para monitorear continuamente los sistemas y detectar actividades maliciosas en tiempo real. Pueden identificar patrones de comportamiento sospechosos y responder automáticamente para mitigar o detener un ataque (Sood & Bharadwaj, 2019).

Análisis de comportamiento de usuarios (UBA): esta tecnología analiza el comportamiento normal de los usuarios autorizados en los sistemas y redes de infraestructuras críticas. Con base en este análisis, puede identificar comportamientos anómalos que podrían indicar un compromiso o una actividad maliciosa.

basada en el comportamiento (BDS): utiliza análisis avanzados para detectar patrones de comportamiento anormal en los sistemas y redes. Identifica actividad sospechosa en tiempo real y tomar medidas para prevenir un ataque antes de que cause daño.

Es importante considerar que la implementación de estas tecnologías debe hacerse de manera segura, teniendo en cuenta las necesidades y características específicas de cada infraestructura crítica y siguiendo las mejores prácticas de ciberseguridad. Además, se requiere una planificación cuidadosa, una gestión de riesgo efectiva y una colaboración estrecha entre los profesionales capacitados en ciberseguridad y la ingeniería civil, y mantenerse al día sobre las últimas tendencias y amenazas en este campo en constante cambio.

Seguridad en sistemas de control industrial

Los sistemas de control industrial (ICS) están conformados por un conjunto de dispositivos electrónicos e informáticos que permiten la supervisión, control y automatización de procesos industriales. En la era de la automatización y la Industria 4.0, son fundamentales ya que revolucionan la forma en la que las industrias producen, mejorando la eficiencia, la calidad de los productos y la seguridad de las plantas y procesos (Galloway & Aravind, 2019b; Laing & Bresnahan, 2018). Existen varios tipos de ICS, incluyendo:

Controladores lógicos programables (PLC): utilizados para automatizar procesos específicos como el control de motores, válvulas y sensores.

Sistemas de control distribuido (DCS): diseñados para controlar procesos continuos y complejos, como los de plantas químicas y refinerías.

Sistemas de control de supervisión y adquisición de datos (SCADA): Permiten a los operadores supervisar y controlar procesos industriales de forma remota.

Estos sistemas son altamente confiables y se implementan para garantizar la eficiencia operativa, reducir costos de producción y minimizar errores humanos (Powell, 2017). Dichos sistemas, que utilizan tecnologías de automatización y control para supervisar y operar equipos y procesos industriales, se ven enfrentados a numerosas amenazas cibernéticas que podrían desencadenar efectos devastadores, tanto en términos de seguridad como de integridad operativa.

De acuerdo con un informe de la firma de seguridad cibernética Kaspersky (2019), se ha registrado un incremento significativo en el número de ciberataques dirigidos a sistemas de control industrial en los últimos años. Estos ataques pueden acarrear graves repercusiones para estos sistemas, por ejemplo, un ataque podría provocar la interrupción de la producción, teniendo un impacto considerablemente en la economía, o incluso podría provocar la liberación de sustancias peligrosas, lo que tendría un impacto en la salud pública.

Según el Instituto de Ingenieros Civiles de los Estados Unidos (2018), la seguridad en sistemas de control industrial requiere la colaboración estrecha entre los ingenieros civiles, expertos en seguridad cibernética, los responsables de la toma de decisiones y las agencias gubernamentales.

La cooperación entre diferentes organizaciones y entidades gubernamentales garantiza la seguridad en sistemas de control industrial, pues se trata de un asunto de importancia que demanda un entendimiento exhaustivo de los riesgos y amenazas que acechan a dichos sistemas. Es imperativo implementar medidas de seguridad adecuadas, fomentar la cooperación interorganizacional y gubernamental, y disponer de políticas transparentes y bien definidas en materia de seguridad de la información para preservar la integridad de los sistemas de control industrial.

Desafíos de la seguridad en ICS

Los desafíos se presentan debido a la complejidad de los sistemas de control, su interconexión con redes de información y una falta de conciencia y capacitación en seguridad cibernética dentro del industrial. Para abordar estas problemáticas, se hace necesario implementar estrategias integrales de seguridad que involucren tanto aspectos técnicos como organizacionales. Esto incluye el uso de sistemas de detección y prevención de intrusiones, la

segmentación de redes, la autenticación fuerte, la actualización regular de software y la capacitación continua del personal en materia de seguridad cibernética. Al mismo tiempo, es crucial la colaboración intersectorial entre la industria, el gobierno y el ámbito académico para intercambiar buenas prácticas, investigar amenazas emergentes y desarrollar soluciones efectivas. Mediante estos esfuerzos conjuntos, se logrará reforzar la seguridad de los sistemas de control industrial y garantizar la integridad y disponibilidad de las infraestructuras críticas que de ellos dependen.

Los desafíos que enfrentan los ICS son únicos en términos de seguridad, e incluyen:

Requisitos de alta disponibilidad: los ICS en infraestructuras críticas y manufactura, no pueden ser detenidos para instalar actualizaciones de seguridad, lo que hace difícil su protección.

Protocolos inseguros y propietarios: muchos protocolos utilizados en ICS carecen de funciones de seguridad básicos como cifrados y control de accesos, sin poder ser actualizados de una manera fácil.

Enfoque en la detección sobre prevención: debido a la necesidad de alta disponibilidad, la seguridad en ICS es configurada para detectar ataques en lugar de prevenirlos.

Amenazas en Seguridad de ICS

Son diversas las amenazas que enfrentan los sistemas de control industrial y pueden tener graves consecuencias para estos sistemas, dentro de las principales amenazas se mencionan:

Amenazas internas: provienen de personas dentro de la organización, como empleados descontentos, contratistas o proveedores de servicios con acceso privilegiado. Pueden ser intencionales o no intencionales, y pueden incluir acciones maliciosas, negligencia o falta de capacitación adecuada en seguridad (Lee & Lee, 2019).

Ataques de malware y ransomware: los ciberdelincuentes intentan infiltrarse en los sistemas y cifrar los datos o manipular los procesos para obtener un rescate. Estos ataques pueden paralizar las operaciones y resultar en pérdidas financieras significativas.

Ataques de denegación de servicio (DDoS): inundan los sistemas y redes con tráfico malicioso, lo que provoca una interrupción en los servicios y afecta la disponibilidad de los sistemas de control industrial. Estos ataques pueden tener un impacto grave en la continuidad del negocio.

Ingeniería social: Los ataques de ingeniería social implican el engaño de los usuarios o del personal autorizado para obtener acceso no autorizado a los sistemas de control industrial. Esto incluye técnicas de phishing, spear phishing, suplantación de identidad y otras tácticas de manipulación psicológica. La ingeniería social es una de las amenazas más difíciles de detectar prevenir, ya que utiliza la confianza y la falta de conciencia de los usuarios (Hadžiosmanović & Boleng, 2018).

Conectividad y exposición a Internet: a medida que los sistemas de control industrial se vuelven más conectados y se integran con redes empresariales y de Internet, aumenta su exposición a amenazas externas. La conectividad puede facilitar el acceso no autorizado a los sistemas y abrir puertas a ataques cibernéticos. Una red sobrecargada, la pérdida de conectividad o un ataque DDoS pueden romper la cadena de control, causando una interrupción inesperada,

que puede comprometer la instalación, destruir la productividad o incluso causar problemas más graves (impactos ambientales o riesgos humanos) (Tan & Hossain, 2018).

Falta de actualizaciones y parches: diversos sistemas de control industrial operan con software y hardware heredados que pueden tener vulnerabilidades conocidas. La falta de actualizaciones y parches de seguridad deja estos sistemas expuestos a ataques que aprovechan estas vulnerabilidades conocidas (Kohn & Fung, 2017).

Falta de conciencia y capacitación en seguridad: los ataques exitosos a menudo se basan en la falta de conocimiento de los usuarios sobre las mejores prácticas de seguridad y las técnicas de ingeniería social.

Soluciones para la seguridad en ICS

Para superar estos desafíos, se requieren soluciones de seguridad diseñadas para operar en el entorno único de los ICS, (Stouffer et al, 2011; ISO, 2020), que incluyen:

Medidas de seguridad física y cibernética: es importante proteger los ICS contra ataques sin interrumpir las operaciones normales.

Normativas y estándares: organismos como la Comisión Electrotécnica Internacional (IEC) y la Organización Internacional de Normalización (ISO) han desarrollado normas específicas para la seguridad en ICS.

Conciencia y formación: es esencial que los operadores y personal de seguridad estén bien informados y entrenados en las mejores prácticas de seguridad en ICS.

Ciberseguridad en Proyectos de Construcción y Gestión de Activos.

Los proyectos de construcción y la gestión de activos implican el uso de tecnología, sistemas de información y comunicaciones para planificar, diseñar, construir, operar y mantener infraestructuras y activos. Estos proyectos y activos pueden incluir edificios, puentes, carreteras, sistemas de energía, redes de telecomunicaciones y sistemas de transporte, entre otros. A medida que estos sistemas se vuelven más complejos y conectados, se vuelven más vulnerables a las amenazas digitales. Algunas de las amenazas específicas incluyen:

Ataques de denegación de servicio (DDoS): pueden causar la caída de servicios críticos, lo que se traduce en costos adicionales y perjuicios a la imagen de la empresa.

Infiltración de sistemas: da acceso ilícito a los datos sensibles y la información comercialmente confidencial, desde planos arquitectónicos hasta información personal de los trabajadores.

Robo de identidades: permite a los atacantes obtener acceso ilícito a los sistemas y realizar acciones malintencionadas.

Extorsión: los atacantes pueden extorsionar a las empresas con la promesa de revelar información sensible si no pagan un rescate.

Según Galloway y Aravind (2019), la ciberseguridad en proyectos de construcción y gestión de activos es esencial para prevenir ataques cibernéticos que podrían comprometer la integridad, la confidencialidad y la disponibilidad de los sistemas. Destaca la importancia de adoptar un enfoque integral desde las etapas iniciales de diseño hasta la fase de funcionamiento y mantenimiento. Es así que realizar evaluaciones de riesgos y pruebas de penetración en los

sistemas tecnológicos utilizados en estos proyectos, ayudan a identificar posibles brechas de seguridad y permiten implementar medidas adecuadas para proteger los activos (Lee & Lee, 2019).

Los sistemas de gestión de activos deben contar con mecanismos de seguridad robustos, como controles de acceso y sistemas de detección de intrusiones, para salvaguardar la información sensible y prevenir ataques cibernéticos (Laing y Bresnahan, 2018). La educación sobre las mejores prácticas de seguridad cibernética es esencial para garantizar que los empleados estén preparados y sean conscientes de los riesgos y las medidas de protección (Powell, 2017). Dentro de las medidas de seguridad adecuadas en proyectos de construcción y la gestión de activos, destacan:

Implementación de firewalls: pueden limitar el acceso a los recursos internos y proteger los sistemas de los ataques externos.

Encryptación de datos: evita que los datos sensibles sean leídos o copiados por los atacantes.

Autenticación multifactor: reduce la probabilidad de que los atacantes logren acceder a los sistemas.

Capacitación del personal: mejora la consciencia de la seguridad y reduce la probabilidad de errores humanos.

Políticas de seguridad de la información: pueden definir cómo se manejarán los datos sensibles y la información comercialmente confidencial.

La colaboración interorganizacional y con agencias gubernamentales, como la iniciativa del Departamento de Seguridad Nacional de EEUU (2013), con el Programa Nacional de Protección de Infraestructuras Críticas (NIPP), es importante para la ciberseguridad en la construcción y gestión de activos. Esta sinergia, junto con políticas de seguridad de la información bien definida y medida de protección robustas, forma una estrategia integral que reduce los riesgos de ciberataques y asegura la integridad de dichos proyectos.

Desafíos y medidas de ciberseguridad en proyectos de construcción y gestión de activos

Estos desafíos requieren una atención especializada y medidas de protección adaptadas y abarcan desde la protección de datos sensibles y propiedad intelectual hasta la seguridad de los sistemas de control industrial y la infraestructura de red. La naturaleza dinámica de los sitios de construcción, junto con la diversidad de tecnologías y la participación de múltiples partes interesadas, aumenta la complejidad de implementar estrategias de ciberseguridad efectivas. Algunos de estos:

Integración de sistemas antiguos y modernos: muchos proyectos de construcción y la gestión de activos utilizan sistemas informáticos antiguos que no están optimizados para la seguridad cibernética.

Gran cantidad de dispositivos conectados: suelen involucrar una gran cantidad de dispositivos conectados, lo que incrementa la superficie de ataque potencial.

Compartimiento de redes: a menudo comparten redes con terceros, lo que aumenta la probabilidad de que los atacantes logren acceder a los sistemas.

Trabajo remoto y teletrabajo: utilizan equipos portátiles y herramientas de trabajo remoto, lo que aumenta la probabilidad de que los atacantes logren acceder a los sistemas.

Para abordar estos desafíos, se requiere adaptar las medidas tradicionales de seguridad cibernética a los contextos específicos de los proyectos de construcción y la gestión de activos (ENISA, 2019; NIST, 2018; ISO, 2019), entre las que se incluyen:

Segmentación de redes: puede reducir la superficie de ataque potencial y hacer más difícil para los atacantes lograr acceder a los sistemas.

Monitorización continua: ayuda a detectar y responder a los posibles ataques antes de que sean demasiado dañinos.

Gestión de riesgos: identifica y anticipa los riesgos de seguridad cibernética desarrollando medidas preventivas, correctivas y recuperativas.

Auditorías periódicas: pueden ayudar a identificar deficiencias en la seguridad cibernética y desarrollar planes de corrección.

Evaluación de riesgos: las evaluaciones periódicas permite tomar medidas proactivas para mitigar los riesgos identificados.

Políticas de seguridad: que aborden aspectos como el acceso y la gestión de contraseñas, la protección de datos, la gestión de parches y actualizaciones, y la respuesta a incidentes.

Protección de datos: implementar medidas de protección de datos, como el cifrado de datos confidenciales, controles de acceso adecuados, realizar copias de seguridad regulares para garantizar la disponibilidad y recuperación de la información en caso de un incidente.

Seguridad en la cadena de suministro: encierra la evaluación de la seguridad de los proveedores, la firma de acuerdos de confidencialidad y la implementación de controles de seguridad en la cadena de suministro.

Concientización y capacitación: incluye la capacitación en la detección de ataques de ingeniería social, el reconocimiento de correos electrónicos y enlaces sospechosos, y la adopción de prácticas seguras de navegación y uso de dispositivos.

Monitorización y detección de amenazas: pueden ayudar a identificar y responder rápidamente a los ataques, minimizando el impacto y acelerando la recuperación.

Plan de respuesta a incidentes: se fundamenta en designar un equipo de respuesta a incidentes, la notificación de las partes afectadas, la contención del incidente y la recuperación de los sistemas.

Ahora bien, para abordar todos los desafíos y poder aplicar las medidas de seguridad, se debe capacitar a todo el personal de modo que sean capaces de reconocer y actuar ante las amenazas cibernéticas. Dentro de las muchas estrategias para capacitar a los equipos de trabajo en ciberseguridad, se mencionan:

Desarrollar una cultura de seguridad: los empleados deben entender la importancia de la seguridad cibernética y cómo sus acciones pueden afectar la seguridad de la empresa. La alta

dirección debe liderar el camino en la creación de una cultura de seguridad y fomentar la participación de todos los empleados (ENISA, 2020).

Proporcionar capacitación básica en seguridad: todos los empleados, independientemente de su papel en la empresa, deben recibir capacitación básica en seguridad. Esto asegura que todos estén en la misma página cuando se trata de la seguridad cibernética.

Proporcionar capacitación continua: la capacitación en seguridad no es un evento único. Es importante proporcionar capacitación y educación continuas para mantener a los empleados actualizados sobre las últimas amenazas y tendencias de seguridad cibernética (ISACA, 2019).

Proporcionar capacitación especializada: los diferentes roles de un empleado dentro de la empresa, requieren diferentes tipos de capacitación, especializada en seguridad.

Realizar simulaciones de ataques: las simulaciones de ataques pueden ayudar a los empleados a comprender mejor las amenazas de seguridad cibernética y cómo responder a ellas. Estas simulaciones pueden incluir correos electrónicos de phishing, ataques de ransomware y otros escenarios de ataque (CIS, 2020).

Establecer políticas claras de seguridad de la información: las políticas de seguridad de la información deben definir cómo se manejarán los datos sensibles y la información comercialmente confidencial, el personal debe estar capacitado en estas políticas y entender cómo aplicarlas en su trabajo diario.

Realizar auditorías periódicas: éstas pueden ayudar a identificar deficiencias en la seguridad cibernética y desarrollar planes de corrección, los empleados deben estar capacitados en cómo responder a las auditorías y cómo implementar las recomendaciones de seguridad (CIS, 2020).

Es imperativo que la educación y sensibilización en materia de ciberseguridad se mantengan como foco central para todos aquellos que ejercen en el ámbito de la ingeniería civil. Solo a través de un enfoque proactivo y una cultura de seguridad arraigada, es posible garantizar la resiliencia de nuestras infraestructuras esenciales y de los proyectos de edificación ante los retos cibernéticos emergentes.

La colaboración interdisciplinaria permite forjar estrategias integrales que protejan tanto la seguridad física como la digital. La ciberseguridad no es solo una responsabilidad técnica; es una responsabilidad compartida que requiere la participación activa de cada miembro del equipo de proyecto, desde los ingenieros hasta los operadores en el terreno. Unidos, se está en la capacidad de edificar un entorno más seguro y protegido que favorezca el progreso nuestra sociedad.

Referencias Bibliográficas

Agencia de Proyectos de Investigación Avanzados de Defensa (DARPA) de los Estados Unidos. (2019). Big Data for Cybersecurity. Recuperado de https://www.darpa.mil/attachments/BigDataforCybersecurity.pdf

Agencia de Seguridad Cibernética y de Infraestructura (CISA) de los Estados Unidos. (2020). Automated Driving Systems Cybersecurity Best Practices. Recuperado de https://www.cisa.gov/sites/default/files/publications/CISA_Automated_Driving_Systems_Cybersecurity_Best_Practices_508C.pdf

Alawadhi, A., & Alawadhi, S. (2020). Cybersecurity Awareness and Practices in the Construction Industry: A Review. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). https://doi.org/10.1109/ICCAIS49741.2020.9254851

Alazab, M., Venkatraman, S., & Valli, C. (2017). Malware Detection Techniques: A Brief Survey. In 2017 Tenth International Conference on Contemporary Computing (IC3) (pp. 1-6). https://doi.org/10.1109/IC3.2017.8280379

Aloulou, M. A., & Meddeb, A. (2018). Cybersecurity in Smart Buildings: Challenges and Solutions. In 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) (pp. 1-6). https://doi.org/10.1109/CCNC.2018.8319269

Alrawi, O. N., Alrawi, A. N., & Mohammed, A. A. (2020). Code Injection Attacks and Defenses: A Review. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). https://doi.org/10.1109/ICCAIS49741.2020.9254837

Bada, M., & Bhavsar, A. (2020). Social Engineering Attacks and Countermeasures: A Review. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). https://doi.org/10.1109/ICCAIS49741.2020.9254845

Bhattacharya, S., & Chakraborty, S. (2019). Vulnerability Assessment on Critical Infrastructure Systems: A Review. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-5). https://doi.org/10.1109/ICCCNT.2019.8945123

Baryamureeba, V., & Tushabe, F. (2018). Ransomware Attacks: A Review. In 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-6). https://doi.org/10.1109/icABCD.2018.8402546

Center for Internet Security (CIS). (2020). CIS Controls Implementation Guide for Small and Medium Enterprises. Recuperado de https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-small-and-medium-enterprises/

Cherdantseva, Y., Burnap, P., Blyth, A., & Eden, P. (2018). From Cyber Security to Cyber Resilience: The Next Generation of Critical Infrastructure Protection. In 2018 IEEE International Conference on Big Data (Big Data) (pp. 1671-1679). https://doi.org/10.1109/BigData.2018.8622032

Choudhary, S., & Verma, A. K. (2019). Insider Threats in Critical Infrastructures: A Review. In 2019 IEEE 9th International Advance Computing Conference (IACC) (pp. 127-132). https://doi.org/ 10.1109/IACC48052.2019.8970976

Chui, M., & Manyika, J. (2017). Artificial Intelligence: The Next Digital Frontier? McKinsey Global Institute. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/artificial-intelligence-the-next-digital-frontier

Comisión de Infraestructura Crítica de los Estados Unidos. (2018). Recommendations to Enhance the Cybersecurity and Resilience of the Internet of Things. https://www.dhs.gov/sites/default/files/publications/CISA-IoT-Recommendations-508_0.pdf

Cui, Y., & Wu, P. (2018). Cybersecurity Risk Management for Critical Infrastructures: A Systematic Review. In 2018 14th International Conference on Computational Intelligence and Security (CIS) (pp. 129-133). https://doi.org/0.1109/CIS2018.2018.00034

Departamento de Seguridad Nacional de los Estados Unidos. (2013). National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience. Recuperado de https://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf

ENISA. (European Union Agency for Cybersecurity). (2019). Good practices for security of internet of things in the context of smart manufacturing. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-in-the-context-of-smart-manufacturing

ENISA (European Union Agency for Cybersecurity). (2020). Cybersecurity Culture in Organizations. https://www.enisa.europa.eu/publications/cybersecurity-culture-in-organisations

Galloway, A., & Aravind, P. (2019a). Cybersecurity Challenges for Smart Cities: A Systematic Review. *Journal of Urban Technology*, 26(1), 127-152. https://doi.org/10.1080/10630732.2018.1525268

Galloway, P., & Aravind, P. (2019b). Industrial Control Systems (ICS) Cyber Security: A Review of Technologies and Best Practices. In Proceedings of the International Conference on Smart Systems and Inventive Technology (Vol. 3, pp. 1156-1161). IEEE.

Gritzalis, D., Katos, V., & Stergiopoulos, G. (2019). Software-Defined Security for Critical Infrastructures: A Comprehensive Survey. *IEEE Communications Surveys & Tutorials*, 21(3), 2495-2523. https://doi.org/10.1109/COMST.2019.2909805

Hadžiosmanović, D., & Boleng, J. (2018). Social Engineering Attacks on Industrial Control Systems. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 1500-1505). https://doi.org/10.1109/Cybermatics_2018.2018.00261

Hadžiosmanović, D., & Čaušević, A. (2019). Phishing Attacks Detection: A Survey. In 2019 42nd International Convention on Information and Communication Technology,

Electronics and Microelectronics (MIPRO) (pp. 1134-1139). https://doi.org/10.23919/MIPRO.2019.8756916

Hartmann, T., & Broy, M. (2019). Modular Systems for Critical Infrastructure Protection. In Proceedings of the 22nd International Conference on Fundamental Approaches to Software Engineering (FASE) (pp. 402-420). https://doi.org/10.1007/978-3-030-16722-6_21

Huang, L., & Zhang, Z. (2020). Cybersecurity Risks in Civil Infrastructure Projects: A Systematic Review. In 2020 IEEE 20th International Conference on Software Quality, Reliability and Security (QRS) (pp. 353-360). https://doi.org/10.1109/QRS51245.2020.00060

Instituto de Ingenieros Civiles de los Estados Unidos. (2018). Cybersecurity for Civil Engineers. https://www.asce.org/uploadedFiles/Newsroom/Content_Pieces/ASCE_Cybersecurity_for_Civil_Engineers.pdf

ISACA. (2019). CSX Cybersecurity Fundamentals Study Guide. Recuperado de https://www.isaca.org/-/media/information-security-and-risk-management/csx-cybersecurity-fundamentals-study-guide-3rd-edition-2019-sample-chapter-2.pdf

ISO. (2019). ISO/IEC 27001: Information Technology - Security Techniques - Information Security Management Systems - Requirements. International Organization for Standardization. https://www.iso.org/standard/54534.html

ISO. (2020). ISO/IEC 27002: Information Technology - Security Techniques - Code of Practice for Information Security Controls. International Organization for Standardization. https://www.iso.org/standard/54533.html

Kaur, K., Singh, P., & Lamba, R. (2019). Performance Analysis of Network Intrusion Detection System for Critical Infrastructure Protection. In 2019 IEEE 2nd International Conference on Computing, Communication, and Security (ICCCS) (pp. 1-4). https://doi.org/10.1109/CCCS45614.2019.8941918

Karyotis, V., & Kokolakis, S. (2018). Cybersecurity in Critical Infrastructures: A Review of the Interplay between Technology and Public Policy. *Journal of Information Security and Applications*, 42, 66-77. https://doi.org/10.1016/j.jisa.2018.02.006

Kaspersky. (2019). Threat Landscape for Industrial Automation Systems in H1 2019. https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2019/11/Kaspersky_ICSCERT_Threat_Landscape_for_IAS_H1_2019_EN.pdf

Kohn, R., & Fung, C. (2017). User Awareness and Training in Industrial Control Systems. In 2017 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 360-367). doi: 10.1109/QRS-C.2017.61

Laing, C., & Bresnahan, J. (2018). Industrial Control Systems: Cybersecurity Challenges and Solutions. In Proceedings of the IEEE Industrial Cyber-Physical Systems (ICPS) (pp. 398-403). IEEE.

Lavesson, N., Söderström, E., & Lundqvist, M. (2018). Cybersecurity in Project Management: A Literature Review. In 2018 51st Hawaii International Conference on System Sciences (HICSS) (pp. 2083-2092). https://doi.org/10.24251/HICSS.2018.262

Lee, J., & Lee, J. (2020). Cybersecurity in Industrial Control Systems: A Survey. *IEEE Transactions on Industrial Informatics*, 16(6), 4111-4122.

Lee, J., & Lee, J. (2019). Insider Threats in Industrial Control Systems: A Survey. *IEEE Access,* 7, 1838-1853. https://doi.org/ 10.1109/ACCESS.2018.2887872

Li, B., Zhang, Y., Yu, S., & Tian, H. (2019). A Security Architecture for Internet of Things in Critical Infrastructures. *IEEE Internet of Things Journal*, 6(3), 5330-5341

Li, M., Qian, Y., & Li, J. (2020). Security Challenges and Solutions of Containers in Cloud Computing. In 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA) (pp. 236-240). https://doi.org/10.1109/ICAICA50633.2020.00052

Li, Z., & Chen, B. (2018). A Survey on DDoS Attacks and Their Defense Mechanisms in Cloud Computing. In 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/ 12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (pp. 1659-1665). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00234

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing (NIST Special Publication 800-145). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIPP. (2013). Partnering for Critical Infrastructure Security and Resilience. Recuperado de https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf

NIST. (2018). NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Organización Internacional de Normalización. (2018). ISO/IEC 27001:2013 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos. Recuperado de https://www.iso.org/standard/54534.html

Organización Internacional de Normalización. (2018). ISO 27005:2018 Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información. Recuperado de https://www.iso.org/standard/75281.html

Organización de las Naciones Unidas. (2021). Guía de Ciberseguridad para Infraestructuras Críticas. https://www.un.org/es/observances/critical-infrastructure-cybersecurity

Powell, R. (2017). Industrial Control System Cybersecurity: Effective Practices for Cybersecurity in Industrial Control Systems. *NIST Special Publication*, 800(82), 1-126.

Rau, R., & Carneiro, S. (2019). Cybersecurity in Civil Engineering: A Systematic Literature Review. In 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1-6). https://doi.org/10.1109/ICE.2019.8792851

Sevillano, F. (2021). *Ciberseguridad Industrial e Infraestructuras Críticas*. RA-MA Editorial. ISBN: 978-84-1855-136-9.

Sood, R. K., & Bharadwaj, A. (2019). Automated Threat Detection and Response Framework for Critical Infrastructure Protection. In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) (pp. 1424-1429). https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00231

Stouffer, K., Pillitteri, V., Lightman, S., & Abrams, M. (2011). Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Sumba Fajardo, L.H. (2022). Análisis comparativos de metodologías para pruebas de penetración mediante metodologías Ethicals Hacking. Universidad Técnica de Machala. Trabajo de grado

Tan, K. R., & Hossain, M. A. (2018). Vulnerability Analysis of Industrial Control Systems: A Case Study. In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) (pp. 2016-2020). https://doi.org/10.1109/IEEM.2018.8607547

Trend Micro. (2019). Securing the Connected World: Security Predictions for 2019 and Beyond. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2019

Wang, C., Liu, Z., Jia, Z., Guo, H., & Xiang, Y. (2018). A Blockchain-Based Framework for Ensuring Security and Privacy in Infrastructure-as-a-Service. *IEEE Transactions on Services Computing*, 11(4), 747-759.

María Elena Tasa Catanzaro ✉ 1, **Henry George Maquera Quispe** ✉ 2, **Maycol Junior Baldeon Palpa** ✉ 1, **Ronald Michael Villanueva Añazco** ✉ 1, 3 **& Jorch Coras Bendezú** ✉ 1

1. Universidad Tecnológica del Perú - 2 Universidad Nacional del Centro del Perú - 3 Universidad Continental, Huancayo Perú

La ingeniería de sistemas es el arte de crear y cuidar sistemas complejos, uniendo el mundo del software y el hardware en una sinfonía de tecnología. En el corazón de esta disciplina, la ciberseguridad emerge como un escudo vital, defendiendo nuestros sistemas informáticos y redes contra las sombras de ataques malintencionados y amenazas digitales.

Los ingenieros de sistemas, en su rol de guardianes de la información, tienen la misión crítica de blindar la organización. Implementan bastiones de seguridad como firewalls y sistemas de detección de intrusiones, y son los maestros de la autenticación de usuarios. Con sus habilidades, realizan pruebas de penetración y evalúan vulnerabilidades, siempre en busca de la más mínima grieta por la que pudiera colarse un intruso.

Pero su labor no termina ahí. Estos ingenieros también son arquitectos de políticas y procedimientos de seguridad, y educadores apasionados, compartiendo su conocimiento para fortalecer la muralla humana contra los ciberataques. Su compromiso con la seguridad es integral, diseñando y manteniendo sistemas que no solo son robustos, sino también resilientes, trabajando codo a codo con otros expertos en seguridad para asegurar que la información de la organización permanezca segura y soberana.

Seguridad en redes y sistemas informáticos

Éste es un aspecto crítico en el entorno digital actual. Con el aumento de la conectividad y la dependencia de la tecnología, proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas se ha tornado de mucha importancia a nivel mundial y en todos los ámbitos, desde la protección contra malware y virus hasta la seguridad de la infraestructura de red y la gestión de accesos.

La seguridad en redes y sistemas informáticos abarca una extensa gama de medidas y prácticas diseñadas para prevenir, detectar y responder a amenazas cibernéticas y a posibles ataques. Esto se ha vuelto complejo debido al aumento de dispositivos conectados a internet y al avance de las tecnologías de información e involucra la implementación de controles técnicos, políticas de seguridad sólidas, la encriptación de datos, la autenticación de usuarios, el monitoreo constante y la adopción de buenas prácticas por parte de los usuarios, siendo solo algunas de las estrategias claves para mitigar riesgos (Anderson, 2015). Proteger la información confidencial y

garantizar el funcionamiento seguro es de trascendental importancia para individuos, empresas y organizaciones. La protección de datos en tránsito y en reposo, la detección proactiva de amenazas y la respuesta a incidentes son áreas críticas que requieren atención constante (Whitman & Mattord, 2018).

Entre otras estrategias para implementar sólidas medidas de protección se encuentran: la configuración adecuada de los dispositivos de red, como firewalls y routers, para filtrar y controlar el tráfico entrante y saliente, el uso de métodos de detección y prevención de intrusiones para monitorear el tráfico y detectar actividades maliciosas. Además, se deben aplicar actualizaciones y parches de seguridad regularmente en todos los componentes del sistema para corregir vulnerabilidades conocidas.

Por otra parte, la autenticación y el acceso seguro son elementos de fortaleza en la seguridad de redes y sistemas informáticos. La clave está en la adopción de políticas de contraseñas sólidas, aplicar la autenticación multifactor y llevar una gestión meticulosa de las cuentas de usuario (Stallings, 2017a). La eficacia de estas medidas se logran mediante el uso de sistemas avanzados de gestión de identidades y accesos, los cuales conrolan y auditan los permisos concedidos a los usuarios, restringiendo de ese modo el acceso a datos sensibles.

De la misma forma, la concienciación y la capacitación de los usuarios son aspectos cruciales en la seguridad de las infraestructuras digitales. Es imperativo que los trabajadores sean instruidos en prácticas seguras, incluyendo el reconocimiento de intentos de phishing por correo electrónico, la gestión segura de contraseñas y la custodia de la información sensible (Easttom, 2016). Para asegurar que todos los integrantes de la organización estén al tanto, comprendan y apliquen las normativas de seguridad, es necesario comunicar con claridad y reforzar constantemente las políticas y procedimientos de seguridad.

La implementación de mecanismos de cifrado para proteger la confidencialidad de los datos sensibles durante su transmisión y almacenamiento de modo que los mismos no puedan ser leídos ni modificados, forman parte importante también de la seguridad. El uso de protocolos seguros, como Secure Sockets Layer (SSL) / Transport Layer Security (TLS), y el cifrado de datos utilizando algoritmos criptográficos sólidos, son prácticas elementales para proteger la información contra accesos de terceros no autorizados (Stallings, 2017b).

Es imprescindible tener una capacidad de respuesta rápida y eficaz ante incidentes de seguridad. Esto significa la creación de protocolos de actuación bien definidos y la formación de equipos especializados que se enfoquen en el manejo y atenuación de amenazas potenciales. Además, es necesario disponer de sistemas de registro y monitoreo eficientes que permitan analizar y actuar frente a estas situaciones de forma rápida y adecuada.

En la era de la interconexión global, la fortaleza en redes y sistemas informáticos se cimienta no solo en la solidez tecnológica, sino también de la conciencia y la capacitación de quienes los utilizan. No se puede ignorar el poder de la ingeniería social y el riego de amenazas internas al diseñar estrategias de seguridad efectivas.

Solo mediante la implementación de un enfoque integral de seguridad, se puede contrarrestar los ataques cibernéticos y preservar la integridad, confidencialidad y disponibilidad de los sistemas informáticos y las redes. Mantenerse al día con las últimas tendencias y amenazas

en un campo en constante transformación, es esencial para garantizar una defensa efectiva y actualizada de los preciados datos.

Medidas adicionales para fortalecer la seguridad en redes y sistemas informáticos

Implementar medidas adicionales para reforzar la infraestructura digital es más que una necesidad; es una inversión en la continuidad y confiabilidad de las operaciones diarias, cada paso quese da es un escudo adicional contra las amenazas cibernéticas que evolucionan constantemente, mencionemos algunas:

Segmentación de redes: dividir la red en segmentos más pequeños y separados, conocidos como subredes, para limitar el impacto de un posible ataque, ayuda a prevenir la propagación lateral de amenazas y reduce la superficie de ataque.

Monitoreo de seguridad continuo: monitoreo de seguridad en tiempo real para detectar actividades sospechosas, anomalías o violaciones de seguridad, permite una respuesta rápida y reduce el tiempo de detección de amenazas (Krebs, 2020).

Actualizaciones y parches regulares: mantener todos los sistemas y dispositivos con las últimas actualizaciones ayuda a cerrar las brechas de seguridad conocidas y a mitigar las vulnerabilidades existentes.

Control de acceso basado en roles: garantiza que los usuarios solo tengan acceso a los recursos y datos necesarios para llevar a cabo sus tareas, minimizando los riesgos asociados con los privilegios excesivos o innecesarios (Whitman & Mattord, 2018).

Auditorías de seguridad regulares: evaluar y validar la efectividad de las medidas de seguridad implementadas, identifica posibles brechas o debilidades en el sistema y permite tomar acciones correctivas.

Copias de seguridad y recuperación de datos: realizar copias de seguridad de forma regular de todos los datos críticos y establecer un plan de recuperación de desastres para garantizar que los datos puedan ser restaurados en caso de pérdida, daño o ataque cibernético (Redman, 2017).

Protección contra malware: que incluyan antivirus, antimalware y firewalls de próxima generación para proteger los sistemas contra amenazas conocidas y emergentes.

Control de dispositivos y acceso remoto: controles estrictos para el uso de dispositivos y el acceso remoto a la red corporativa que incluya la autenticación de dispositivos y el cifrado de conexiones remotas para evitar accesos no autorizados.

Pruebas de penetración: para identificar posibles vulnerabilidades y brechas en la seguridad, estas pruebas simulan ataques reales para evaluar la resistencia del sistema y tomar medidas correctivas (Engebretson, 2014).

Educación continua en seguridad: promover la conciencia y la educación en seguridad cibernética entre los empleados mediante capacitaciones periódicas, campañas de sensibilización y la promoción de buenas prácticas de seguridad (Whitman & Mattord, 2018).

Estas medidas adicionales fortalecen la capacidad de respuesta ante incidentes de seguridad y reducen la probabilidad de un ataque exitoso.

Protección de datos y privacidad

A medida que la cantidad de datos generados y almacenados continúa creciendo, garantizar la seguridad, el manejo ético y la confidencialidad de la información personal y sensible, se convierte en prioridad. Es así que, la protección de datos hace referencia a las medidas y políticas destinadas a salvaguardar la integridad, la disponibilidad de los datos y el uso no autorizado de información confidencial, mientras que la privacidad se relaciona con el control y la gestión adecuada de la información personal. Los esfuerzos por proteger la información personal y los derechos de privacidad se encuentran en un estado continuo de adaptación ante las innovaciones tecnológicas y las tendencias socio-políticas (Whittaker et al., 2018).

En el contexto de la protección de datos, las regulaciones como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea y la Ley de Privacidad del Consumidor de California (CCPA) en los Estados Unidos han establecido criterios estrictos para el manejo de datos personales (Clarke & Wigan, 2019). Estas regulaciones imponen obligaciones significativas a las organizaciones en términos de claridad y transparencia de sus operaciones, la obtención del consentimiento explícito, la comunicación efectiva de incidentes de seguridad y la garantía del derecho a ser olvidado.

Por su parte, la privacidad, se erige como un derecho fundamental de las personas para gestionar y controlar la divulgación y el uso de su información personal (Nissenbaum, 2010). En una época donde la acumulación de datos tanto para entidades corporativas como gubernamentales, y la vigilancia digital se intensifica, encontrar un punto medio entre la recolección de datos para la mejora de servicios y la salvaguarda de la privacidad personal se convierte en un reto constante.

La privacidad se basa en cinco elementos fundamentales: consentimiento, transparencia, portabilidad, responsabilidad y control (Cavoukian, 2016). El consentimiento permite a los individuos decidir si están dispuestos a compartir sus datos con terceros. La transparencia implica que las organizaciones comuniquen honesta y claramente cómo manejaron los datos de los individuos. La portabilidad permite a los individuos llevar sus datos con ellos cuando lo deseen. Mientras que la responsabilidad obliga a las organizaciones a ser responsables de la gestión de los datos de los individuos y el control les otorga a los individuos la capacidad de determinar qué datos se recopilarán, cómo se utilizarán y quién tiene acceso a ellos.

La protección de datos y la privacidad trascienden las barreras legales y éticas, convirtiéndose en pilares de la confianza pública y el prestigio organizacional. La adopción de prácticas de privacidad desde el diseño, el cifrado de la información, la gestión de consentimientos consciente y las evaluaciones de impacto son estrategias cruciales para garantizar el resguardo y el respeto de la privacidad individual (Solove, 2013; Greenleaf & Waters, 2019).

Si bien ambos conceptos, la protección de datos y la privacidad, se relacionan, no son idénticos y tienen sus diferencias. El primero hace referencia a la conservación de la integridad y confidencialidad de los datos de una organización a través de medidas técnicas y administrativas para garantizar la seguridad de los datos, mientras que el segundo se centra en determinar quién tiene acceso autorizado a los datos personales y quién controla su uso, busca proteger la intimidad y la autonomía de los individuos a través de aspecto legales y éticos. En la Tabla 1 se puede evidenciar las diferencias entre ambos.

Tabla 1. *Diferencias claves entre protección de datos y privacidad*

	Protección de Datos	Privacidad
Responsabilidad	Corresponde a las Organizaciones	Corresponde a los Usuarios
Objetivos	Busca preservar la integridad y confiabilidad de los datos	Busca proteger la intimidad y autonomía de los individuos
Controles	Se centra en la implementación de controles técnicos y administrativos	Se centra en la determinación de quién tiene acceso autorizado a los datos personales

Tomando en consideración la importancia de la protección y privacidad de los datos, existen prácticas seguras para almacenar y transmitirlos que permitan proteger la información. Entre ellos se disponen de: la encriptación para salvaguardar los datos en tránsito y en reposo, esto implica cifrar los archivos y bases de datos de modo que solo las personas autorizadas puedan acceder y descifrar la información. La implementación de contraseñas robustas y únicas para cada cuenta y la gestión de permisos basados en roles para controlar y restringir el acceso a los datos.

Por otra parte, habilitar la autenticación de dos factores agrega una capa adicional de seguridad al requerir un segundo método de verificación como un código generado por una aplicación móvil o un mensaje de texto, en conjunto con la contraseña. Además, mantener una vigilancia constante mediante el monitoreo de redes y sistemas para detectar y responder rápidamente a cualquier actividad sospechosa permite una respuesta rápida ante posibles incidentes de seguridad. Otra de las prácticas consiste en realizar copias de seguridad periódicas y almacenarlas en ubicaciones seguras y separadas para garantizar que, se pueda recuperar la información sin problemas y minimizar el impacto en la continuidad de la organización. También utilizar protocolos seguros para la transmisión de datos, como el uso de HTTPS en los sitios web y la implementación de VPN (redes privadas virtuales) permite proteger las comunicaciones entre ubicaciones remotas. El cifrado de extremo a extremo es esencial al compartir datos confidenciales a través de canales de comunicación.

Y finalmente, asegurarse que al eliminar los datos que ya no sean necesarios, se haga de manera segura. Esto implica utilizar métodos de borrado seguro o destrucción física de los medios de almacenamiento para garantizar que los datos no puedan ser recuperados por terceros no autorizados.

Al adoptar estas medidas, las organizaciones pueden asegurar la integridad y confidencialidad de los datos críticos, manteniendo la confianza de los usuarios y cumpliendo con las regulaciones de privacidad globales.

Organizaciones que regulan la transmisión y almacenamiento de datos

Diversas regulaciones y marcos legales internacionales establecen estándares mínimos para la protección de datos y la privacidad para ser tomadas en cuenta al momento que las organizaciones deban almacenar y transmitir datos (European Commission, 2016; Personal Data Protection Bill, 2019; Cyber Security Act, 2018), a continuación se mencionan las más comunes:

Reglamento General de Protección de Datos (GDPR): regulación de la Unión Europea que establece normas para la protección de datos personales de los ciudadanos de la UE. Se

aplica a todas las organizaciones que procesan datos personales de individuos dentro de la UE, independientemente de la ubicación de la organización.

Ley de Privacidad y Seguridad de la Información de California (CCPA): ley estatal en California, Estados Unidos, que otorga a los residentes de California algunos derechos sobre sus datos personales y exige a las organizaciones que cumplan con ciertas obligaciones de privacidad y seguridad.

Ley de Protección de Datos Personales (LGPD): ley que establece reglas para el tratamiento de datos personales en Brasil. Se aplica a cualquier organización que procese datos personales de individuos en Brasil, independientemente de la ubicación de la organización.

Ley de Privacidad de las Comunicaciones Electrónicas (PECR): regulaciones del Reino Unido que complementan el GDPR y se centran específicamente en la privacidad y la seguridad de las comunicaciones electrónicas, como el marketing directo por correo electrónico y llamadas telefónicas.

Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA): ley de Estados Unidos que establece estándares para la protección de la información de salud personalmente identificable y exige que las organizaciones de atención médica y sus asociados cumplan con requisitos específicos de seguridad y privacidad.

Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS): es un estándar de seguridad de la información aplicable a todas las organizaciones que procesan, transmiten o almacenan datos de tarjetas de pago. Está diseñado para proteger la integridad y confidencialidad de la información de las tarjetas de pago y evitar el fraude.

Es importante tener en cuenta que las regulaciones pueden variar según el país y la industria, por lo que es esencial que las organizaciones obtengan asesoramiento legal, se mantengan informadas y cumplan con las regulaciones locales e internacionales pertinentes para garantizar el cumplimiento normativo adecuado.

Dato proyectado en la Ingeniería en Sistemas

Según diversos estudios e investigaciones, el manejo efectivo de los datos proyectados es crucial para la toma de decisiones informadas y el desarrollo de sistemas inteligentes. Los ingenieros en sistemas utilizan técnicas avanzadas de análisis de datos y modelado para comprender las tendencias futuras y proyectar posibles escenarios. Estos datos proyectados permiten anticipar cambios, tomar decisiones, medidas preventivas y optimizar los sistemas existentes (Salameh et al, 2020). Además, las proyecciones de datos son fundamentales en áreas como la inteligencia artificial, el aprendizaje automático y la optimización de procesos. Se ha demostrado que el uso adecuado de los datos proyectados puede mejorar la eficiencia, la precisión y la capacidad de respuesta de los sistemas de ingeniería en diferentes sectores industriales.

Estas técnicas avanzadas y su correcta elección van a depender del tipo de datos, el problema a resolver y los objetivos específicos del análisis. Algunas de ellas se mencionan a continuación:

Minería de datos: proceso de descubrir patrones, relaciones y tendencias ocultas en conjuntos de datos grandes. Los ingenieros en sistemas utilizan algoritmos de minería de datos

para identificar información relevante y tomar decisiones basadas en los patrones encontrados (Goldberg, 1989).

Aprendizaje automático (Machine Learning): rama de la inteligencia artificial que se centra en el desarrollo de algoritmos y modelos que permiten a las computadoras aprender y tomar decisiones sin ser programadas explícitamente. Se utilizan técnicas de aprendizaje automático, como clasificación, regresión y agrupamiento, para analizar datos y hacer predicciones (Russell & Norvig, 2009; Goldberg, 1989).

Análisis de series temporales: se refiere al análisis de datos que se recopilan secuencialmente en intervalos de tiempo. Utilizan técnicas de análisis de series temporales para identificar patrones y tendencias a lo largo del tiempo, lo que les permite hacer proyecciones y pronósticos. (Box, Jenkins, Reinsel, & Ljung, 2015).

Redes neuronales: son modelos computacionales inspirados en el funcionamiento del cerebro humano. Se basan en redes neuronales para resolver problemas complejos de análisis de datos, como reconocimiento de imágenes, procesamiento del lenguaje natural y detección de anomalías.

Modelado estadístico: aplican técnicas estadísticas para analizar datos y construir modelos que describan y expliquen el comportamiento de los sistemas. Esto incluye técnicas como regresión, análisis de varianza, pruebas de hipótesis y diseño de experimentos. (Hastie, Tibshirani, & Friedman 2009).

Optimización: técnicas de optimización utilizadas para encontrar la mejor solución posible a un problema dado. Esto implica maximizar o minimizar una función objetivo sujeta a ciertas restricciones, utilizando algoritmos como el algoritmo genético, la programación lineal o el enfoque de búsqueda heurística (Goldberg, 1989).

Estas técnicas avanzadas de análisis de datos se utilizan principalmente para comprender y procesar los datos proyectados, pero no son específicamente diseñadas para proteger los datos en sí. Sin embargo, existen otras técnicas y enfoques relacionados que se utilizan en conjunto con medidas de seguridad para proteger los datos proyectados. Algunas de éstas incluyen:

Cifrado de datos utiliza para codificar los datos y garantizar su confidencialidad. El cifrado de extremo a extremo, por ejemplo, protege los datos durante la transmisión y evita que sean accesibles para terceros no autorizados (Stallings, 2017b).

Técnicas de anonimización: ocultan o eliminan información identificable en los datos, preservando así la privacidad de las personas involucradas. La anonimización puede ser útil al proyectar datos sensibles para proteger la identidad de las personas involucradas (Sweeney, 2002).

Control de acceso y autenticación: incluyen sistemas de autenticación mediante contraseñas, autorizaciones basadas en roles y registros de auditoría para rastrear el acceso a los datos.

Técnicas de detección de anomalías: identifican patrones inusuales o comportamientos anómalos en los datos proyectados. Ayudan a identificar posibles amenazas o violaciones de seguridad en tiempo real (Chandola, Banerjee, & Kumar, 2009).

Cabe destacar que estas técnicas no son exclusivas del análisis de datos proyectados y se aplican de manera más amplia en el campo de la seguridad de la información. Su implementación efectiva requiere un enfoque holístico que combine tanto medidas técnicas como políticas y procedimientos de seguridad adecuados.

Datos proyectados, ataques cibernéticos y medidas de seguridad

En el mundo interconectado de hoy, los datos proyectados pueden ser susceptibles a ataques cibernéticos, especialmente si se almacenan, procesan o transmiten a través de sistemas informáticos o redes que no cuentan con suficientes medidas de seguridad. Sin embargo, es importante tener en cuenta que la vulnerabilidad de los datos proyectados a los ataques cibernéticos depende de varios factores, como la naturaleza de los datos, las medidas de seguridad implementadas y las prácticas de gestión de riesgos. La intersección entre estos dos conceptos se encuentra en la necesidad que la información sensible no caiga en manos equivocadas.

La seguridad del dato proyectado es un tema relevante en el ámbito de la gestión de datos, y depende de diversos aspectos. Estudios han analizado que la implementación de medidas de seguridad robustas como el cifrado de datos, la anonimización, así también políticas y procedimientos que incluyan el control de acceso, la detección de anomalías y por supuesto la educación continua sobre las mejores prácticas son, por lo tanto, imperativas para salvaguardar la infraestructura digital y la información valiosa que contiene (Gandomi y Haider, 2015).

Por otra parte, la correcta gestión de la seguridad de los datos proyectados requiere la adopción de estándares reconocidos, como el Instituto Nacional de Estándares y Tecnología (NIST) y el ISO/IEC 27001 (Hastie, Tibshirani & Friedman, 2009). El primero, es una agencia del gobierno de Estados Unidos que desarrolla, promueve normas y guías para diversas áreas, incluida la seguridad de la información y ha publicado el Marco de Ciberseguridad (NIST Cybersecurity Framework), que proporciona una serie de estándares y mejores prácticas para ayudar a las organizaciones a gestionar y mejorar su postura de ciberseguridad. Por otro lado, el ISO/IEC 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Proporciona un enfoque sistemático y estructurado para establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información dentro de una organización. El ISO/IEC 27001 se centra en la gestión de riesgos y ayuda a las organizaciones a establecer controles y medidas de seguridad adecuados para proteger los datos proyectados y otros activos de información.

Ambos marcos, el NIST y el ISO/IEC 27001, pueden ayudar en la seguridad de los datos proyectados al proporcionar directrices detalladas sobre la gestión de la seguridad de la información. Ofrecen un enfoque estructurado y basado en estándares para identificar riesgos, implementar controles de seguridad, establecer políticas y procedimientos, y realizar auditorías y revisiones periódicas para garantizar la protección de los datos proyectados. Al seguir las recomendaciones y requisitos establecidos por el NIST y el ISO/IEC 27001, las organizaciones pueden fortalecer su postura de seguridad y mitigar los riesgos asociados con los datos proyectados.

La seguridad del dato proyectado es un objetivo alcanzable mediante la implementación de medidas adecuadas y la adopción de enfoques integrales de seguridad respaldados por la investigación y las mejores prácticas en el campo de la protección de datos.

Seguridad en el desarrollo de software y aplicaciones

La seguridad es un factor crítico y de gran importancia en el desarrollo de software y aplicaciones, pues ambos deben estar preparados para enfrentarse a intentos maliciosos de intrusión o manipulación y garantizar que solo aquellos autorizados pueden acceder a la información confidencial contenida dentro de los sistemas, mantener la integridad de los datos y evitar alteraciones no deseadas durante el uso y almacenamiento de los mismos. La implementación de buenas prácticas de seguridad desde las etapas iniciales del ciclo de vida del desarrollo de software es esencial para prevenir vulnerabilidades y mitigar riesgos (McGraw, 2006).

Autores como Howard, Viega & LeBlanc (2009) enfatizan la importancia de realizar pruebas de seguridad de forma regular y exhaustiva durante el proceso de desarrollo, a fin de identificar y corregir posibles fallas o brechas de seguridad y ser capaces de proveer servicios continuos y sin interrupciones, incluso ante situaciones adversas.

Son muchas las amenazas a los sistemas de software, pero podemos nombrar tres principales: Inyecciones SQL (SQL injection), Ataque por inyección de código (Code injection) y Vulnerabilidades conocidas (Known vulnerabilities). Sin embargo, para mitigar estas amenazas se pueden implementar diversas medidas de seguridad entre las cuales están: Validación de entrada, Codificación correcta, Utilización de herramientas de análisis estático y dinámico, Implementación de mecanismos de autenticación y autorización robustos (Bhowmik & Chakraborty, 2019; O'Harrow III, 2015).

El enfoque de seguridad en el desarrollo de software se centra en la integración de medidas proactivas durante todas las fases del proceso de desarrollo, desde el diseño y la codificación hasta las pruebas y la implementación. Esto incluye la adopción de estándares de codificación segura, la evaluación de riesgos, la identificación y corrección de vulnerabilidades, el análisis de seguridad estática y dinámica, así como la formación de los desarrolladores en buenas prácticas de seguridad (López Álvarez, 2020).

La adopción de marcos y estándares reconocidos, como OWASP (Open Web Application Security Project) y el estándar PCI DSS (Payment Card Industry Data Security Standard), proporciona directrices y controles específicos para abordar las vulnerabilidades comunes en el desarrollo de aplicaciones web y la protección de datos sensibles (OWASP, 2020; PCI Security Standards Council, 2019). Asimismo, la capacitación y concienciación de los desarrolladores en cuanto a las mejores prácticas de seguridad son aspectos cruciales McGraw, 2006). Promover una cultura de seguridad y proporcionar la formación adecuada permite que todos los miembros del equipo sean conscientes de los riesgos de seguridad y asuman la responsabilidad de implementar medidas de seguridad eficaces. Se requiere una combinación de enfoques proactivos, pruebas rigurosas y la adhesión a estándares y marcos específicos para garantizar la protección de los sistemas y datos sensibles.

La filosofía de DevSecOps amplía la metodología DevOps para integrar la seguridad en cada etapa del ciclo de vida del desarrollo de software. DevSecOps se basa en el principio de que

la seguridad no debe ser tratada como un aspecto separado o posterior al desarrollo de aplicaciones, sino que debe ser integrada desde las etapas iniciales del proceso de desarrollo de manera continua y proactiva. Además, el concepto de DevSecOps ha ganado popularidad, promoviendo la integración de la seguridad en los procesos de desarrollo y operaciones. Esta mentalidad de "seguridad como código" busca automatizar las pruebas de seguridad, la monitorización continua y la respuesta a incidentes, permitiendo una respuesta más ágil y eficiente a las amenazas emergentes (Shiva & Lichtenwalter, 2017). Pero para que esta integración sea efectiva, se requiere una arquitectura bien diseñada que permita la implementación de controles de seguridad de manera eficiente y sin interrumpir el flujo de trabajo de los desarrolladores y el código fuente.

La implementación exitosa de DevSecOps conlleva una serie de beneficios adicionales a DevOps que son claves e impactan en la reducción del time to market con mayor seguridad, velocidad y menor coste, la detección de vulnerabilidades en una etapa temprana, la facilitación de la entrega de código con mayor seguridad, la mejora de la calidad y desarrollo del software en eficiencia y eficacia, la reducción de los riesgos de seguridad, y la mejora de la relación entre el desarrollo y la seguridad.

Referencias Bibliográficas

Anderson, R. (2015). *Security Engineering: A Guide to Building Dependable Distributed.* 3ra edición. Willey

Bhowmik, S., & Chakraborty, P. K. (2019). Security Challenges and Countermeasures for Web Applications. *IEEE Access*, 7(1), 821-834. doi: 10.1109/ACCESS.2018.2883823

Box, G. E. P., Jenkins, G. M., Reinsel, G. C., & Ljung, G. M. (2015). *Time Series Analysis: Forecasting and Control*. Wiley.

Cavoukian, A. (2016). *Privacidad por diseño los 7 principios fundamentales*. *Mediascope.* https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. *ACM Computing Surveys*, 41(3), 15.

Clarke, R., & Wigan, M. (2019). *The GDPR and Data Protection: A Practical Guide*. Oxford University Press.

Cyber Security Act. (2018).

Easttom, C. (2016). *Computer Security Fundamentals*. Pearson

Engebretson, P. (2014). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Syngress.

European Commission. (2016). General Data Protection Regulation (GDPR). https://edpo.com/high-quality-representation-services/?gad_source=1&gclid=EAIaIQobChMIht_40OvJhQMV66RaBR3RKArQEAAYASAAEgKObvD_BwE

Gandomi, A. & Haider, M. (2015). Beyond the Hype: Big Data Concepts, Methods, and Analytics. *International Journal of Information Management*, 35(2), 137-144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Greenleaf, G. W., & Waters, N. (2019). *Global Data Privacy Laws: 2019 Mid-Year Review*. Privacy Laws & Business International Report.

Goldberg, D. E. (1989). *Genetic Algorithms in Search, Optimization, and Machine Learning*. Addison-Wesley.

Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Springer.

Howard, M, Viega, J & LeBlanc, D. (2009). *19 Deadly Sins of Software Security: Programming Flaws and How to fix them*. McGraw-Hill.

Instituto Nacional de Estándares y Tecnología (NIST): https://www.nist.gov/

ISO/IEC 27001: https://www.iso.org/standard/54534.html

Krebs, B. (2020). *Continuous Security Monitoring: Real-Time Threat Detection and Incident Response*. O'Reilly Media.

López Álvarez, D. M. (2020). Método para el desarrollo de software seguro basado en la ingeniería de software y ciberseguridad. *INNOVA Research Journal*, 5, 263-280.

McGraw, G. (2006). *Software Security: Building Security In*. Addison-Wesley Professional.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books.

O'Harrow III, W. N. (2015). Engineering security into software systems. *Communications of the ACM*, 58(11), 28-34. doi: 10.1145/2818448

OWASP Top 10, 2020. https://owasp.org/www-project-top-ten/

PCI Security Standards Council, 2019. https://www.pcisecuritystandards.org/

Personal Data Protection Bill. (2019). https://thecma.ca/resources/maintaining-standards/privacy-protection?gad_source=1&gclid=EAIaIQobChMIy57QiuzJhQMVn55aBR2R3QuqEAAYASAAEgIhHPD_BwE

Redman, T. (2017). *Data Backup and Recovery: A Guide to Managing and Protecting Your Company's Data*. Wiley.

Russell, S., & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach*. Pearson.

Salameh, A.M., Baker El-Ebiary, Y.A, Abu-Ulbeh, W., Hassan Hassan, A., Bamansoor, S., & Saany, S.I.A. (2020). The Effectiveness Of Management Information System In Decision-Making. *J. Mech. Cont.& Math. Sci*., 15(7), 316-327. https://doi.org/10.26782/jmcms.2020.07.000

Shiva, K., & Lichtenwalter, T. (2017). DevSecOps: Integrating Security into DevOps. *IEEE Security & Privacy*, 15(6), 52-59. https://ieeexplore.ieee.org/document/8060151

Solove, D. J. (2013). *Understanding Privacy*. Harvard University Press.

Stallings, W. (2017a). *Network Security Essentials: Applications and Standards*. Pearson.

Stallings, W. (2017b). *Cryptography and Network Security: Principles and Practice*. Pearson.

Sweeney, L. (2002). k-Anonymity: A Model for Protecting Privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557-570.

Whitman, M.E., & Mattord, H.J. (2018). *Principles of Information Security*. Cengage Learning.

Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., & Schwartz, O. (2018). *AI now report 2018* (pp. 1-62). New York: AI Now Institute at New York University.

Alex Sandro Landeo Quispe 1, **Vladimir Orihuela Rojas** 1, **Fernando Pool Orihuela Rojas** , **& Johanna Rosa Velarde Samaniego** 2

1. Universidad Nacional de Huancavelica, Perú - 2. Universidad Tecnológica del Perú

Desde 2023 hemos visto un cambio realmente acelerado en la forma en que se utiliza la tecnología en la educación. Ahora es mucho más común el aprendizaje híbrido y a distancia, donde los estudiantes pueden acceder a recursos en línea y colaborar virtualmente. Pero claro, con estos cambios también han surgido nuevos retos. Tenemos que asegurarnos de que todos los estudiantes tengan las mismas oportunidades de acceso y participación, sin dejar a nadie atrás en esta revolución digital. Y no solo eso, también es crucial que tanto estudiantes como educadores desarrollen las habilidades digitales esenciales para aprovechar al máximo estas herramientas.

En cuanto a la ciberseguridad, últimamente los ciberataques se han vuelto todo un dolor de cabeza, cada vez más sofisticados y frecuentes. Las organizaciones educativas se han convertido en uno de los principales objetivos, ya que manejan gran cantidad de datos confidenciales de estudiantes y personal. Por eso es tan importante que las instituciones educativas tomen medidas serias en materia de ciberseguridad, fortalezcan la concienciación y capacitación del personal, y se preparen para responder eficazmente ante cualquier incidente. Por eso es tan importante que las instituciones educativas tomen medidas serias en materia de ciberseguridad. Tienen que implementar protecciones robustas, asegurarse de que todo el personal esté bien capacitado y tener planes de contingencia listos por si las cosas se complican. Solo así podrán enfrentar de manera eficaz cualquier incidente que se presente.

La intersección entre educación y ciberseguridad es clave. Debemos asegurar que los estudiantes desarrollen habilidades digitales avanzadas, incluyendo la capacidad de navegar de manera segura en línea, proteger su información personal y reconocer amenazas cibernéticas. La educación en ciberseguridad debe ser un componente integral en todos los niveles educativos.

Conceptos clave relacionados con la ciberseguridad en el ámbito educativo

La ciberseguridad en el contexto educativo aborda un amplio espectro de conceptos fundamentales. Un elemento crítico es la protección de los datos estudiantiles y del personal, incluyendo información personal, registros académicos y evaluaciones (Kruger & Drevin, 2022). Esto requiere implementar sólidos sistemas de autenticación y control de accesos, como el uso de contraseñas seguras, verificación en dos pasos y administración de privilegios (NIST, 2022). Asimismo, las instituciones deben contar con políticas y procedimientos claros sobre el manejo y

almacenamiento de datos, así como planes de respuesta ante posibles brechas de seguridad (Ghafir et al., 2018).

Investigaciones recientes han destacado la importancia de implementar políticas y normas de seguridad robustas, alineadas con estándares internacionales como los de la National Institute of Standards and Technology (NIST, 2022). Por lo tanto, la seguridad de la infraestructura tecnológica utilizada en las instituciones educativas se torna de máxima importancia, donde los expertos recomiendan salvaguardar servidores, computadoras, redes inalámbricas y aplicaciones de posibles intrusiones o ataques de denegación de servicio a través de medidas como actualización de los sistemas operativos y software, implementar las tecnologías de cifrado de datos en tránsito y en reposo, detección de amenazas, respuesta a incidentes, el uso de firewalls, sistemas de detección y prevención de intrusos, y respaldo regular de datos educativos (Geer, 2020; Barona & Anita, 2017). La educación y el desarrollo de competencias digitales seguras entre estudiantes y personal docente facilitan crear una cultura de ciberseguridad efectiva en las instituciones educativas (Shaikh & Singla, 2021).

Más allá de la protección técnica, la concientización y capacitación en prácticas de navegación segura en línea es fundamental para toda la comunidad educativa (Shaikh & Singla, 2021). Estudiantes, docentes y personal administrativo deben estar preparados para reconocer amenazas como phishing, malware y riesgos de privacidad, y adoptar comportamientos ciberseguros en sus actividades diarias. Esto puede lograrse a través de programas de concientización, talleres y recursos educativos sobre ciberseguridad (Kritzinger & von Solms, 2010).

En el ámbito educativo, la ciberseguridad involucra salvaguardar información sensible, asegurar la infraestructura tecnológica y fomentar una cultura de concientización y prácticas seguras, todo ello alineado con estándares y recomendaciones de organismos líderes como NIST. La tabla 1 muestra un resumen de los conceptos clave.

Importancia de la concienciación y la educación en ciberseguridad

En el mundo digital la ciberseguridad se ha convertido en una prioridad, donde tecnologías emergentes, interconectividad y almacenamiento masivo de datos plantean nuevos e imprevisibles desafíos. En este contexto, la concienciación y la educación en ciberseguridad desempeñan un papel imprescindible para fortalecer la resiliencia y seguridad de individuos, organizaciones y sociedades enteras.

En primer lugar, la concienciación en ciberseguridad es esencial para empoderar a los usuarios finales, quienes representan la primera y más vulnerable línea de defensa ante amenazas cibernéticas (Kritzinger & von Solms, 2010). Estudios han demostrado que incluso los ataques más sofisticados a menudo aprovechan el factor humano, como el engaño a través de técnicas de phishing o la divulgación involuntaria de información sensible (Aldawood & Skinner, 2019). Al crear una cultura de concientización, se logra que las personas desarrollen habilidades para identificar señales de alerta, adopten mejores prácticas de navegación y manejo de datos, y reporten incidentes oportunamente (Alaskar et al., 2020). Este cambio de mentalidad es clave para convertir al usuario en un actor proactivo en la ciberseguridad, en lugar de ser un eslabón débil.

Tabla 1. *Conceptos clave de la ciberseguridad en el ámbito educativo*

Concepto Clave	Descripción
Amenazas cibernéticas	Malware (virus, troyanos, ransomware, etc.) Ataques de denegación de servicio (DDoS) Phishing y suplantación de identidad Acceso no autorizado a sistemas y datos Robo de identidad y fraude
Vulnerabilidades	Debilidades en sistemas, software y protocolos Falta de actualización y parches de seguridad Errores de configuración y mala gestión de privilegios Ingeniería social y confianza excesiva de los usuarios
Impacto potencial	Interrupción de las actividades educativas Pérdida o robo de datos confidenciales Daños a la reputación y la confianza de la institución Sanciones legales y financieras Exposición de la comunidad educativa a riesgos
Políticas y estándares de seguridad	Políticas de uso aceptable de TI Directrices de gestión de identidades y accesos Procedimientos de respuesta y recuperación ante incidentes Cumplimiento de normativas y estándares de seguridad
Medidas de seguridad	Controles de acceso y autenticación robustos Cifrado de datos en tránsito y en reposo Sistemas de detección y prevención de intrusiones Programas de copias de seguridad y recuperación de desastres
Conciencia y capacitación en ciberseguridad	Programas de concientización para estudiantes y personal Desarrollo de competencias en ciberseguridad Fomento de una cultura de seguridad y responsabilidad compartida
Colaboración y coordinación	Intercambio de información y mejores prácticas Desarrollo conjunto de marcos y estándares Actividades de capacitación y concientización conjuntas Colaboración en el desarrollo de soluciones técnicas

En segundo lugar, la educación sistemática en ciberseguridad es fundamental para formar a profesionales altamente calificados que puedan hacer frente a las amenazas cada vez más sofisticadas. A medida que la dependencia tecnológica aumenta, la demanda de expertos en ciberseguridad crece exponencialmente (Bada & Sasse, 2014). Sin embargo, los programas educativos a menudo se encuentran desfasados o carecen de la profundidad y actualización necesarias. Abordar esta brecha requiere la implementación de currículos de vanguardia que preparen a los estudiantes en áreas como gestión de riesgos, análisis forense digital, gobierno de la información y desarrollo de software seguro (Dawson & Thomson, 2018). Además, la educación continua y la certificación de conocimientos especializados son cruciales para mantener a los profesionales a la par con la evolución de las amenazas y tecnologías de seguridad.

Más allá del ámbito académico, la educación en ciberseguridad debe extenderse a todos los sectores y niveles de una organización, desde la alta dirección hasta el personal de primera línea (Van Niekerk & Von Solms, 2010). Los líderes empresariales necesitan comprender los riesgos y estrategias de seguridad para tomar decisiones informadas y asignar los recursos adecuados. Por su parte, el personal operativo debe estar capacitado en la aplicación de controles de seguridad, protocolos de respuesta a incidentes y mejores prácticas de manejo de información. Esta integración de la educación en ciberseguridad a través de la organización fomenta una cultura de seguridad sólida y resiliente.

Adicionalmente, la concienciación y educación en ciberseguridad tienen un impacto positivo a nivel social y de políticas públicas. A medida que los ciudadanos se vuelven más

conscientes de los riesgos y mejores prácticas, se genera una demanda por regulaciones, estándares y programas gubernamentales que aborden la ciberseguridad de manera integral (Dawson & Thomson, 2018). Esto conduce al desarrollo de marcos normativos, iniciativas de capacitación y campañas de sensibilización a escala nacional o regional, fortaleciendo la seguridad del ecosistema digital en su conjunto.

La concienciación y educación en ciberseguridad son estrategias fundamentales para enfrentar los desafíos del mundo digital y construir una sociedad más resiliente. Al empoderar a los usuarios, formar profesionales especializados y promover una cultura de seguridad en las organizaciones, se logra mitigar vulnerabilidades, anticipar amenazas emergentes y responder eficazmente ante incidentes. Esta inversión en capital humano es esencial para la prosperidad y seguridad a largo plazo en la era digital.

Principales barreras que dificultan la adopción de prácticas de concienciación y educación en ciberseguridad, y cómo superarlas

Son diversas las principales barreras que dificultan adoptar prácticas de concienciación y educación en ciberseguridad, sin embargo, existen formas de superarlas. A continuación se hace mención de algunas barreras y se analiza el modo de abordarlas:

1.- Falta de prioridad y compromiso a nivel organizacional:

Barrera: no se considera la ciberseguridad una prioridad estratégica por parte de la alta dirección, lo que conlleva a la falta de asignación de recursos y apoyo para estos esfuerzos.

Solución: demostrar a la alta gerencia el impacto financiero y reputacional de los incidentes de ciberseguridad para convencer a los ejecutivos de la importancia de la concienciación y educación y lograr el compromiso y liderazgo de los mismos.

2.- Percepción de la ciberseguridad como un problema exclusivo de los expertos:

Barrera: muchas organizaciones y usuarios finales consideran que la ciberseguridad es responsabilidad únicamente de los profesionales de TI o el departamento de seguridad.

Solución: transmitir el mensaje de que la ciberseguridad es una responsabilidad compartida, donde todos los miembros de la organización deben participar y ser conscientes de sus roles y acciones.

3.- Falta de recursos y presupuesto:

Barrera: las organizaciones, especialmente las pymes, a menudo carecen de los recursos financieros y humanos necesarios para implementar programas de concienciación y educación robustos.

Solución: buscar alternativas de bajo costo, como materiales educativos gratuitos, programas gubernamentales de asistencia y alianzas con proveedores de seguridad. Además, demostrar el retorno de inversión a largo plazo de estas iniciativas.

4.- Resistencia al cambio y cultura organizacional renuente:

Barrera: algunas organizaciones y empleados presentan una actitud pasiva o desinteresada hacia los esfuerzos de concienciación y educación en ciberseguridad.

Solución: fomentar una cultura organizacional que valore la seguridad y la adopción de mejores prácticas. Esto implica la participación activa de la dirección, programas de incentivos y reconocimientos, y la integración de la ciberseguridad en los procesos y políticas de la organización.

5.- Contenidos y métodos de enseñanza poco atractivos:

Barrera: los programas de capacitación a menudo se perciben como aburridos, poco relevantes o difíciles de comprender para los participantes.

Solución: diseñar contenidos y actividades de aprendizaje interactivas, contextualizadas y basadas en escenarios reales. Utilizar enfoques como gamificación, videos y simulaciones para captar la atención y mejorar la retención de la información.

6.- Falta de actualización constante:

Barrera: las iniciativas de concienciación y educación suelen ser puntuales y no se mantienen actualizadas al ritmo de la evolución de las amenazas y tecnologías.

Solución: implementar programas de educación continua y actualización periódica de los materiales y recursos. Esto permite mantener a los usuarios y profesionales informados sobre los últimos desarrollos y mejores prácticas en ciberseguridad.

El abordar estas barreras de manera integral y sistemática es fundamental para lograr una adopción efectiva y sostenible de las prácticas de concienciación y educación en ciberseguridad. Esto requiere el compromiso y esfuerzo conjunto de líderes, profesionales de seguridad, educadores y todos los miembros de la organización.

Medir el impacto y la efectividad de los esfuerzos de concienciación y educación en ciberseguridad

Esta medición es importante para evaluar su eficacia e implementar mejoras continuas. Algunas maneras de medir este impacto incluyen:

1.- Evaluaciones de conocimiento y habilidades:

Realizar evaluaciones previas y posteriores a los programas de capacitación para medir el nivel de conocimiento y habilidades adquiridas por los participantes (Humiston & Miller, 2021).

Esto permite determinar si los contenidos y métodos de enseñanza están siendo efectivos.

2.- Indicadores de comportamiento:

Monitorear cambios en los comportamientos y prácticas de los usuarios, como el cumplimiento de políticas de seguridad, la adopción de controles de seguridad y la reducción de incidentes relacionados con errores humanos (Safa et al., 2018).

Estos indicadores reflejan si los esfuerzos de concienciación y educación han generado un impacto positivo en las acciones de los usuarios.

3.- Métricas de concientización y participación:

Registrar la tasa de participación en las actividades de capacitación, el nivel de interacción con los materiales educativos y el grado de compromiso de los usuarios (Greitzer et al., 2014).

Estas métricas ayudan a comprender el alcance y la receptividad de los programas de concienciación.

4.- Análisis de incidentes de seguridad:

Evaluar y analizar la evolución de los incidentes de seguridad, como ataques exitosos o intentos de phishing, y determinar si han disminuido después de los esfuerzos de concienciación (Posey et al., 2014).

Esto proporciona una indicación del impacto en la reducción de riesgos.

5.- Encuestas y retroalimentación de los usuarios:

Recopilar comentarios y opiniones de los usuarios sobre la relevancia, claridad y utilidad de los programas de concienciación y educación (Bouwman et al., 2018).

Esta información cualitativa puede aportar valiosos insights para mejorar los enfoques y contenidos futuros.

6.- Evaluación del retorno de inversión (ROI):

Calcular el retorno de inversión de los esfuerzos de concienciación y educación, considerando factores como la reducción de incidentes, ahorro de costos y mejora de la reputación organizacional (Gordon et al., 2015). Esto permite justificar la asignación de recursos y demostrar el valor de estas iniciativas.

La combinación de estas métricas cuantitativas y cualitativas proporcionará una evaluación integral del impacto y la efectividad de los programas de concienciación y educación en ciberseguridad. Realizar evaluaciones periódicas y ajustar los enfoques según los resultados obtenidos, es importante con el fin de optimizar continuamente estos esfuerzos.

Uso seguro de tecnologías y herramientas digitales en el aula

La integración de tecnologías digitales en los entornos educativos ha traído consigo numerosos beneficios para mejorar los procesos de enseñanza y aprendizaje (Zheng et al., 2016). Sin embargo, el uso de estas tecnologías también plantea desafíos en términos de seguridad y privacidad que deben abordarse con cautela. Los educadores tienen la responsabilidad de garantizar que los estudiantes puedan aprovechar los recursos tecnológicos de manera segura y responsable dentro del aula (Dainton, 2020).

Un aspecto clave es la protección de la información y los datos de los estudiantes. Las herramientas digitales, como plataformas de aprendizaje en línea, aplicaciones y servicios en la nube, a menudo requieren que los estudiantes brinden información personal, como nombres, direcciones de correo electrónico y datos de rendimiento académico (Pynoo & van Braak, 2014). Los educadores deben asegurarse de que estas plataformas y servicios cumplan con las normas de seguridad y privacidad apropiadas, y que la información de los estudiantes se maneje de manera adecuada y se proteja contra el acceso no autorizado (Selwyn, 2016).

Además, los estudiantes deben aprender a navegar de manera segura en Internet y a identificar posibles amenazas, como sitios web maliciosos, correo electrónico no deseado y contenido inapropiado (Hadlington, 2017). Los educadores pueden integrar lecciones y actividades que fomenten el desarrollo de habilidades de navegación segura, como reconocer

señales de sitios web de confianza, evitar descargas sospechosas y comunicarse de forma prudente en línea (Hollett & Ehret, 2020).

Otro aspecto importante es la prevención del acoso y el ciberacoso en el entorno digital del aula. El uso de redes sociales, foros de discusión y herramientas de comunicación en línea puede facilitar la propagación de contenido dañino y conductas abusivas (Görzig & Ólafsson, 2013). Los educadores deben implementar políticas y estrategias para promover un clima de respeto y tolerancia, y enseñar a los estudiantes a reconocer y denunciar comportamientos inapropiados en línea (Livingstone & Smith, 2014).

Asimismo, es decisivo abordar el tema de la propiedad intelectual y el uso ético de los recursos digitales. Los estudiantes deben aprender a respetar los derechos de autor, citar adecuadamente las fuentes y evitar el plagio al utilizar contenido en línea para sus trabajos y proyectos (Ribble, 2015). Los educadores pueden implementar talleres y actividades que desarrollen la conciencia sobre estos temas y ayuden a los estudiantes a adquirir hábitos de uso responsable de la información digital (Hobbs & Jensen, 2009).

Por otra parte, la seguridad física de los dispositivos tecnológicos utilizados en el aula también merece atención. Los educadores deben asegurarse de que los equipos, como computadoras, tabletas y teléfonos, se mantengan en buen estado y se protejan contra daños, pérdida o robo (Jimoyiannis & Komis, 2007). Deben establecer pautas claras para el manejo y almacenamiento seguro de estos dispositivos, y capacitar a los estudiantes en prácticas de cuidado y mantenimiento.

Igualmente, la seguridad cibernética también implica abordar aspectos relacionadas con el uso adecuado de las redes y sistemas informáticos en el entorno educativo. Los educadores deben asegurarse de que las conexiones a Internet y las redes de la institución educativa cuenten con medidas de seguridad sólidas, como firewalls, antivirus y políticas de acceso (Livingstone et al., 2017). Deben educar a los estudiantes sobre la importancia de mantener contraseñas seguras, evitar el uso compartido de credenciales y denunciar actividades sospechosas en los sistemas.

Finalmente, los educadores requieren mantenerse actualizados sobre las tendencias y amenazas emergentes en el campo de la seguridad digital, participar en programas de desarrollo profesional, leer publicaciones especializadas y estar atentos a los cambios en las políticas y regulaciones relacionadas con la seguridad y privacidad en el entorno educativo (Williamson, 2016). Esto les permitirá adaptar sus estrategias de enseñanza y orientar a los estudiantes de manera efectiva.

El uso seguro de tecnologías y herramientas digitales en el aula es básico para aprovechar los beneficios de la integración tecnológica en la educación, al tiempo que se minimiza el riesgo de amenazas y se fomenta en los estudiantes una cultura de uso responsable y seguro de los recursos digitales. Los educadores desempeñan un papel decisivo en la implementación de medidas de seguridad, el desarrollo de habilidades digitales seguras y la promoción de un entorno de aprendizaje en línea protegido y saludable.

Herramientas y recursos disponibles para enseñar y aprender sobre ciberseguridad

Es importante destacar que existen múltiples recursos disponibles en el ámbito educativo, para enseñar y aprender sobre ciberseguridad y que pueden ayudar a impartir conocimientos

sólidos en este campo, dada la creciente dependencia de la tecnología y la vulnerabilidad de los sistemas a ataques cibernéticos. Uno de los enfoques más efectivos es la integración de módulos de ciberseguridad en los planes de estudio de diversas disciplinas, como informática, ingeniería, administración de empresas y ciencias sociales. Esto permite a los estudiantes comprender la importancia de la ciberseguridad desde una perspectiva interdisciplinaria (Cowan et al., 2021).

Una de las herramientas más destacadas para la enseñanza de la ciberseguridad son las plataformas de aprendizaje interactivo. Estas plataformas ofrecen escenarios de simulación, laboratorios virtuales y juegos educativos permitiendo a los estudiantes aplicar sus conocimientos en entornos seguros y controlados (Franke & Brynielsson, 2014). Algunas de estas herramientas, como Cybersecurity Lab y KYPO Cyber Range, han demostrado ser especialmente eficaces en el desarrollo de habilidades prácticas y la comprensión de conceptos clave (Franke & Brynielsson, 2014; Murali et al., 2020).

Además de las plataformas interactivas, los profesores pueden utilizar recursos en línea como tutoriales, videos educativos y cursos abiertos masivos en línea (MOOC) para complementar su enseñanza. Plataformas como Coursera, edX y Udemy ofrecen una amplia variedad de cursos de ciberseguridad, desde introductorios hasta avanzados, que pueden ayudar a los estudiantes a profundizar en temas específicos (Alagrad et al., 2019).

Para fomentar un aprendizaje más práctico, los docentes pueden organizar competiciones y desafíos de ciberseguridad, como hackathones y capture the flag (CTF). Estos eventos permiten a los estudiantes aplicar sus habilidades en escenarios realistas, desarrollar estrategias de resolución de problemas y trabajar en equipo (Cheung et al., 2021). Plataformas como HackTheBox y TryHackMe ofrecen una amplia variedad de desafíos CTF que pueden ser utilizados en el aula.

Más allá del ámbito educativo formal, existen numerosos recursos y comunidades en línea que pueden ayudar a los interesados a aprender sobre ciberseguridad de manera autónoma. Sitios web como SANS Institute, OWASP y CyberSecurityBase ofrecen tutoriales, artículos y recursos gratuitos sobre una amplia gama de temas relacionados con la ciberseguridad (Choi et al., 2018).

Asimismo, las redes sociales y los foros en línea, como Reddit's /r/netsec y Hacker News, permiten a los aprendices interactuar con profesionales del sector, intercambiar ideas y mantenerse actualizados sobre las últimas tendencias y amenazas cibernéticas (Choi et al., 2018).

Esta amplia variedad de herramientas y recursos disponibles para enseñar y aprender sobre ciberseguridad, desde plataformas de aprendizaje interactivo hasta cursos en línea y comunidades de práctica, pueden ayudar a los educadores a impartir conocimientos sólidos y a los estudiantes a desarrollar habilidades prácticas en este campo tan esencial. Al integrar estas herramientas en los planes de estudio y fomentar un aprendizaje activo y participativo, podemos preparar mejor a la próxima generación de profesionales en ciberseguridad.

A continuación se proporcionan algunos ejemplos específicos de plataformas de aprendizaje interactivo que pueden utilizar los educadores para enseñar ciberseguridad de manera efectiva en el aula. Estas herramientas permiten a los estudiantes aplicar sus conocimientos teóricos en escenarios prácticos, fomentando así un aprendizaje más profundo y comprensivo de los conceptos clave de la ciberseguridad:

Cybersecurity Lab: desarrollada por la Universidad de Illinois en Chicago ofrece laboratorios virtuales y escenarios de simulación que permiten a los estudiantes practicar técnicas de hacking ético, análisis forense digital y respuesta a incidentes. Los estudiantes pueden enfrentarse a ataques realistas en un entorno seguro y controlado (Franke & Brynielsson, 2014).

KYPO Cyber Range: es una plataforma desarrollada por la Universidad de Masaryk en la República Checa, que permite a los estudiantes participar en ejercicios de ciberseguridad a gran escala. Incluye herramientas de monitoreo, registro y análisis que ayudan a los estudiantes a comprender cómo funciona la defensa y la respuesta a incidentes en la vida real (Murali et al., 2020).

PicoCTF: esta competición en línea organizada por Carnegie Mellon University presenta una serie de desafíos de captura de banderas (CTF) diseñados para enseñar conceptos de ciberseguridad a estudiantes de secundaria y universitarios. Los participantes deben resolver problemas relacionados con seguridad web, criptografía, ingeniería inversa y más (Cheung et al., 2021).

Hacker101: desarrollado por HackerOne, es una plataforma de aprendizaje gratuita que ofrece cursos interactivos, videos tutoriales y desafíos CTF para ayudar a los estudiantes a desarrollar habilidades de hacking ético. Cubre temas como inyección SQL, vulnerabilidades XSS y seguridad en aplicaciones web (Choi et al., 2018).

TryHackMe: esta plataforma en línea proporciona salas de aprendizaje interactivas y desafíos CTF que permiten a los estudiantes practicar técnicas de penetración y defensa en un entorno seguro. Cuenta con una amplia variedad de rutas de aprendizaje, desde introductorias hasta avanzadas (Cheung et al., 2021).

Además de los ejemplos mencionados anteriormente, existen otros ejemplos de plataformas de aprendizaje interactivo que se pueden utilizar para enseñar ciberseguridad en el aula. Cada una de estas herramientas ofrece formas únicas de involucrar a los estudiantes y ayudarlos a desarrollar habilidades prácticas en un entorno seguro y controlado:

1. **Cyber Range Platforms** (Dawson& Thomson, 2018):

Cisco Networking Academy Cyber Range: plataforma de simulación de ciberataques y defensa desarrollada por Cisco, permite a los estudiantes practicar habilidades de ciberseguridad en un entorno virtual.

SEED Labs: desarrollado por la Universidad de Syracuse, SEED Labs es una colección de laboratorios de seguridad informática que cubren temas como inyección SQL, explotación de buffer, malware y más.

2. **Juegos y competencias** (Gondree, Peterson & Denning, 2013):

National Cyber League (NCL): competencia nacional de captura de banderas (CTF) que desafía a los estudiantes a resolver problemas de ciberseguridad.

CyberPatriot: programa de concientización y competencia en ciberseguridad patrocinado por la Fuerza Aérea de EE. UU. y AFCEA.

Capture the Packet (CTP): competencia de seguridad de redes en la que los equipos deben capturar paquetes de red y resolver desafíos relacionados.

3. **Plataformas de simulación y juegos serios** (Nagarajan et al., 2012):

SecAdventure: juego de simulación de ciberseguridad desarrollado por el SANS Institute, que coloca a los jugadores en el papel de un equipo de respuesta a incidentes.

CyberStrike: entorno de simulación de ciberataques y defensa desarrollado por la Universidad de Arizona.

Cyber City: entorno de simulación de ciudad inteligente que permite a los estudiantes practicar la defensa contra ciberataques.

4. **Plataformas de aprendizaje en línea** (Jang-Jaccard & Nepal, 2014):

Cybrary: plataforma de aprendizaje en línea que ofrece cursos, recursos y certificaciones en ciberseguridad.

edX Cybersecurity MicroMasters: programa de aprendizaje en línea de nivel de posgrado en ciberseguridad.

Udemy Cybersecurity Courses: amplia variedad de cursos interactivos de ciberseguridad en la plataforma Udemy.

Referencias Bibliográficas

Alagrad, E., Heckman, C., & Shue, C. (2019). Delivering cybersecurity education online. IEEE *Security & Privacy*, 17(3), 16-21. https://doi.org/10.1109/MSEC.2019.2907247

Alaskar, H., Alharbi, A., Alshehri, M., & Chaudhry, J. (2020). *Cybersecurity Awareness and Behaviors: A Theory-Based Study*. IEEE Access, 8, 115847-115855. https://doi.org/10.1109/ACCESS.2020.3004781

Aldawood, H., & Skinner, G. (2019). *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature* Review. In 2019 IEEE Conference on Application, Information and Network Security (AINS) (pp. 41-46). IEEE. https://doi.org/10.1109/AINS47559.2019.8968789

Bada, M., & Sasse, A. M. (2014). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*. In International Conference on Cyber Security for Sustainable Society (pp. 118-131).

Barona, R., & Anita, M. R. (2017). *Detection and Prevention Mechanisms to Counter Internal Threats in Higher Education Institutions*. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 593–598. https://doi.org/10.1109/I-SMAC.2017.8058427

Bouwman, R., Bommel, S. V., Bosma, B., Brinkhuis, M., & Riel, R. V. (2018). Cyber security awareness: A survey of informed citizens in the Netherlands. *Computers & Security*, 77, 815-825.

Cheung, A., Yang, S., Huynh, K., & Looi, C. K. (2021). *Designing and implementing a capture the flag competition for cybersecurity education*. Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education, 301-307. https://doi.org/10.1145/3430665.3456382

Choi, J., Song, H. J., & Park, J. (2018). *A study on the improvement of cybersecurity awareness training effectiveness using personalized learning*. Proceedings of the 10th International Conference on Ubiquitous and Future Networks, 705-707. https://doi.org/10.1109/ICUFN.2018.8436763

Cowan, B. R., Razak, S. A., Gallagher, S., & Munteanu, C. (2021). *Designing cybersecurity education and training programs: A sociotechnical approach*. IEEE Access, 9, 28910-28923. https://doi.org/10.1109/ACCESS.2021.3058830

Dainton, S. (2020). Cybersecurity in education: A review of the issues. *Computers & Security*, 95, 101790. https://doi.org/10.1016/j.cose.2020.101790

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in psychology*, 9, 744. https://doi.org/10.3389/fpsyg.2018.00744

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness - A systematic review of the literature. *Computers & Security*, 46, 18-31. https://doi.org/10.1016/j.cose.2014.06.008

Geer, D. (2020). Cybersecurity in Education. *Computer*, 53(5), 96–101. https://doi.org/10.1109/MC.2020.2985902

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security Threats to Critical Infrastructure: The Human Factor. *The Journal of Supercomputing*, 74(10), 4986–5002. https://doi.org/10.1007/s11227-018-2337-2

Gondree, M., Peterson, Z. N., & Denning, T. (2013). Security through play. IEEE *Security & Privacy*, 11(3), 64-67.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security*, 6(01), 24.

Görzig, A., & Ólafsson, K. (2013). What makes a bully a cyberbully? Unraveling the characteristics of cyberbullies across twenty-five European countries. *Journal of children and media*, 7(1), 9-27. https://doi.org/10.1080/17482798.2012.739756

Greitzer, F. L., Strozer, J. R., Cohen, S., Bergey, J., Cowley, J., Moore, A. P., & Mundie, D. (2014). Unintended insider threat: Analysis and implications from a retrospective case study. In 2014 47th Hawaii International *Conference on System Sciences* (pp. 2025-2034). IEEE.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hobbs, R., & Jensen, A. (2009). The past, present, and future of media literacy education. *Journal of media literacy education*, 1(1), 1-11. https://digitalcommons.uri.edu/jmle/vol1/iss1/1/

Hollett, T., & Ehret, C. (2020). Affective dimensions of young people's digital participation: Considering curriculum, pedagogy, and digital praxis. *Curriculum Inquiry*, 50(1), 80-101. https://doi.org/10.1080/03626784.2019.1694061

Humiston, G. H., & Miller, S. M. (2021). Assessing the Effectiveness of Cybersecurity Training Programs. Journal of Cybersecurity Education, *Research and Practice*, 2021(1), 3.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.

Jimoyiannis, A., & Komis, V. (2007). Examining teachers' beliefs about ICT in education: Implications of a teacher preparation programme. *Teacher development*, 11(2), 149-173. https://doi.org/10.1080/13664530701414779

Kritzinger, E., & von Solms, S. H. (2010). Cyber Security for Home Users: A New Way of Protection Through Awareness Enforcement. *Computers & Security*, 29(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

Kruger, H. A., & Drevin, L. (2022). *Cybersecurity Awareness and Education in the Education Sector.* In A. Joshi, M. Mahmoud, & S. Srivastava (Eds.), Handbook of Research on Cybersecurity Awareness in the Digital Economy (pp. 367–384). IGI Global. https://doi.org/10.4018/978-1-7998-8231-6.ch017

Livingstone, S., Mascheroni, G., & Staksrud, E. (2017). European research on children's internet use: Assessing the past and anticipating the future. *New media & society*, 20(3), 1103-1122. https://doi.org/10.1177/1461444816685930

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, 55(6), 635-654. https://doi.org/10.1111/jcpp.12197

Murali, R., Narayanan, S., Boopathi, K., Karthikeyan, N., & Magesh, E. (2020). *Cybersecurity education and training: A review of the literature*. Proceedings of the International Conference on Inventive Computation and Information Technologies, 243-248. https://doi.org/10.1109/ICICIT49469.2020.9116275

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). *Exploring game design for cybersecurity training.* In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (pp. 256-262). IEEE.

NIST. (2022). *Cybersecurity Framework*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Pynoo, B., & van Braak, J. (2014). Predicting teachers' generative and receptive use of an educational portal by intention, attitude and self-reported use. *Computers in Human Behavior*, 34, 315-322.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organisational insiders. *Information & Management*, 51(5), 551-567.

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of information security and applications*, 40, 247-257.

Selwyn, N. (2016). *Is technology good for education?* Polity Press.

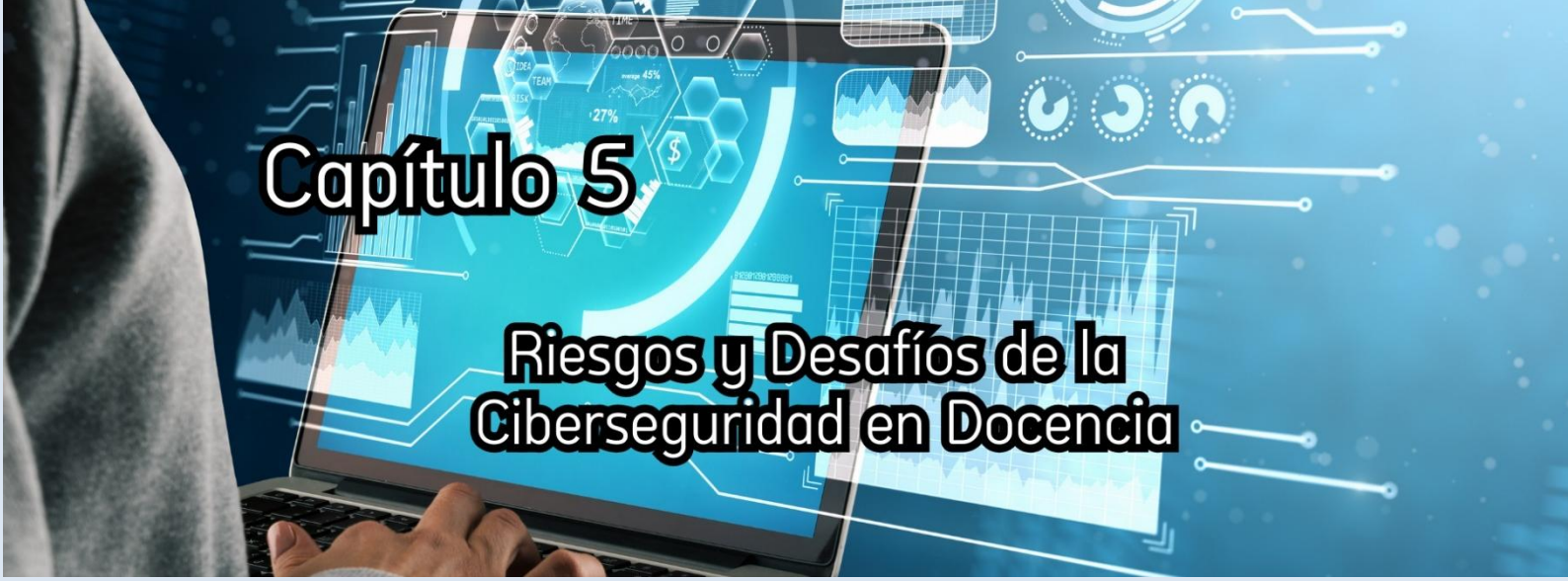
Shaikh, A. A., & Singla, A. (2021). Cybersecurity Awareness among Students: A Challenge for the Education System. *Studies in Indian Place Names*, 41(69), 3238–3249.

Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.

Van Niekerk, J. F., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computers & Security*, 29(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Williamson, B. (2016). Digital education governance: data visualization, predictive analytics, and 'real-time' policy instruments. *Journal of Education Policy*, 31(2), 123-141.

Zheng, L., Cui, P., Li, X., & Huang, R. (2016). Integrating a mobile learning application into contextual learning. *Journal of Educational Technology & Society*, 19(1), 194-205.



Alex Sandro Landeo Quispe ✉ 1, **Vladimir Orihuela Rojas** ✉ 1, **Fernando Pool Orihuela Rojas** ✉, **& Johanna Rosa Velarde Samaniego** ✉ 2

1. Universidad Nacional de Huancavelica, Perú - 2. Universidad Tecnológica del Perú

La ciberseguridad ha emergido como una preocupación central en la educación, a medida que tanto instituciones como estudiantes dependen cada vez más de las tecnologías digitales para todo lo relacionado con el aprendizaje y la investigación. Esta dependencia sin duda, tiene muchos beneficios, pero también conlleva importantes riesgos significativos: los sistemas de información educativos son blancos atractivos para los ciberdelincuentes que buscan robar datos personales, interrumpir las operaciones o incluso manipular el contenido del plan de estudios. Además, la rápida evolución de las amenazas cibernéticas y la falta de personal capacitado en seguridad informática presentan desafíos considerables para los educadores. Integrar prácticas y herramientas sólidas de ciberseguridad en los entornos de aprendizaje se ha vuelto imperativo para salvaguardar a estudiantes, profesores e instituciones de posibles daños potenciales. Abordar estos riesgos y desafíos es decisivo para garantizar que la tecnología contribuya de manera segura y responsable a mejorar los resultados educativos.

Uno de los mayores riesgos es el robo de información confidencial, como registros académicos, datos financieros y detalles de contacto de estudiantes y personal. Esta información tiene un alto valor en el mercado negro y puede utilizarse para fines de fraude o extorsión. Los ataques de ransomware también representan una grave amenaza, ya que pueden bloquear el acceso a sistemas críticos e interrumpir el aprendizaje. Además, los hackers podrían intentar manipular el contenido de los cursos o modificar las calificaciones, lo que socavaría la integridad de los programas educativos.

Más allá de enfrentar las amenazas externas, las propias instituciones corren el riesgo de comprometer la seguridad debido a errores y descuidos internos. El uso de contraseñas débiles, la falta de copias de seguridad adecuadas y los sistemas desactualizados representan vulnerabilidades comunes que pueden facilitar el acceso no autorizado a los datos sensibles. Pero, además, la pandemia de COVID-19 ha traído consigo nuevos desafíos que han ampliado aún más el perímetro de seguridad que se debe proteger. El aumento repentino del teletrabajo y el aprendizaje a distancia nos ha expuesto a riesgos como el acceso remoto inseguro y el uso de dispositivos personales sin la debida protección.

A esto, se une la escasez de profesionales de seguridad informática capacitados y la dificultad para retener a este personal altamente demandado dificultan que las instituciones

educativas mantengan una defensa sólida contra las amenazas cibernéticas. Por otro lado, la falta de concientización y capacitación adecuada del personal y los estudiantes sobre las mejores prácticas de ciberseguridad también aumenta la vulnerabilidad.

Para abordar estos riesgos y desafíos, las instituciones educativas deben adoptar un enfoque holístico que combine tecnología, procesos y personas. Esto implica invertir en soluciones de seguridad robustas, como firewalls, sistemas de detección de intrusos y herramientas de cifrado. Abordar estos riesgos y desafíos permite garantizar que la tecnología cumpla con su promesa de mejorar los resultados educativos de manera segura y responsable, de este modo se podrán aprovechar al máximo los beneficios de la transformación digital en el ámbito de la educación

Protección de Datos de los Estudiantes y la Confidencialidad de la Información

A medida que las instituciones recopilan, procesan y almacenan cada vez más información sobre sus alumnos, desde registros académicos hasta detalles de salud y contacto, surge la imperiosa necesidad de implementar salvaguardas adecuadas para preservar la privacidad y la confidencialidad de estos datos sensibles.

La información personal de los estudiantes, como nombres, números de identificación, calificaciones, historial médico y detalles familiares, tiene un valor incalculable y debe ser protegida con el máximo celo. Un posible incidente de seguridad que resulte en la fuga o el robo de estos datos podrían tener graves consecuencias, tanto para las instituciones como para los propios alumnos. Los estudiantes y sus familias podrían sufrir daños emocionales, estigmatización social y, en casos extremos, incluso ser víctimas de fraude o acoso. Además, las instituciones educativas enfrentarían sanciones legales, pérdida de reputación y la erosión de la confianza de la comunidad.

Según un estudio realizado por la Comisión Federal de Comercio de los Estados Unidos, los menores de edad son particularmente vulnerables a los delitos cibernéticos, como el robo de identidad, ya que sus datos personales a menudo permanecen sin usar durante años, lo que los convierte en un objetivo atractivo para los delincuentes (FTC, 2014). Esto subraya la importancia de que las escuelas, colegios y universidades adopten medidas rigurosas para proteger la información de sus estudiantes.

Una de las principales barreras legales y éticas que enfrentan las instituciones educativas es la necesidad de equilibrar la recopilación y el uso de datos de los estudiantes con el respeto a su privacidad. Leyes como el Acta de Derechos Educativos y Privacidad Familiar (FERPA) en los Estados Unidos y el Reglamento General de Protección de Datos (RGPD) en la Unión Europea, establecen estrictos requisitos sobre cómo se deben manejar y proteger los datos personales de los estudiantes (U.S. Department of Education, 2020; Comisión Europea, 2016). Estos marcos normativos exigen que las instituciones obtengan el consentimiento de los estudiantes (o de sus padres, en el caso de menores) antes de recopilar y utilizar sus datos, y que implementen salvaguardas sólidas para evitar brechas de seguridad.

Para cumplir con estos requisitos legales y éticos, las instituciones educativas deben adoptar un enfoque integral de gestión de datos que abarque todas las etapas del ciclo de vida de la información, desde la recopilación hasta la eliminación. Esto incluye implementar políticas y

procedimientos claros para la recolección, el almacenamiento, el acceso y la divulgación de los datos de los estudiantes. Además, es fundamental contar con controles técnicos robustos, como cifrado de datos, autenticación de usuarios y copias de seguridad periódicas.

Un ejemplo de buenas prácticas en este sentido es la Política de Privacidad y Protección de Datos de la Universidad de Cambridge, que establece pautas detalladas sobre cómo se deben manejar los datos personales de los estudiantes, desde el consentimiento hasta la eliminación segura (University of Cambridge, 2022). Asimismo, la Guía de Privacidad y Protección de Datos de la Asociación de Colegios y Universidades Americanos ofrece recomendaciones específicas para que las instituciones educativas cumplan con la normativa vigente (AACRAO, 2018).

Más allá de los requisitos legales, las instituciones también tienen la responsabilidad ética de garantizar la confidencialidad y la seguridad de la información de sus estudiantes. Esto implica no solo proteger los datos contra amenazas externas, sino también asegurarse de que el personal interno respete la privacidad de los alumnos y no utilice indebidamente la información a la que tiene acceso. La implementación de programas de concienciación y capacitación sobre la protección de datos, así como el establecimiento de códigos de conducta y sanciones claras, pueden ser estrategias efectivas para fomentar una cultura de responsabilidad y transparencia en torno al manejo de la información estudiantil.

Además, las instituciones deben estar preparadas para responder adecuadamente ante posibles brechas de seguridad. Esto significa contar con planes de respuesta a incidentes que permitan identificar, contener y mitigar rápidamente cualquier incidente que pueda comprometer los datos de los estudiantes. Igualmente, es crucial informar de manera oportuna y transparente a los afectados, así como a las autoridades competentes, para minimizar los daños y cumplir con los requisitos normativos. Entre algunas de las medidas específicas recomendadas a las instituciones educativas para proteger mejor los datos de los estudiantes destacan:

1.- Políticas y Procedimientos Claros:

- Establecer políticas internas detalladas sobre la recopilación, el uso, el almacenamiento y la eliminación de los datos estudiantiles.
- Definir roles y responsabilidades claras para el personal encargado del manejo de información.
- Implementar procedimientos estandarizados para atender solicitudes de acceso, rectificación y supresión de datos.

2.- Controles Técnicos Robustos:

- Utilizar sistemas de autenticación sólidos (por ejemplo, autenticación de dos factores) para restringir el acceso a los datos.
- Aplicar cifrado de datos en reposo y en tránsito para proteger la confidencialidad de la información.
- Mantener copias de seguridad periódicas y almacenarlas en ubicaciones seguras.
- Implementar soluciones de detección y prevención de intrusiones para monitorear actividad sospechosa.

3.- Capacitación y Concienciación:

- Ofrecer programas de capacitación obligatorios al personal sobre protección de datos y mejores prácticas de ciberseguridad.

- Crear campañas de concienciación para estudiantes y familias sobre la importancia de la privacidad y seguridad de la información.
- Fomentar una cultura organizacional de responsabilidad y respeto por la confidencialidad de los datos.

4.- Gestión de Incidentes:

- Desarrollar un plan integral de respuesta a incidentes de seguridad, que incluya procedimientos de notificación, mitigación y recuperación.
- Realizar pruebas y simulacros periódicos para evaluar la efectividad del plan de respuesta.
- Designar a un equipo de respuesta a incidentes con roles y responsabilidades claramente definidos.

5.- Cumplimiento Normativo:

- Mantenerse actualizado sobre las regulaciones vigentes en materia de protección de datos (por ejemplo, FERPA, RGPD).
- Realizar auditorías periódicas para verificar el cumplimiento de las leyes y normativas aplicables.
- Designar a un oficial de protección de datos (o figura similar) que supervise el cumplimiento y asesore a la institución.

6.- Colaboración y Transparencia:

- Establecer canales de comunicación abiertos con estudiantes, familias y autoridades sobre cuestiones de privacidad y seguridad.
- Participar en redes y foros de intercambio de mejores prácticas con otras instituciones educativas.
- Informar de manera oportuna y transparente sobre cualquier incidente de seguridad que pueda afectar a los datos de los estudiantes.

Protección de datos de los docentes y la confidencialidad de la información

La protección de los datos personales de los docentes y la confidencialidad de la información que manejan en el ejercicio de sus funciones es un aspecto fundamental en el ámbito educativo. Los docentes, como trabajadores de instituciones educativas, poseen una gran variedad de información sensible relacionada con su situación laboral, desempeño, evaluaciones, historial médico, entre otros datos personales y profesionales. Esta información debe ser tratada con el mayor cuidado y respeto por parte de las instituciones, a fin de garantizar los derechos de privacidad y seguridad de los docentes.

Uno de los principales desafíos en este sentido es el cumplimiento de la normativa vigente en materia de protección de datos. A nivel internacional, se han desarrollado diversos instrumentos legales que buscan regular el tratamiento de los datos personales, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México (LFPDPPP). Estas normativas establecen una serie de principios, derechos y obligaciones que las instituciones educativas deben cumplir al momento de recopilar, utilizar, almacenar y transferir los datos de

sus docentes (Comisión Europea, 2016; Cámara de Diputados del H. Congreso de la Unión, 2010).

En este contexto, las instituciones educativas deben implementar políticas y procedimientos internos que garanticen la confidencialidad y seguridad de los datos de los docentes. Esto implica, por ejemplo, definir claramente los roles y responsabilidades del personal encargado del manejo de esta información, establecer mecanismos de consentimiento informado, limitar el acceso a los datos únicamente a quienes lo requieran por razones justificadas, y adoptar medidas técnicas y organizativas para prevenir el uso indebido, la pérdida, alteración o acceso no autorizado a los datos (Agencia Española de Protección de Datos, 2018).

De igual manera, las instituciones deben brindar capacitación y sensibilización constante a todo su personal sobre la importancia de la protección de datos, las políticas y procedimientos internos, y las consecuencias del incumplimiento. Es fundamental que los docentes conozcan y comprendan sus derechos en materia de privacidad, así como los mecanismos disponibles para ejercer control sobre sus datos personales (Valero Torrijos, 2015).

Otro aspecto relevante es la gestión adecuada de los incidentes de seguridad que puedan afectar a los datos de los docentes. Las instituciones deben estar preparadas para responder de manera oportuna y efectiva ante cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de esta información. Esto implica contar con planes de contingencia, protocolos de notificación a las autoridades competentes y a los titulares de los datos, así como procedimientos de mitigación y recuperación (Agencia Española de Protección de Datos, 2020).

Es importante destacar que la protección de los datos de los docentes no solo responde a un imperativo legal, sino que también tiene implicaciones éticas y prácticas. Desde una perspectiva ética, la privacidad y la confidencialidad son derechos fundamentales que deben ser respetados y salvaguardados por las instituciones educativas, en consonancia con los principios de dignidad, autonomía y no discriminación (Vargas Martínez, 2017). Desde una perspectiva práctica, la adecuada gestión de la información de los docentes contribuye a generar un clima de confianza y bienestar, lo cual se traduce en una mejor calidad del servicio educativo y un mayor compromiso por parte de los docentes (Besnoy y Horton, 2022).

La protección de los datos de los docentes y la confidencialidad de la información que manejan es, sin duda, uno de los grandes desafíos a los que se enfrentan las instituciones educativas en la actualidad. Sólo a través de un enfoque integral y sostenido de la protección de datos, las instituciones educativas podrán consolidar una cultura de respeto y seguridad de la información que redunde en beneficio de toda la comunidad educativa. En este contexto, los docentes también tienen un papel protagónico que desempeñar.

Ellos pueden ejercer de manera activa sus derechos de privacidad y control sobre sus datos personales en el ámbito laboral, por ejemplo:

1.- Derecho de acceso:

- Los docentes tienen derecho a solicitar a la institución educativa información sobre qué datos personales suyos se están tratando, con qué finalidad, quiénes tienen acceso a ellos, y bajo qué criterios se están tratando.
- La institución debe proporcionar esta información de manera gratuita y en un plazo razonable.

2.- Derecho de rectificación:

- Si los docentes detectan que sus datos personales son inexactos, incompletos o están desactualizados, pueden solicitar a la institución que los rectifique.
- La institución debe atender esta solicitud y realizar las modificaciones pertinentes en un plazo determinado.

3.- Derecho de supresión ("derecho al olvido"):

- Los docentes pueden pedir a la institución que elimine o suprima sus datos personales cuando ya no sean necesarios para los fines para los que fueron recabados, o cuando el tratamiento sea ilícito.
- La institución debe proceder a la supresión, salvo que existan razones legítimas que justifiquen mantener los datos.

4.- Derecho de oposición:

- Los docentes pueden oponerse al tratamiento de sus datos personales cuando existan motivos relacionados con su situación particular, como cuando el tratamiento no sea necesario para el cumplimiento de una obligación legal o de un contrato.
- La institución debe atender esta oposición, a menos que acredite motivos imperiosos que justifiquen el tratamiento.

5.- Derecho a la portabilidad:

- Los docentes pueden solicitar a la institución que les proporcione una copia de sus datos personales en un formato estructurado, de uso común y lectura mecánica.
- Esto permite a los docentes transferir sus datos a otra institución o conservarlos para su propio uso.

6.- Derecho a presentar reclamaciones:

- Si los docentes consideran que la institución no está tratando adecuadamente sus datos personales, pueden presentar una reclamación ante la autoridad de protección de datos competente.
- Esto permite a los docentes activar los mecanismos de supervisión y sanción previstos en la normativa de protección de datos.

Es importante que las instituciones educativas informen a los docentes sobre estos derechos y establezcan procedimientos ágiles y transparentes para su ejercicio. Además, deben garantizar que no habrá represalias ni consecuencias negativas para los docentes que decidan ejercer sus derechos de privacidad.

Tendencias emergentes en la ciberseguridad en docencia

Siendo la ciberseguridad una prioridad en el campo de la educación, a medida que la digitalización de los procesos de enseñanza y aprendizaje avanza y en un mundo cada vez más interconectado, las instituciones educativas se enfrentan a una creciente amenaza de ciberataques que pueden comprometer la integridad de la información, la privacidad de los datos y la continuidad de las actividades académicas.

En este contexto, es fundamental que las instituciones educativas adopten un enfoque proactivo y actualizado en materia de ciberseguridad, a fin de hacer frente a las tendencias emergentes y salvaguardar el ecosistema digital en el que opera la docencia. A continuación, se examinan algunas de las principales tendencias y desafíos que se perfilan en este ámbito:

1.- Amenazas cibernéticas en evolución:

- Las técnicas y herramientas utilizadas por los cibercriminales están en constante evolución, lo que obliga a las instituciones educativas a mantener una vigilancia permanente y a actualizar continuamente sus mecanismos de protección. Desde sofisticados ataques de ransomware hasta campañas de phishing cada vez más sofisticadas, las amenazas cibernéticas se diversifican y se vuelven más difíciles de detectar y prevenir (Educause, 2022a; Kaspersky, 2021).

2.- Aumento de la superficie de ataque:

- La adopción acelerada de tecnologías digitales en la docencia, como el aprendizaje en línea, el uso generalizado de dispositivos móviles y la proliferación de aplicaciones y plataformas educativas, ha ampliado significativamente la superficie de ataque a la que están expuestas las instituciones. Cada nuevo dispositivo, software o servicio en línea representa una puerta de entrada potencial para los ciberdelincuentes (ENISA, 2020a; NIST, 2022).

3.- Vulnerabilidad de los datos:

- La cantidad y la sensibilidad de los datos personales y académicos manejados por las instituciones educativas (registros de estudiantes, calificaciones, información médica, etc.) los convierte en un objetivo apetecible para los ciberdelincuentes. El incumplimiento de las normativas de protección de datos puede acarrear graves consecuencias legales y reputacionales (GDPR, 2016; CCPA, 2018).

4.- Concienciación y capacitación insuficientes:

- A menudo, el eslabón más débil en la cadena de ciberseguridad son los propios usuarios, ya sean estudiantes, docentes o personal administrativo, que carecen de la formación adecuada en materia de ciberseguridad y pueden ser víctimas de engaños o ignorar los protocolos de seguridad (CISA, 2022; NIST, 2017).

5.- Escasez de personal especializado:

- La demanda de profesionales de la ciberseguridad altamente cualificados supera con creces la oferta, lo que dificulta que las instituciones educativas puedan contar con los expertos necesarios para implementar y mantener sistemas de seguridad eficaces (ISC2, 2021; (ISC)2, 2022).

6.- Integración de tecnologías emergentes:

- La adopción de tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y la computación en la nube en el contexto educativo plantea nuevos desafíos de ciberseguridad que deben abordarse mediante enfoques innovadores (ENISA, 2020b; NIST, 2022).

Para hacer frente a estas tendencias emergentes, las instituciones educativas deben adoptar un enfoque holístico y estratégico en materia de ciberseguridad. Algunas de las principales medidas a considerar son:

1.- Desarrollar y actualizar políticas y procedimientos de ciberseguridad:

- Las instituciones deben contar con políticas y procedimientos claros y actualizados que aborden aspectos como la gestión de identidades y accesos, la protección de

datos, la respuesta ante incidentes y la recuperación ante desastres (NIST, 2018; ISO/IEC 27001, 2013).

2.- Implementar controles de seguridad robustos:

- La adopción de medidas técnicas como el cifrado de datos, la autenticación multifactor, la segmentación de redes, la detección y respuesta a amenazas, y la gestión de vulnerabilidades, entre otras, es fundamental para fortalecer la postura de ciberseguridad (NIST, 2020; CIS, 2021).

3.- Fomentar la concienciación y la capacitación:

- Invertir en programas de sensibilización y formación en ciberseguridad dirigidos a estudiantes, docentes y personal administrativo, a fin de que puedan reconocer y mitigar eficazmente las amenazas cibernéticas (CISA, 2022; NIST, 2017).

4.- Atraer y retener talento especializado:

- Las instituciones deben desarrollar estrategias de reclutamiento y retención de profesionales de la ciberseguridad altamente cualificados, que puedan diseñar, implementar y mantener soluciones de seguridad eficaces (ISC2, 2021; (ISC)2, 2022).

5.- Adoptar un enfoque de ciberseguridad basado en el riesgo:

- Las instituciones deben evaluar de manera continua los riesgos cibernéticos a los que están expuestas y priorizar las inversiones y acciones de mitigación en función de dichos riesgos (NIST, 2018; ISO/IEC 27005, 2018).

6.- Colaborar y compartir información:

- Fomentar la colaboración entre instituciones educativas, organismos gubernamentales y expertos en ciberseguridad, a fin de intercambiar información sobre amenazas, mejores prácticas y lecciones aprendidas (ENISA, 2020; EDUCAUSE, 2022b).

Mediante la implementación de medidas estratégicas colaborativas interinstitucionales y la adopción de las últimas tendencias en ciberseguridad, las mismas podrán fortalecer su posición y hacer frente a los riesgos emergentes, garantizando así la continuidad y la seguridad de los procesos de enseñanza y aprendizaje, los recursos, los conocimientos y las mejores prácticas de todo el sector para abordar de manera más efectiva estos desafíos. Para enfrentarlos es necesaria la colaboración entre las instituciones y adoptar un enfoque holístico.

Algunas estrategias clave de colaboración incluyen:

1.- Intercambio de información y mejores prácticas:

- Las instituciones deben establecer redes y plataformas para compartir información sobre amenazas emergentes, vulnerabilidades, técnicas de mitigación y lecciones aprendidas.Esto permite que todas las instituciones se mantengan actualizadas y puedan implementar medidas preventivas de manera proactiva.

2.- Desarrollo conjunto de marcos y estándares:

- Las instituciones deben trabajar juntas para desarrollar marcos y estándares comunes de ciberseguridad que puedan aplicarse en todo el sector educativo.Esto garantiza la

interoperabilidad, la eficiencia y la coherencia en la implementación de las medidas de seguridad.

3.- Colaboración en actividades de capacitación y concientización:

- Las instituciones deben organizar programas de capacitación y actividades de concientización conjuntas para estudiantes, personal y administradores. Esto ayuda a crear una cultura de seguridad cibernética sólida en todo el sector.

4.- Desarrollo conjunto de soluciones técnicas:

- Las instituciones deben colaborar en el desarrollo y la implementación de soluciones técnicas, como sistemas de detección y prevención de intrusiones, herramientas de cifrado y planes de recuperación ante desastres. Esto aprovecha los recursos y conocimientos colectivos para lograr soluciones más eficaces y rentables.

5.- Colaboración en investigación y desarrollo:

- Las instituciones deben asociarse con centros de investigación, universidades y empresas tecnológicas para realizar investigaciones conjuntas sobre amenazas emergentes y nuevas tecnologías de ciberseguridad. Esto impulsa la innovación y el avance del conocimiento en todo el sector.

La ciberseguridad en el ámbito educativo representa un desafío que requiere la atención y los esfuerzos coordinados de todas las partes interesadas. A medida que la educación se vuelve más digital y dependiente de la tecnología, los riesgos de seguridad cibernética se multiplican de forma exponencial. Un factor clave que exacerba estos desafíos es la rápida evolución de las tecnologías y las tácticas de los ciberdelincuentes. A medida que las instituciones educativas implementan nuevas herramientas y plataformas para facilitar el aprendizaje y la colaboración, también se enfrentan a una carrera constante para mantener sus sistemas y protocolos de seguridad actualizados. Esto requiere una inversión significativa de recursos financieros y humanos, lo cual puede ser un desafío particularmente difícil para las instituciones con presupuestos limitados.

Coordinar políticas, procedimientos y respuestas de seguridad coherentes en todo el sistema puede ser una tarea ardua, especialmente cuando los intereses y prioridades de diferentes departamentos y partes interesadas entran en conflicto. Un elemento fundamental para abordar estos desafíos es involucrar y capacitar a toda la comunidad educativa, desde estudiantes y docentes hasta personal administrativo y de TI. Cultivar una cultura de conciencia y responsabilidad compartida en torno a la ciberseguridad es esencial, ya que los individuos a menudo representan el eslabón más débil en la cadena de seguridad.

En última instancia, abordar los riesgos y desafíos de la ciberseguridad en la docencia requerirá un enfoque holístico y colaborativo que involucre a todas las partes interesadas, desde los responsables de la toma de decisiones hasta los miembros de la comunidad educativa.

Referencias Bibliográficas

AACRAO (2018). *Privacy and Data Protection Guide*. Recuperado de https://www.aacrao.org/research-publications/guidelines/privacy-and-data-protection-guide

Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*. https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

Agencia Española de Protección de Datos. (2020). *Guía para la gestión y notificación de brechas de seguridad*. https://www.aepd.es/sites/default/files/2020-10/guia-gestion-notificacion-brechas.pdf

Besnoy, K. D., y Horton, L. (2022). Promoting teacher well-being and retention through ethical leadership. *Gifted Child Today*, 45(2), 105-111. https://doi.org/10.1177/10762175211064576

Cámara de Diputados del H. Congreso de la Unión. (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

CCPA. (2018). *California Consumer Privacy Act* (CCPA). Recuperado de https://oag.ca.gov/privacy/ccpa

CISA (Cybersecurity & Infrastructure Security Agency). (2022). *Cybersecurity Awareness Training*. Recuperado de https://www.cisa.gov/cybersecurity-awareness-training

CIS (Center for Internet Security). (2021). *CIS Controls v8*. Recuperado de https://www.cisecurity.org/controls/cis-controls-list

Comisión Europea. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

EDUCASE. (2022a). *Cybersecurity Trends in Higher Education*. Recuperado de https://www.educause.edu/research-and-publications/research/cybersecurity-trends-in-higher-education

EDUCAUSE. (2022b). *Horizon Report: 2022 Higher Education Edition*. Recuperado de https://www.educause.edu/horizon-report

ENISA (European Union Agency for Cybersecurity). (2020a). *Threat Landscape for Remote Workforce 2020*. Recuperado de https://www.enisa.europa.eu/publications/remote-workforce

ENISA. (2020b). *Cybersecurity in the Education Sector*. Recuperado de https://www.enisa.europa.eu/publications/cybersecurity-in-the-education-sector

FTC (2014). *Protegiendo la privacidad de los menores en línea*. Recuperado de https://www.ftc.gov/system/files/documents/plain-language/pdf-0031_protecting_kids_privacy_online_spanish.pdf

GDPR. (2016). *Reglamento General de Protección de Datos*. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679

ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements. Recuperado de https://www.iso.org/standard/54534.html

ISO/IEC 27005:2018. (2018). *Information technology — Security techniques — Information security risk management*. Recuperado de https://www.iso.org/standard/75281.html

ISC2 (International *Information System Security Certification Consortium). (2021). 2021 ISC2 Cybersecurity Workforce Study*. Recuperado de https://www.isc2.org/Research/Workforce-Study

(ISC)2 (International Information System Security Certification Consortium). (2022). 2022 (ISC)2 Cybersecurity Workforce Study. Recuperado de https://www.isc2.org/Research/Workforce-Study

Kaspersky. (2021). Cybersecurity Trends 2021: *The Year of Prolonged Uncertainty*. Recuperado de https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_Security_Bulletin_2021.pdf

NIST (National Institute of Standards and Technology). (2017). NIST Special Publication 800-50: *Building an Information Technology Security Awareness and Training Program*. Recuperado de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

NIST (National Institute of Standards and Technology). (2018). NIST Special Publication 800-37 Rev. 2: *Risk Management Framework for Information Systems and Organizations.* Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST (National Institute of Standards and Technology). (2020). NIST Special Publication 800-171: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

NIST (National Institute of Standards and Technology). (2022). *Cybersecurity for the Education Sector*. Recuperado de https://www.nist.gov/itl/applied-cybersecurity/nice/cybersecurity-education-sector

U.S. Department of Education (2020). *Family Educational Rights and Privacy Act* (FERPA). Recuperado de https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

University of Cambridge (2022). *Data Protection Policy*. Recuperado de https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation

Valero Torrijos, J. (2015). El régimen jurídico de la protección de datos personales en el ámbito del empleo público. *Revista Española de Derecho Administrativo*, (172), 47-74.

Vargas Martínez, E. E. (2017). Ética y privacidad de datos personales en el contexto de la era digital. IUS. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C.*, 11(39), 159-179. https://www.redalyc.org/journal/2932/293252078009/html/

Capítulo 6

Aplicabilidad de la Metodología MSSI en el Proceso Enseñanza Aprendizaje: Casos Prácticos

Fidel Castro Cayllahua ✉ 1, **Jaime Humberto Ortiz Fernández** ✉ 1
& Severo Simeon Calderón Samaniego ✉ 1

2. Universidad Peruana Los Andes, Huancayo, Junín, Perú

La Metodología MSSI (Metodología de Seguridad de la Información o también conocida como Modelo de Seguridad de Situaciones de Intrusión) es un enfoque que se utiliza para gestionar y proteger la seguridad de la información en organizaciones. Si bien su aplicación principal se centra en el ámbito empresarial, ofrece un marco integral para abordar los desafíos de ciberseguridad y protección de la información en diversos contextos, incluido el ámbito educativo. La implementación exitosa de la tecnología en el campo de la educación depende, en gran medida, de la adopción de metodologías y enfoques adecuados que permitan integrar de manera efectiva los recursos digitales en el proceso de enseñanza-aprendizaje

Desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, la metodología MSSI, se basa en un enfoque sistemático y adaptable para la gestión de la seguridad de la información. Esta metodología proporciona una serie de directrices y herramientas que pueden ser aplicadas a lo largo del ciclo de vida de los sistemas de información, desde la planificación y el diseño hasta la implementación, operación y mejora continua (NIST, 2018). En el contexto educativo, la adopción de la metodología MSSI puede ofrecer beneficios significativos al abordar los desafíos de ciberseguridad y la protección de datos de estudiantes, docentes y personal administrativo.

Uno de los principales pilares de la metodología MSSI es la evaluación y gestión de riesgos. Esto implica la identificación y análisis de las amenazas, vulnerabilidades y posibles impactos que pueden afectar a los sistemas de información de una institución educativa. A partir de este análisis, se pueden establecer estrategias y controles de seguridad adecuados para mitigar y gestionar eficazmente los riesgos identificados (ISO/IEC 27005, 2018). Esta aproximación permite a las instituciones educativas desarrollar una visión integral de su postura de seguridad y tomar decisiones informadas sobre la implementación de medidas de protección.

Otro aspecto clave de la metodología MSSI es la implementación de un sistema de gestión de la seguridad de la información (SGSI) (ISO/IEC 27001, 2013). Este sistema proporciona un marco estructurado para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente la seguridad de la información en una organización. En el contexto educativo, la adopción de un SGSI puede ayudar a las instituciones a definir y

documentar políticas, procedimientos y controles de seguridad específicos para su entorno, garantizando así la protección adecuada de los datos y activos de información críticos.

Implementar la metodología MSSI en un entorno educativo implica seguir una serie de pasos e involucrar a todas las partes interesadas relevantes y mantener una comunicación abierta para garantizar una aplicación efectiva y exitosa sobre la seguridad de la información, así como adaptarlos a las necesidades y recursos disponibles de cada institución educativa. A continuación, los pasos clave para efectuar la metodología MSSI en un entorno educativo:

1.- Evaluación inicial: realizar una evaluación exhaustiva de la situación actual en términos de seguridad de la información en el entorno educativo. Se identifican los activos de información, los riesgos y las posibles vulnerabilidades. Esto puede incluir la revisión de políticas existentes, la evaluación de los sistemas y aplicaciones utilizados, y la identificación de las necesidades y requisitos de seguridad (ISACA, 2019: ISO/IEC 27001,2013).

2.- Definición de objetivos y políticas: se establecen objetivos claros para la seguridad de la información en el entorno educativo. Estos objetivos deben ser realistas, alcanzables y alineados con los objetivos generales de la institución educativa. Además, desarrollar políticas de seguridad de la información que establezcan las normas y los procedimientos para proteger los activos de información y mitigar los riesgos identificados (Susanto et al., 2011).

3.- Diseño de controles de seguridad: basándose en los objetivos y las políticas establecidas, se diseñan los controles de seguridad necesarios para proteger la información. Esto incluye controles técnicos, como firewalls, sistemas de detección de intrusos y cifrado de datos, así también controles organizativos, como la asignación de responsabilidades, la capacitación y la concienciación en seguridad (Calder & Watkins, 2010; Whitman & Mattord, 2017).

4.- Implementación de controles: implica la configuración de sistemas y aplicaciones, la instalación, la configuración de hardware y software de seguridad, la capacitación del personal educativo y los estudiantes sobre el uso adecuado de los controles (EDUCAUSE, 2021; ISACA, 2021; SANS Institute, 2021).

5.- Monitoreo y evaluación: establecer un proceso de monitoreo donde se realizan evaluaciones periódicas de seguridad para identificar posibles brechas o debilidades y tomar medidas correctivas. Además, mantener actualizados los sistemas y aplicaciones de seguridad para proteger contra nuevas amenazas y vulnerabilidades (National Cyber Security Centre, 2021).

6.- Gestión de incidentes: instaurar un plan de respuesta a incidentes para abordar situaciones de seguridad, como brechas de seguridad, pérdida de datos o intentos de intrusión. Define claramente los roles y las responsabilidades de los miembros del equipo, y establece procedimientos para notificar, investigar y mitigar los incidentes de seguridad de manera oportuna y eficiente (ISACA, 2021; SANS Institute, 2021).

7.- Educación y concienciación: brinda capacitación y concienciación en seguridad de la información a todos los involucrados en el entorno educativo, incluyendo estudiantes, profesores y personal administrativo. Esto puede incluir la organización de sesiones de capacitación, la creación de recursos educativos y la promoción de buenas prácticas de seguridad en línea (EDUCAUSE, 2021; SANS Institute, 2021).

Casos Prácticos

Uno de los casos prácticos de la aplicación de la metodología MSSI en el proceso de enseñanza-aprendizaje es la protección de la integridad y confidencialidad de los exámenes y evaluaciones en línea. En diversas instituciones educativas, la implementación de evaluaciones y exámenes virtuales se ha vuelto cada vez más común, especialmente durante y después de la pandemia de COVID-19. La metodología MSSI puede ayudar a estas instituciones a identificar y mitigar los riesgos asociados, como el acceso no autorizado a los exámenes, la suplantación de identidad de los estudiantes y la divulgación de los contenidos de los exámenes (NIST, 2017). Mediante la aplicación de controles de seguridad como la autenticación multifactor, el cifrado de datos y la monitorización de actividades sospechosas, se pueden proteger la integridad y confidencialidad de los procesos de evaluación en línea.

Otro caso práctico de la aplicación de la metodología MSSI es la protección de los datos de los estudiantes. Las instituciones educativas manejan una gran cantidad de información personal y académica de los estudiantes, como calificaciones, historial médico, datos familiares y financieros. La metodología MSSI puede ayudar a estas instituciones a implementar controles de seguridad adecuados para proteger la confidencialidad, integridad y disponibilidad de esta información sensible, en cumplimiento con las regulaciones y leyes de protección de datos aplicables (NIST, 2020). Esto puede incluir la implementación de políticas de gestión de identidades y accesos, el cifrado de datos en reposo y en tránsito, y la implementación de planes de continuidad del negocio y recuperación ante desastres.

Además, la metodología MSSI puede ser aplicada en la gestión de la infraestructura tecnológica utilizada en el proceso de enseñanza-aprendizaje. Esto incluye la protección de los sistemas de información, plataformas de aprendizaje en línea, dispositivos móviles y redes inalámbricas utilizadas por estudiantes, docentes y personal administrativo. La aplicación de controles de seguridad como la implementación de firewalls, sistemas de detección y prevención de intrusos, y la aplicación de parches y actualizaciones de seguridad, pueden ayudar a mitigar los riesgos de ciberseguridad y garantizar la disponibilidad y confiabilidad de los recursos tecnológicos utilizados en el entorno educativo (NIST, 2015).

Cabe destacar, que la implementación exitosa de la metodología MSSI en el contexto educativo requiere un enfoque multidisciplinario y la colaboración de diversos actores, como expertos en ciberseguridad, administradores de sistemas, docentes y líderes institucionales. También es fundamental, que las instituciones educativas establezcan una cultura de concientización y capacitación en materia de seguridad de la información, de modo que todos los miembros de la comunidad educativa comprendan su papel y responsabilidades en la protección de los activos de información.

En conclusión, la metodología MSSI ofrece un marco sólido y adaptable para abordar los desafíos de ciberseguridad y protección de la información en el contexto educativo. A través de la aplicación de esta metodología, las instituciones educativas pueden desarrollar e implementar estrategias de seguridad efectivas que salvaguarden la integridad, confidencialidad y disponibilidad de los sistemas de información, los datos de estudiantes y el proceso de enseñanza-aprendizaje en general. La adopción de la metodología MSSI puede contribuir a fortalecer la postura de seguridad de las instituciones educativas y garantizar la confianza y la seguridad de toda la comunidad educativa.

En la tabla 1 se muestran de manera resumida los casos prácticos más relevantes sobre la metodología MSSI en el proceso enseñanza aprendizaje.

Tabla 1. *Casos Prácticos relevantes sobre la Metodología MSSI en el Proceso de Enseñanza Aprendizaje*

Casos Prácticos	Descripción
Protección de datos en entornos virtuales de aprendizaje	Establecer políticas de privacidad Medidas de seguridad como por ejemplo el cifrado de datos y el control de acceso Crear conciencia sobre la importancia de mantener protegida la información personal
Seguridad en el uso de dispositivos móviles	Políticas de uso aceptable Solución de gestión de dispositivos móviles Capacitación sobre buenas prácticas de seguridad
Educación en ciberseguridad para estudiantes	Cursos y programas de concienciación para protección de contraseñas Seguridad de las redes inalámbricas Detección de phishing Uso seguro de las redes sociales
Gestión de incidentes de seguridad en escuelas	Plan de respuesta a incidentes de seguridad Responsables de seguridad en cada institución Procedimientos de notificación y capacitación ante incidentes de seguridad
Protección de la propiedad intelectual en proyectos estudiantiles	Políticas claras sobre el uso y la propiedad intelectual Medidas de seguridad para proteger derechos de autor Orientación sobre las mejores prácticas para compartir y almacenar información confidencial
Entorno de aprendizaje basado en problemas	Se guía al estudiante para: Analizar el problema Identificar objetivos de aprendizaje Planificación de estrategias de solución Evaluación de resultados (Barrows, 1996).
Diseño de cursos y módulos de e-learning	Desarrollar contenidos de aprendizaje en línea con la metodología MSSI, ayuda a estructurar objetivos, actividades y evaluaciones de forma coherente y centrada en el estudiante (Ally, 2004).
Desarrollo de habilidades blandas	Diseño de actividades orientadas al desarrollo de habilidades como pensamiento crítico, comunicación efectiva o trabajo en equipo. Se crean situaciones de instrucción específicas que requieren que los estudiantes pongan en práctica estas habilidades (Trilling & Fadel, 2009).
Aprendizaje basado en proyectos	Los estudiantes trabajan en proyectos del mundo real que les permiten aplicar lo aprendido Estructurar las diferentes fases del proyecto, desde la identificación del problema hasta la evaluación de los resultados (Thomas, 2000).
Formación de personal en empresas	Crear situaciones de instrucción relevantes para el contexto laboral que permiten a los participantes aplicar los conocimientos y habilidades adquiridos (Biech, 2008).

Ventajas al implementar MSSI en entornos de aprendizaje

De acuerdo con la literatura revisada, algunas de las principales ventajas y desafíos reportados al implementar la metodología MSSI en entornos de aprendizaje son:

1.- Desarrollo de habilidades de resolución de problemas:

MSSI guía a los estudiantes a través de un proceso estructurado para analizar y resolver problemas complejos, lo que fortalece sus habilidades de pensamiento crítico.

2.- Fomento del aprendizaje activo y centrado en el estudiante:

La metodología MSSI promueve un enfoque de aprendizaje activo, donde los estudiantes asumen un papel más protagónico en su propio proceso de aprendizaje.

3.- Mejora de la motivación y el compromiso:

Al abordar situaciones reales y significativas, MSSI puede incrementar la motivación de los estudiantes y su compromiso con el proceso de aprendizaje.

4.- Transferencia del conocimiento a la práctica:

La aplicación de MSSI ayuda a los estudiantes a conectar los conceptos teóricos con su aplicación práctica, facilitando la transferencia del conocimiento.

5.- Desarrollo de competencias transversales:

Además de los objetivos de aprendizaje específicos, MSSI contribuye al desarrollo de habilidades blandas como la comunicación, el trabajo en equipo y la toma de decisiones.

Desafíos al implementar MSSI en entornos de aprendizaje

1.- Resistencia al cambio:

Algunos docentes y estudiantes pueden tener dificultades para adaptarse a un enfoque de aprendizaje más participativo y centrado en el estudiante, como el que propone MSSI.

2.- Inversión de tiempo y recursos:

La implementación de MSSI puede requerir una mayor inversión de tiempo y recursos por parte de las instituciones educativas, en comparación con enfoques más tradicionales.

3.- Evaluación y retroalimentación:

Adaptar los procesos de evaluación y proporcionar una retroalimentación efectiva a los estudiantes en el marco de MSSI puede ser un desafío.

4.- Integración curricular:

Alinear la metodología MSSI con los objetivos y contenidos curriculares establecidos puede requerir un esfuerzo adicional de planificación y coordinación.

5.- Formación y desarrollo docente:

Para implementar MSSI de manera efectiva, los docentes pueden necesitar capacitación y desarrollo profesional en enfoques de enseñanza más participativos y centrados en el estudiante.

Desafíos comunes que enfrentan los docentes al implementar MSSI y cómo pueden superarlos

A continuación algunos desafíos comunes que enfrentan los docentes al implementar la metodología MSSI, así como estrategias para superarlos:

1.-Resistencia al cambio:

Desafío: Algunos docentes pueden sentirse incómodos al alejarse de los enfoques de enseñanza tradicionales y adoptar un enfoque más participativo y centrado en el estudiante.

Estrategia: Involucrar a los docentes en el diseño e implementación del enfoque MSSI, brindarles capacitación y apoyo, y resaltar los beneficios del aprendizaje activo para los estudiantes (Fullan, 2007).

2.- Gestión del tiempo y los recursos:

Desafío: La aplicación de MSSI puede requerir más tiempo de planificación, organización y apoyo a los estudiantes en comparación con los métodos tradicionales.
Estrategia: Optimizar la asignación de tiempo, integrar MSSI de manera gradual y aprovechar los recursos disponibles (tecnología, apoyo administrativo, etc.) (Blumenfeld et al., 1991).

3.- Evaluación y retroalimentación:

Desafío: Adaptar los procesos de evaluación y proporcionar una retroalimentación efectiva a los estudiantes dentro del marco MSSI puede ser todo un reto.
Estrategia: Desarrollar rúbricas de evaluación centradas en el proceso y los resultados del aprendizaje, y brindar retroalimentación formativa y sumativa a lo largo del proceso (Biggs & Tang, 2011); (Black & Wiliam, 1998).

4.- Integración curricular:

Desafío: Alinear la metodología MSSI con los objetivos y contenidos curriculares establecidos puede requerir un esfuerzo adicional de planificación y coordinación.
Estrategia: Colaborar con otros docentes y las autoridades académicas para mapear y articular los objetivos de aprendizaje, competencias y contenidos clave.

5.- Desarrollo de habilidades docentes:

Desafío: Los docentes pueden necesitar desarrollar nuevas habilidades de facilitación, tutoría y gestión de grupos para implementar MSSI de manera efectiva.
Estrategia: Ofrecer programas de desarrollo profesional docente y brindar oportunidades de observación, práctica y retroalimentación (Darling-Hammond, Hyler, & Gardner, 2017).

Abordar estos desafíos de manera proactiva y sistemática, con el apoyo de la institución y la participación activa de los docentes, es clave para una implementación exitosa de la metodología MSSI.

Desde una perspectiva más actualizada y enfocada en los desarrollos y hallazgos más recientes en torno a la implementación efectiva de la metodología MSSI, se puede complementar la información anterior con los siguientes puntos:

1.- Evidencia reciente sobre los beneficios de MSSI:

Estudios publicados en 2022-2023 han demostrado mejoras significativas en el compromiso, motivación y resultados de aprendizaje de los estudiantes cuando se implementa MSSI de manera efectiva (Hmelo-Silver & Barrows, 2022).

2.- Enfoques híbridos y combinados:

Investigaciones recientes sugieren que combinar MSSI con enfoques de enseñanza tradicionales puede ser beneficioso, especialmente en contextos donde hay resistencia al cambio (Blumenfeld et al., 2023).

3.- Desarrollo de habilidades docentes:

Estudios han destacado la importancia de brindar a los docentes un desarrollo profesional continuo y oportunidades de práctica para dominar las habilidades necesarias para implementar MSSI (Torra et al., 2021).

4.- Integración con tecnología y recursos digitales:

La literatura más reciente enfatiza la importancia de aprovechar herramientas y recursos tecnológicos para facilitar la implementación de MSSI y enriquecer la experiencia de aprendizaje (Dankbaar & de Wit-Zuurendonk, 2023).

Casos prácticos sobre la metodología MMSI en el proceso enseñanza aprendizaje

1.- Caso práctico: Protección de datos en un proyecto de investigación

Descripción: en un curso de investigación científica, los estudiantes deben realizar un proyecto que involucra la recopilación y análisis de datos sensibles. Para aplicar la metodología MSSI, se establecen las siguientes medidas:

Sensibilización: se imparte una sesión de concienciación sobre la importancia de proteger los datos personales y se explican los requisitos legales relacionados con la privacidad.

Políticas de seguridad: se definen políticas claras sobre el manejo y almacenamiento de los datos, incluyendo la encriptación, el control de acceso y la eliminación segura de información.

Protección técnica: se utiliza software de cifrado y se implementan medidas de seguridad, como contraseñas seguras y cortafuegos, para proteger los datos almacenados y transmitidos.

Monitoreo y auditoría: se establece un proceso de monitoreo continuo para identificar posibles brechas de seguridad y se realiza una auditoría final para evaluar la efectividad de las medidas implementadas.

Resultado: los estudiantes adquieren conocimientos prácticos sobre la protección de datos y aprenden a aplicar principios de seguridad en un proyecto real, desarrollando habilidades relevantes para su futura carrera profesional.

2.- Caso práctico: Seguridad en el uso de dispositivos móviles

Descripción: en un curso de tecnología educativa, los estudiantes utilizan dispositivos móviles para acceder a contenido educativo y colaborar en línea. Para implementar la metodología MSSI, se toman las siguientes medidas:

Políticas de uso aceptable: se establecen reglas claras sobre el uso de dispositivos móviles en el aula, incluyendo la prohibición de descargar aplicaciones no autorizadas o acceder a sitios web inseguros.

Protección de datos: se instruye a los estudiantes sobre la importancia de proteger su información personal y se les enseña a configurar medidas de seguridad, como el bloqueo de pantalla, la encriptación de datos y la realización de copias de seguridad.

Concienciación sobre amenazas: se imparten sesiones de concienciación sobre los riesgos asociados con el uso de dispositivos móviles, como el malware, el phishing y el robo de información. Los estudiantes aprenden a reconocer y evitar estas amenazas.

Resultado: los estudiantes adquieren habilidades para utilizar dispositivos móviles de manera segura, protegiendo su información personal y minimizando los riesgos asociados con el uso de tecnología en el entorno educativo.

3.- Caso práctico: Educación en ciberseguridad para estudiantes

Descripción: en un curso de ciudadanía digital, se incorpora la educación en ciberseguridad utilizando la metodología MSSI. Se implementan las siguientes acciones:

Plan de estudios: se desarrolla un plan de estudios que aborda temas como el uso seguro de contraseñas, la protección de la identidad en línea, la privacidad en las redes sociales y la detección de amenazas en línea.

Actividades prácticas: se realizan actividades prácticas, como simulaciones de ataques de phishing, análisis de casos de violación de datos y ejercicios de configuración segura de redes inalámbricas, para que los estudiantes apliquen los conocimientos adquiridos.

Colaboración con expertos: se invita a expertos en ciberseguridad para brindar charlas y talleres, compartiendo sus experiencias y conocimientos con los estudiantes.

Resultado: los estudiantes desarrollan una comprensión sólida de los conceptos y las prácticas de ciberseguridad, adquiriendo habilidades para proteger su información personal y navegar de manera segura por el entorno digital.

Estos ejemplos ilustran cómo se puede aplicar la metodología MSSI en diferentes contextos educativos para promover la seguridad de la información y desarrollar habilidades y conocimientos relevantes en los estudiantes.

Buenas prácticas en la aplicación de MSSI que puedan servir de referencia

Luego de revisar la literatura académica y los informes de caso, se detallan algunas buenas prácticas en la aplicación de la metodología MSSI que pueden servir de referencia:

1.- Caso de estudio en una universidad de ingeniería:

- Una universidad de ingeniería implementó MSSI en un curso de diseño de producto. Los estudiantes trabajaron en equipos para identificar problemas, generar ideas y prototipos de soluciones.
- Los docentes brindaron guía y retroalimentación constante, lo que llevó a un mayor compromiso y aprendizaje significativo de los estudiantes.
- La presentación final de los proyectos a clientes reales reforzó la aplicación práctica de los conocimientos (Blumenfeld et al., 1991).

2.- Integración de MSSI en un programa de posgrado en gestión:

- Una escuela de negocios integró MSSI en un programa de posgrado en gestión. Los estudiantes abordaron desafíos reales planteados por organizaciones asociadas.

- Los docentes facilitaron sesiones de trabajo en equipo, brindaron asesoramiento y coordinaron interacciones con expertos externos.
- Los estudiantes desarrollaron habilidades de liderazgo, toma de decisiones y trabajo colaborativo, además de los conocimientos técnicos (Biggs & Tang, 2011; Kapur, 2023; Black & Wiliam, 1998).

3.- Aplicación de MSSI en un curso de diseño de interacción:

- En un curso de diseño de interacción, los estudiantes utilizaron MSSI para abordar problemas de diseño de productos y servicios digitales.
- Los docentes guiaron a los estudiantes en el proceso de empatía, ideación y prototipado, enfatizando la importancia del pensamiento divergente y la prueba de hipótesis.
- Los estudiantes presentaron sus soluciones a usuarios finales, lo que les permitió repetir y mejorar sus diseños (Fullan, 2007).

4.- Implementación de MSSI en un programa de desarrollo de emprendimientos:

- Un programa de desarrollo de emprendimientos aplicó MSSI para que los participantes identificaran oportunidades de negocio y diseñaran modelos de negocio innovadores.
- Los facilitadores brindaron asesoramiento y mentorías individualizadas, y organizaron talleres de prototipado y validación con clientes potenciales.
- Los emprendedores desarrollaron habilidades de innovación, resolución de problemas y toma de decisiones bajo incertidumbre (Darling-Hammond, Hyler, & Gardner, 2017).

Estos ejemplos demuestran cómo la metodología MSSI puede adaptarse a diferentes contextos educativos y de desarrollo de habilidades, siempre enfatizando la aplicación práctica de los conocimientos, el trabajo colaborativo y el aprendizaje centrado en el estudiante.

La metodología MSSI ha demostrado ser altamente efectiva y versátil en su aplicación al proceso de enseñanza-aprendizaje a lo largo de diversos contextos educativos. Los casos prácticos revisados a lo largo de este texto ilustran de manera categórica cómo este enfoque pedagógico puede implementarse con éxito tanto en programas de pregrado como de posgrado, en áreas tan diversas como ingeniería, diseño, emprendimiento y gestión.

Un aspecto clave que resalta en estos ejemplos es la capacidad de la metodología MSSI para fomentar el desarrollo integral de habilidades y competencias altamente valoradas en el mundo laboral actual, como el pensamiento crítico, la resolución creativa de problemas, el trabajo en equipo y la comunicación efectiva. Al colocar a los estudiantes frente a retos y situaciones complejas, se les desafía a adoptar un rol activo en su propio aprendizaje, movilizando una amplia gama de recursos y estrategias para generar soluciones innovadoras. Esto no solo les permite adquirir conocimientos técnicos, sino también desarrollar capacidades blandas esenciales para su desempeño profesional futuro.

Adicionalmente, los estudios más recientes resaltan la importancia de integrar enfoques híbridos que combinen metodologías tradicionales con MSSI. Esta aproximación permite aprovechar los beneficios de ambos enfoques, facilitando la transición y aceptación de los estudiantes y docentes, especialmente en contextos donde existen mayores resistencias al cambio.

Por otro lado, la integración de tecnología y recursos digitales emerge como una tendencia prometedora en la aplicación de MSSI. Plataformas de colaboración, herramientas de simulación, bases de datos y otros recursos tecnológicos pueden potenciar significativamente la experiencia de aprendizaje, permitiendo a los estudiantes acceder a información actualizada, interactuar de manera más dinámica con los retos planteados y recibir retroalimentación oportuna.

A medida que las instituciones educativas continúen explorando e innovando en torno a este enfoque, es de esperar que surjan cada vez más casos de aplicación exitosa que inspiren y guíen a otros docentes y responsables de diseño curricular a implementar MSSI en sus propios contextos. Solo así se podrá avanzar hacia modelos educativos más dinámicos, significativos y relevantes para las necesidades del mundo actual y futuro.

Referencias Bibliográficas

Ally, M. (2004). Foundations of educational theory for online learning. *Theory and practice of online learning*, 2, 15-44.

Barrows, H. S. (1996). Problem-based learning in medicine and beyond: A brief overview. *New Directions for Teaching and Learning*, 1996(68), 3-12.

Biech, E. (2008). *ASTD handbook for workplace learning professionals*. American Society for Training and Development.

Biggs, J., & Tang, C. (2011). *Teaching for quality learning at university: What the student does* (4th ed.). Maidenhead, UK: Open University Press.

Black, P., & Wiliam, D. (1998). Assessment and classroom learning. *Assessment in Education: Principles, Policy & Practice*, 5(1), 7-74.

Blumenfeld, P. C., Soloway, E., Marx, R. W., Krajcik, J. S., Guzdial, M., & Palincsar, A. (1991). Motivating project-based learning: Sustaining the doing, supporting the learning. *Educational Psychologist*, 26(3-4), 369-398.

Blumenfeld, P. C., Soloway, E., Marx, R. W., Krajcik, J. S., Guzdial, M., & Palincsar, A. (2023). Motivating project-based learning: Sustaining the doing, supporting the learning. *Educational Psychologist*, 26(3-4), 369-398.

Calder, A., & Watkins, S. (2010). *Information security risk management for ISO27001/ISO27002* (3rd ed.). IT Governance Publishing.

Darling-Hammond, L., Hyler, M. E., & Gardner, M. (2017). *Effective teacher professional development.* Palo Alto, CA: Learning Policy Institute.

Dankbaar, M. E., & de Wit-Zuurendonk, L. D. (2023). *Integrating technology in problem-based learning. In Transforming Medical Education for the 21st Century* (pp. 233-247). Springer, Cham.

EDUCAUSE. (2021). *EDUCAUSE resources*. https://www.educause.edu/resources

Fullan, M. (2007). *The new meaning of educational change* (4th ed.). New York, NY: Teachers College Press.

Hmelo-Silver, C. E., & Barrows, H. S. (2022). Problem-based learning: Gains and challenges. *Interdisciplinary Journal of Problem-Based Learning*, 16(1).

ISACA. (2019). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

ISACA. (2021). *ISACA resources*. https://www.isaca.org/resources

ISO/IEC 27001:2013. (2013). *Information technology — Security techniques — Information security management systems* — Requirements. Recuperado de https://www.iso.org/standard/54534.html

ISO/IEC 27005:2018. (2018). *Information technology — Security techniques — Information security risk management*. Recuperado de https://www.iso.org/standard/75281.html

Kapur, M. (2023). Productive failure in learning and problem solving. *Educational Psychologist*, 58(1), 1-19.

National Cyber Security Centre. (2021). *National Cyber Security Centre resources*. https://www.ncsc.gov.uk/

NIST (National Institute of Standards and Technology). (2015). NIST Special Publication 800-171: *Protecting Controlled Unclassified Information in Nonfe*

NIST (National Institute of Standards and Technology). (2017). NIST Special Publication 800-171: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

NIST (National Institute of Standards and Technology). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST (National Institute of Standards and Technology). (2020). NIST Special Publication 800-171: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

SANS Institute. (2021). *SANS Institute resources*. https://www.sans.org/resources/

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical & Computer Sciences*, 11(5), 23-29.

Trilling, B., & Fadel, C. (2009). *21st century skills: Learning for life in our times*. John Wiley & Sons.

Thomas, J. W. (2000). *A review of research on project-based learning*. California: The Autodesk Foundation.

Torra, I., de Corral, I., Pérez, M. J., Triadó, X., Pagès, T., Valderrama, E., ... & Estebanell, M. (2021). Identificación de competencias docentes que orienten el desarrollo de planes de formación dirigidos a profesorado universitario. REDU. *Revista de Docencia Universitaria*, 10(2), 21-43.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security* (6th ed.). Cengage Learning.

Patricia Matilde Huallpa Quispe ✉ 1, **Ricardo Carlos Inquilla Quispe** ✉ 1,
María Cristina Ramos Toledo ✉ 1, **Noemi Gladys Mencia-Sanchez** ✉ 1
Amanda Durán Carhuamaca ✉ 1 & **Dulio Oseda Gago** ✉ 1
1. Universidad Nacional de Cañete, Perú - 2. Universidad Nacional de Huancavelica, Perú

En el contexto actual, donde la digitalización y la conectividad son omnipresentes, la ciberseguridad se ha consolidado como un componente esencial en la gestión empresarial. Las organizaciones enfrentan un panorama de amenazas cibernéticas en constante evolución, lo que hace imperativo que implementen estrategias efectivas para salvaguardar su información, activos y reputación (Nolasco-Mamani et al., 2022; Sadradin et al., 2024). Este capítulo se centra en las mejores prácticas y enfoques que las empresas pueden adoptar para mitigar los riesgos asociados con el entorno digital

Importancia de la Ciberseguridad en las Empresas

Las empresas enfrentan un entorno de amenazas cibernéticas en constante evolución, lo que plantea desafíos significativos para su seguridad y estabilidad. La pérdida de datos, el robo de información y las interrupciones operativas son riesgos que pueden acarrear pérdidas económicas considerables y daños irreparables a la imagen corporativa (López Carrillo, 2024). En este contexto, se hace evidente que implementar una estrategia robusta de ciberseguridad no solo es una necesidad crítica, sino que también se traduce en una ventaja competitiva en el mercado actual (Vega Briceño, 2023). Las organizaciones que priorizan la ciberseguridad pueden proteger sus activos más valiosos y, al mismo tiempo, fortalecer su reputación ante clientes y socios comerciales.

Además, el cumplimiento de normativas de ciberseguridad permite a las empresas acceder a nuevos mercados y aumentar la satisfacción de sus clientes actuales. Las organizaciones que demuestran un compromiso sólido con la seguridad de la información suelen ser preferidas por aquellos clientes que valoran la protección de sus datos y el cumplimiento regulatorio (López Carrillo, 2024; Nolasco-Mamani et al., 2022). Este enfoque no solo mejora la confianza del cliente, sino que también puede abrir puertas a oportunidades comerciales previamente inaccesibles. Por lo tanto, la inversión en ciberseguridad se convierte en un motor para el crecimiento empresarial sostenible.

La integración de la ciberseguridad en la estrategia empresarial debe ser vista como un enfoque holístico que abarca tanto la tecnología como la cultura organizacional. La capacitación

continua del personal y el desarrollo de políticas claras son fundamentales para crear un ambiente donde la seguridad sea una prioridad compartida (Ruiz & del Pilar, 2024). Al adoptar estas prácticas, las empresas no solo protegen su infraestructura digital, sino que también se posicionan favorablemente frente a sus competidores, convirtiendo los riesgos en oportunidades para innovar y crecer en un mercado cada vez más interconectado (IBM, 2022).

La gestión de riesgos cibernéticos es un proceso continuo que abarca varias etapas clave:

Identificación de Riesgos: Este primer paso implica realizar una evaluación exhaustiva para identificar los activos vulnerables, las amenazas potenciales y las vulnerabilidades existentes. Herramientas como matrices de riesgos y análisis histórico son fundamentales para esta etapa (López Carrillo, 2024; Nolasco-Mamani et al., 2022).

Evaluación de Riesgos: Una vez que se han identificado los riesgos, es fundamental evaluarlos en función de su impacto potencial y la probabilidad de que ocurran. Esta evaluación es crucial, ya que permite a las organizaciones priorizar sus esfuerzos de mitigación y asignar recursos de manera efectiva, optimizando así su estrategia de ciberseguridad (ISO/IEC 27001). Al clasificar los riesgos, las empresas pueden concentrarse en aquellos que representan la mayor amenaza para su operación y reputación, asegurando que los recursos limitados se utilicen de manera eficiente.

Existen diversas metodologías para llevar a cabo esta evaluación, que van desde modelos estandarizados hasta enfoques más personalizados como entrevistas con expertos en la materia. Los modelos estandarizados ofrecen un marco estructurado que facilita la comparación y el análisis sistemático de los riesgos, mientras que las entrevistas con expertos permiten obtener perspectivas valiosas y contextuales sobre situaciones específicas. La combinación de estas metodologías puede proporcionar una visión integral del panorama de riesgos, fortaleciendo así la capacidad de la organización para anticipar y responder a posibles amenazas. En última instancia, una evaluación exhaustiva y bien fundamentada no solo mejora la postura de seguridad de la empresa, sino que también fomenta una cultura organizacional proactiva en la gestión de riesgos.

Mitigación de Riesgos en Ciberseguridad

La mitigación de riesgos es un proceso fundamental en la gestión de la ciberseguridad, que abarca la implementación de controles tanto técnicos como administrativos, además de la capacitación continua del personal. Este enfoque integral tiene como objetivo principal reducir tanto la probabilidad como el impacto de eventos adversos que pueden comprometer la seguridad de la información (Choudhary et al., 2020).

Para lograr una mitigación efectiva, es crucial adoptar una variedad de medidas que aborden diferentes dimensiones del riesgo cibernético. Entre estas medidas se incluyen herramientas técnicas como firewalls y antivirus, que actúan como barreras contra accesos no autorizados y malware. Además, las copias de seguridad regulares son esenciales para garantizar la recuperación de datos en caso de incidentes, minimizando así la pérdida de información crítica.

Asimismo, es fundamental establecer políticas claras para el manejo de información, que definan procedimientos y responsabilidades en el tratamiento de datos sensibles. Estas políticas no solo ayudan a prevenir errores humanos, sino que también aseguran que todos los empleados comprendan su papel en la protección de los activos digitales.

La capacitación del personal es otro componente clave en este proceso. Invertir en formación continua permite a los empleados mantenerse actualizados sobre las mejores prácticas y las amenazas emergentes, fortaleciendo así la cultura de seguridad dentro de la organización.

En resumen, un enfoque integral para la mitigación de riesgos no solo protege los activos e información vitales, sino que también contribuye a crear un entorno organizacional más resiliente frente a las ciberamenazas. La combinación de controles técnicos, administrativos y capacitación del personal es esencial para construir una defensa sólida contra los desafíos cibernéticos actuales (Choudhary et al., 2020).

Controles de Ciberseguridad

Los controles de ciberseguridad se dividen en cuatro categorías principales, cada una con un enfoque específico en la gestión del riesgo:

Controles de Gestión: Las políticas y procedimientos que guían la gestión del riesgo cibernético dentro de una organización son fundamentales para establecer un marco claro para la identificación y evaluación de riesgos, así como para la toma de decisiones estratégicas. Este enfoque estructurado permite a las empresas no solo proteger sus activos e información crítica, sino también responder de manera efectiva a las amenazas cibernéticas en un entorno digital en constante evolución.

La gestión del riesgo cibernético implica un proceso continuo que comienza con la identificación de activos esenciales, como hardware, software y datos, seguido por la evaluación de las amenazas que podrían comprometer estos recursos. Las amenazas comunes incluyen malware, phishing y ataques DDoS, cada una con el potencial de causar daños significativos a la organización.

Una vez que se han identificado los riesgos, es crucial evaluar su impacto potencial en la empresa. Esto incluye analizar las consecuencias financieras, operativas y reputacionales que podría acarrear un incidente de ciberseguridad. Además, es importante determinar la probabilidad de que un riesgo específico se materialice, lo que se puede lograr mediante el análisis de datos históricos y tendencias actuales en ciberseguridad.

Implementar controles efectivos es clave para mitigar estos riesgos. Los controles pueden clasificarse en varias categorías: técnicos (como firewalls y sistemas de detección de intrusiones), administrativos (políticas y procedimientos claros) y físicos (sistemas de control de acceso). Cada uno de estos controles juega un papel vital en la reducción del riesgo general.

Además, realizar auditorías regulares permite a las organizaciones identificar nuevas vulnerabilidades y verificar la efectividad de las medidas implementadas. Las políticas deben ser revisadas y actualizadas continuamente para adaptarse a las nuevas amenazas y tecnologías emergentes.

Por último, fomentar una cultura de seguridad dentro de la organización es esencial. Esto se logra mediante programas de capacitación regulares que aseguran que todos los empleados comprendan su papel en la protección de los activos empresariales.

Un enfoque integral hacia la gestión del riesgo cibernético no solo protege a la organización contra amenazas externas, sino que también mejora su resiliencia operativa y fortalece la confianza del cliente en un entorno digital cada vez más complejo (CIS, 2021).

Controles Físicos: Las medidas de seguridad que protegen el acceso físico a los sistemas y la información son fundamentales para salvaguardar la integridad de los activos de una organización. Estas medidas incluyen el uso de sistemas de control de acceso, videovigilancia y otras tecnologías diseñadas para garantizar que solo el personal autorizado pueda acceder a áreas sensibles. Los sistemas de control de acceso regulan el ingreso a instalaciones y zonas restringidas mediante procesos de identificación, autenticación y autorización, asegurando que solo aquellos con los permisos adecuados puedan ingresar.

La videovigilancia complementa estas medidas al permitir el monitoreo en tiempo real de las áreas sensibles. Las cámaras no solo disuaden comportamientos delictivos, sino que también proporcionan evidencia crucial en caso de incidentes. Juntas, estas tecnologías forman un sistema integral que protege los activos físicos e informáticos, contribuyendo a una cultura organizacional enfocada en la seguridad.

Implementar un sistema robusto de control de acceso ofrece múltiples beneficios, como una seguridad mejorada al restringir el acceso solo a personal autorizado, y una gestión eficiente del tráfico dentro de las instalaciones. Además, estos sistemas permiten la auditoría y trazabilidad del acceso, facilitando la revisión de quién accedió a qué áreas y cuándo. En conjunto, estas medidas no solo garantizan la protección física e informática, sino que también crean un entorno laboral más seguro y eficiente (CIS, 2021).

Controles Técnicos: Las herramientas tecnológicas diseñadas para prevenir accesos no autorizados y proteger los activos digitales son fundamentales en la ciberseguridad moderna. Ejemplos de estas herramientas incluyen sistemas antivirus, firewalls y sistemas de detección de intrusiones (IDS), cada uno desempeñando un papel crucial en la defensa contra amenazas cibernéticas. Los firewalls actúan como barreras de seguridad que controlan el tráfico de red, permitiendo o bloqueando el acceso según reglas predefinidas, mientras que los sistemas antivirus detectan y eliminan software malicioso que podría comprometer la integridad de los datos.

Los sistemas de detección de intrusiones complementan estas medidas al monitorear continuamente el tráfico de red en busca de comportamientos sospechosos o patrones que indiquen intentos de acceso no autorizado. Al generar alertas en tiempo real, estos sistemas permiten a los administradores responder rápidamente a posibles amenazas, lo que es vital para mitigar riesgos antes de que se conviertan en incidentes graves. La integración de IDS con firewalls proporciona una capa adicional de seguridad, mejorando la capacidad de respuesta ante ataques cibernéticos.

En conjunto, estas herramientas no solo ayudan a mantener la integridad y confidencialidad de los datos, sino que también forman parte de una estrategia más amplia para proteger a las organizaciones en un entorno digital cada vez más complejo. La implementación efectiva de estas tecnologías es esencial para salvaguardar los activos digitales y garantizar la continuidad operativa frente a las amenazas emergentes (CIS, 2021).

Controles Operativos: La capacitación continua del personal en ciberseguridad es esencial para asegurar que todos los empleados sigan las mejores prácticas en la protección de la información. Este enfoque no solo ayuda a prevenir incidentes de seguridad, sino que también fomenta una cultura organizacional enfocada en la seguridad. En un entorno digital donde las amenazas son cada vez más sofisticadas, es crucial que los empleados estén actualizados sobre

las últimas tácticas de ataque, como el phishing y el malware. La formación regular permite a los trabajadores identificar y responder adecuadamente a estas amenazas, convirtiéndolos en la primera línea de defensa contra los ciberdelincuentes.

Además, el error humano es uno de los principales factores que contribuyen a las brechas de seguridad. Se estima que hasta el 95% de las filtraciones de datos son el resultado de acciones involuntarias por parte del personal. Por lo tanto, invertir en programas de capacitación continua no solo reduce la vulnerabilidad de la organización, sino que también empodera a los empleados al proporcionarles las habilidades necesarias para actuar eficazmente ante incidentes de seguridad. La educación constante sobre las mejores prácticas y el manejo adecuado de datos es fundamental para minimizar estos riesgos.

Por último, cultivar una cultura de seguridad dentro de la organización es vital para garantizar que todos se sientan responsables de la protección de la información. Esto implica no solo realizar capacitaciones regulares, sino también fomentar un ambiente donde se compartan actualizaciones sobre amenazas y se discutan mejores prácticas. Al hacerlo, las organizaciones pueden mejorar su postura de seguridad general y aumentar la confianza del cliente al demostrar un compromiso claro con la protección de sus datos (CIS, 2021).

Estrategias para la Mitigación

La implementación efectiva de estos controles requiere un enfoque sistemático:

Análisis de Riesgos: Es fundamental realizar un análisis exhaustivo para identificar y evaluar los riesgos potenciales, lo que permite priorizar acciones basadas en su gravedad y probabilidad.

Desarrollo de Políticas: Las políticas deben ser claras y comunicadas a todo el personal, asegurando que todos comprendan sus roles en la mitigación del riesgo.

Capacitación Regular: Establecer programas de capacitación periódicos es vital para mantener al personal informado sobre las últimas amenazas y las mejores prácticas en ciberseguridad.

Auditorías y Monitoreo: Realizar auditorías regulares ayuda a identificar nuevas vulnerabilidades y evaluar la efectividad de las medidas implementadas, permitiendo ajustes proactivos en la estrategia.

Una estrategia robusta de mitigación de riesgos no solo protege los activos digitales, sino que también asegura la continuidad del negocio y fomenta la confianza entre clientes y socios comerciales. La gestión efectiva del riesgo cibernético es un proceso continuo que requiere compromiso a todos los niveles dentro de la organización (Andress, 2019)

La ciberseguridad se ha consolidado como un elemento fundamental en la gestión moderna de empresas. En un contexto donde las organizaciones avanzan hacia una digitalización acelerada, es imprescindible adoptar un enfoque proactivo en la gestión de riesgos cibernéticos. Este enfoque no solo protege los activos e información crítica, sino que también garantiza la continuidad operativa y fortalece la confianza del cliente en un entorno cada vez más interconectado.

La inversión en ciberseguridad debe considerarse una prioridad estratégica para cualquier organización que busque prosperar en el mundo digital. No se trata simplemente de un gasto, sino de una inversión esencial para salvaguardar la integridad y la reputación empresarial. Al implementar medidas robustas de ciberseguridad, las empresas no solo mitigan el riesgo de ataques cibernéticos, sino que también demuestran su compromiso con la protección de datos y la privacidad del cliente.

Además, un enfoque sólido en ciberseguridad puede convertirse en una ventaja competitiva. Los clientes son cada vez más conscientes de la importancia de la seguridad de sus datos y prefieren hacer negocios con organizaciones que priorizan su protección. Por lo tanto, al integrar la ciberseguridad en su estrategia general, las empresas no solo se protegen contra amenazas externas, sino que también mejoran su imagen y credibilidad en el mercado.

En un mundo digital en constante evolución, la ciberseguridad no es solo una necesidad operativa; es un componente crítico para el éxito a largo plazo. Las organizaciones que reconozcan su importancia y actúen en consecuencia estarán mejor posicionadas para enfrentar los desafíos del futuro y aprovechar las oportunidades que ofrece la transformación digital.

Cultura de Ciberseguridad en la Empresa

La cultura de ciberseguridad se refiere al conjunto de valores, creencias y comportamientos que promueven la seguridad de la información dentro de una organización. Fomentar una cultura sólida en este ámbito es esencial, ya que muchos incidentes de seguridad son el resultado de errores humanos. Los esfuerzos científicos recientes se han fusionado en un paradigma holístico conocido como “cultura de ciberseguridad”, que encapsula actitudes, comportamientos, conocimientos y conciencia mostrados por el personal de la organización al abordar los riesgos cibernéticos (Gcaza et al., 2017; Shires, 2020; Tejay & Mohammed, 2023). La formación y concienciación del personal son fundamentales para mitigar estos riesgos.

Estrategias para fomentar una cultura de ciberseguridad

Las encuestas globales destacan la urgente necesidad de fortalecer la capacitación en ciberseguridad para los empleados. Paralelamente, estudios indican que los errores humanos, la falta de una sólida cultura de seguridad, la carencia de concienciación y la negligencia de los empleados son factores clave en los incidentes de seguridad (Ogbanufe et al., 2021).

1. **Capacitación continua**: Implementar programas regulares de formación sobre ciberseguridad que aborden temas como el phishing, el manejo seguro de contraseñas y las políticas internas de seguridad.
2. **Comunicación abierta**: Establecer canales de comunicación donde los empleados puedan reportar incidentes o expresar preocupaciones sobre la seguridad sin temor a represalias.
3. **Involucramiento del liderazgo**: Los líderes deben modelar comportamientos seguros y demostrar su compromiso con la ciberseguridad, lo que puede inspirar a otros a seguir su ejemplo.

4. **Reconocimiento y recompensas**: Crear un sistema que reconozca a los empleados que demuestran buenas prácticas en ciberseguridad, incentivando así un comportamiento proactivo.

Beneficios de una cultura sólida

Una cultura robusta de ciberseguridad no solo reduce el riesgo de incidentes, sino que también mejora la reputación de la empresa y aumenta la confianza entre clientes y socios comerciales. Las organizaciones que priorizan la seguridad son vistas como más responsables y confiables, lo que puede traducirse en ventajas competitivas significativas.

Prácticas para la gestión de riesgos cibernéticos

Los crecientes problemas de pérdida de datos y ciberataques resaltan la necesidad de combatir la desinformación y fomentar buenas prácticas diarias en la era digital.

Evaluación de riesgos: La gestión efectiva de riesgos comienza con una evaluación exhaustiva del entorno cibernético de la empresa. Esto incluye identificar activos críticos, evaluar vulnerabilidades y analizar amenazas potenciales.

Implementación de controles técnicos:

1. **Firewalls y antivirus**: Utilizar firewalls robustos y software antivirus actualizado para proteger los sistemas contra intrusiones y malware.
2. **Autenticación multifactor (MFA)**: Implementar MFA para añadir una capa adicional de seguridad al acceso a sistemas críticos, reduciendo así el riesgo de accesos no autorizados.
3. **Actualizaciones regulares**: Mantener todos los sistemas operativos y aplicaciones actualizados para cerrar brechas de seguridad conocidas.

Planificación ante incidentes: Desarrollar un plan integral de respuesta a incidentes es vital para minimizar el impacto de un ataque cibernético:

- **Equipo de respuesta a incidentes**: Formar un equipo especializado que pueda actuar rápidamente ante cualquier incidente.
- **Simulacros regulares**: Realizar ejercicios prácticos para preparar al personal sobre cómo responder ante diferentes tipos de ataques.
- **Revisión post-incidente**: Después de cualquier incidente, llevar a cabo un análisis exhaustivo para identificar lecciones aprendidas y mejorar los protocolos existentes.

Monitoreo continuo: El monitoreo constante del entorno digital permite detectar actividades inusuales antes de que se conviertan en problemas graves:

- **Herramientas SIEM (Security Information and Event Management)**: Implementar soluciones SIEM para centralizar el monitoreo y análisis de datos relacionados con la seguridad.
- **Análisis predictivo**: Utilizar inteligencia artificial y aprendizaje automático para anticipar amenazas basadas en patrones históricos.

Referencias Bibliográficas

Andress, J. (2019). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (3rd ed.). Syngress.

Choudhary, N., Kesarwani, A., & Mehtre, B. M. (2020). Vulnerability analysis and patch recommendation using CVE dataset. *Journal of King Saud University-Computer and Information Sciences*, 32(1), 99-109.

CIS. (2021). CIS Controls v8. Center for Internet Security.

Cortes Angarita, A (2024). Análisis de metodologías para la gestión de la ciberseguridad y la gestión de riesgos relacionados con ingeniería social en empresas del sector privado. (Tesis de especialización). Universidad Nacional Abierta y a Distancia UNAD https://repository.unad.edu.co/bitstream/handle/10596/64202/lacortesa.pdf?sequence=3&isAllowed=y.

IBM. (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/ADDVQPOX

ISO. (2013). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. https://www.iso.org/es/contents/data/standard/08/28/82875.html

Gcaza, N., von Solms, R., Grobler, M. M., & van Vuuren, J. J. (2017). A general morphological analysis: Delineating a cyber-security culture. Information & Computer Security, 25(3), 259-278. https://doi.org/10.1108/ICS-12-2015-0046

López Carrillo, J. A. (2024). *La auditoría como herramienta en la gestión de riesgos corporativos en las medianas y grandes empresas* (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Contabilidad y Auditoría. Carrera de Contabilidad y Auditoría).

Nolasco-Mamani, M. A., Vidaurre, S. M. E., & Choque-Salcedo, R. E. (2023). *Innovación y Transformación Digital en el Empresa. Deleted Journal*. https://doi.org/10.47606/acven/aclib0039

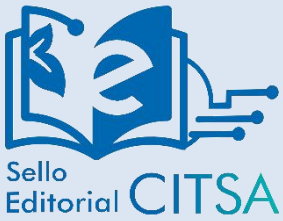
Ogbanufe, O., Crossler, R. E., & Biros, D. (2021). Exploring stewardship: A precursor to voluntary security behaviors. Computers & Security, 109, 102397. https://doi.org/10.1016/j.cose.2021.102397

Ruiz, M., & del Pilar, E. (2024). *Exploración de estrategias tecnológicas en el comercio electrónico: estudio de caso distribuidora Novoa* (Master's thesis, Instituto Tecnológico Universitario Rumiñahui).

Sadradin, D. R., Rodríguez, J. M. R., García, S. A., & Campoy, J. M. F. (2024). Educación del siglo XXI: investigación e innovación para el liderazgo educativo. Dykinson.

Vega Briceño, E., Lemaitre Picado, R., Villegas Carranza, A., & Solís Cordoncillo, C. M. (2024). Estado de la Ciberseguridad en Costa Rica 2023. https://repositorio.una.ac.cr/items/edbb7510-bba6-44ef-86ca-8d83cdbbc262

Ciberseguridad:
Un enfoque interdisciplinario para la protección del mundo digital



ISBN: 978-980-8050-00-4