La ciberseguridad en el tratamiento de información y datos sensibles en las instituciones educativas en el Perú

Caruajulca Tiglla Alex Eli
Diaz Barboza Roy Aldrhym
Link https://acortar.link/VtPXJJ

En la era digital actual, el uso de tecnologías de la información y la comunicación (TIC) ha transformado radicalmente la educación, convirtiéndose en un pilar fundamental para adaptarse a las demandas del siglo XXI. Estas tecnologías no solo facilitan el acceso a la información, sino que también abren nuevas oportunidades para la enseñanza y el aprendizaje en las instituciones educativas del Perú. Sin embargo, este avance tecnológico también ha planteado desafíos en cuanto a seguridad de la información y protección de datos sensibles. Además, se sabe que la ciberseguridad juega un papel crucial en el tratamiento de la información y datos sensibles en las instituciones educativas peruanas. La creciente preocupación por la privacidad de los datos, especialmente debido a la recolección masiva de información, resalta la importancia de implementar medidas de seguridad efectivas para proteger la integridad de la información. Ante esta situación, surge la interrogante: ¿Considera que la ciberseguridad es crucial en el tratamiento de la información y datos sensibles en las instituciones educativas del Perú? Para abordar esta pregunta, es necesario examinar el impacto de la ciberseguridad en el ámbito educativo y su papel en la protección de datos sensibles. A continuación, se argumentará que la ciberseguridad es fundamental para garantizar el tratamiento seguro de la información y datos sensibles en las instituciones educativas del Perú en la actualidad. Analizando aspectos relacionados con la ciberseguridad en el contexto educativo, se demostrará que aplicar medidas de seguridad adecuadas es esencial para proteger la integridad de la información y garantizar un entorno educativo seguro para todos los involucrados.

En primer lugar, **la ciberseguridad asegura la protección de la información y los datos sensibles ante posibles amenazas en línea en las Instituciones Educativas.** Puesto que esta se asemeja al rol de un guardián que protege un tesoro invaluable. Para fortalecer esta defensa, es crucial capacitar adecuadamente al personal educativo en ciberseguridad, lo cual es esencial para salvaguardar la integridad de la información. Además, la implementación de políticas y protocolos de seguridad cibernética refuerza la protección de los datos sensibles, como una fortaleza bien resguardada. Por ello se debe colaborar con expertos en ciberseguridad y utilizar herramientas tecnológicas avanzadas, indispensables para mejorar la defensa contra amenazas en línea, de manera similar a cómo un equipo confía en sus entrenadores y tecnología para mejorar su rendimiento. (Paredes & Chicaiza, 2021)

En segundo lugar, **la ciberseguridad incrementa un entorno digital protegido que salvaguarda la confidencialidad y la integridad de los datos.** Debido a la implementación de medidas de ciberseguridad que se presenta como la causa principal de la creación de un entorno digital seguro en las instituciones educativas del Perú. Esta medida surge para la comprensión de las posibles amenazas que enfrentan los estudiantes al utilizar Internet y participar en la educación virtual. Así, los centros educativos reconocen su responsabilidad de velar por la seguridad de los estudiantes. Para que así fomenten conscientemente sobre la importancia de la ciberseguridad, tanto entre los estudiantes como entre docentes y padres, para garantizar un entorno digital protegido y así evitar futuros ataques. (Torres & Galarza,2022)

En tercer lugar, l**a ciberseguridad implementa la encriptación de datos asegurando el manejo seguro de la información en entornos educativos donde se manejen datos sensibles estudiantiles**. La encriptación convierte los datos escolares sensibles en un formato incomprensible, a menos que se cuente con la clave de encriptación correspondiente para descifrarlos (Urbina, 2019). Al utilizar la encriptación, se garantiza que solo aquellos autorizados puedan acceder y comprender la información (Fernández, 2007). Aunque un atacante logre acceder a los datos, estos permanecerán ilegible. La encriptación también preserva la integridad de los datos al detectar cualquier intento de modificación o manipulación no autorizada (Mendoza & Mesias, 2017). Si se intenta alterar datos encriptados, se detectará la intrusión a través de técnicas como los hashes. La encriptación es una defensa efectiva contra diversos ataques cibernéticos, como el robo de datos o el ransomware. Aunque los atacantes accedan a los datos encriptados, no podrán aprovechar la información sin la clave correspondiente. Por ello, la encriptación de datos es crucial en la protección de la información sensible en instituciones educativas, proporcionando confidencialidad e integridad, lo que contribuye a garantizar un tratamiento seguro de la información.

Finalmente, los sistemas de detección de amenazas en la ciberseguridad garantizan el tratamiento seguro de los datos. Estos sistemas de detección están diseñados para identificar y responder a posibles amenazas cibernéticas de manera rápida (Jiménez, 2022). Los sistemas de detección de amenazas monitorean los sistemas informáticos en busca de comportamientos sospechosos o patrones de actividad maliciosa. Esto permite identificar y responder rápidamente a posibles ataques antes de que causen daños significativos. Estos sistemas pueden ayudar a prevenir intrusiones detectando y bloqueando intentos de acceso no autorizado a los sistemas informáticos de la institución educativa (Vilcarromero, 2018). Esto ayuda a proteger la información confidencial y a evitar que los atacantes comprometan la seguridad de los datos. Los sistemas de detección de amenazas pueden generar alertas y notificaciones automáticas cuando se detecta actividad sospechosa o se identifica una posible amenaza. Esto permite a los equipos de seguridad responder de manera rápida y efectiva para mitigar el riesgo y proteger la información. Estos sistemas también pueden proporcionar capacidades de análisis forense (Mendoza S. L., 2019), que permiten investigar incidentes de seguridad, determinar el alcance del daño y tomar medidas correctivas para evitar futuros ataques. La implementación de sistemas de detección de amenazas en ciberseguridad es fundamental para garantizar el tratamiento seguro de la información en instituciones educativas al detectar y responder proactivamente a posibles amenazas cibernéticas, protegiendo así los datos sensibles y manteniendo la integridad y confidencialidad de la información.

En definitiva, la ciberseguridad desempeña un papel crucial en el tratamiento seguro de la información y datos sensibles en las instituciones educativas del Perú en la actualidad. Debido que, al actuar como un guardián ante amenazas en línea, la implementación de medidas como la encriptación de datos y los sistemas de detección de amenazas fortalece la defensa de la integridad de la información. Pues, esta protección no solo abarca la confidencialidad y la integridad de los datos, sino que también promueve un entorno digital seguro para todos los involucrados en el proceso educativo. Por lo tanto, la ciberseguridad no es solo una cuestión técnica, sino también una responsabilidad compartida y una oportunidad para promover la conciencia sobre la importancia de la seguridad cibernética.

REFERENCIAS

Gómez, F. S. (2007). *Seguridad de la información.* Repositorio de la Universidad Nacional de Ingeniería. https://repositorio.uni.edu.pe/handle/20.500.14076/9764

Jimenez, C. F. (2022). *Modelo de detección de amenazas digitales para mitigar los riesgos de ciberseguridad en las organizaciones, 2019.* Universidad Nacional Federico Villareal. https://alicia.concytec.gob.pe/vufind/Record/RUNF_6e064c4e5f4e00ffe027b5662db4fd67/Details

Mendoza, L. R., & Mesias, M. L. (2017). *Simulación de un sistema transaccional mediante. un canal seguro, usando criptografía RSA.* Universidad De Guayaquil. https://repositorio.ug.edu.ec/handle/redug/23901

Mendoza, S. L. (2019). *Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa sisc.* Universidad del Pacífico. https://repositorio.up.edu.pe/handle/11354/2250

Paredes, P. I. M., & Chicaiza, P. M. (2021). "*Ciberseguridad en plataformas educativas institucionales de educación superior de la provincia de Tungurahua"* – Ecuador. Cuadernos de desarrollo aplicados a las TIC, 49–75. https://doi.org/10.17993/3ctic.2021.102.49-75

Torres, M. M. B., & Galarza, M. D. Á. (2022). "*Ciberriesgos a los que están expuestos los adolescentes con la educación virtual*". Dominio de las Ciencias, 1080–1096. https://doi.org/10.23857/dc.v8i1.2623

Urbina, H. A. (2019). *Análisis de algoritmos de encriptación de datos de texto, una revisión de la literatura científica.* Lima. https://repositorio.upn.edu.pe/handle/11537/31391

Vilcarromero, Z. L. (2018). *Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones.* Universidad Peruana de Ciencias Aplicadas. https://repositorioacademico.upc.edu.pe/handle/10757/624832