UNIVERSIDAD INTERNACIONAL SAN ISIDRO LABRADOR

ESCUELA DE EDUCACIÓN

SEDE GRECIA

Artículo Especializado para obtener el grado de Maestría Profesional en Administración Educativa.

La gestión de la ciberseguridad en los centros educativos del contexto costarricense: la gestión de un director.

Escuela Timoleón Morera Soto, circuito escolar 03 Dirección Regional de Enseñanza de Alajuela, de octubre 2023 a abril 2024.

Proponente: María Vanessa Torres Jara.

Alajuela, abril, 2024

María Vanessa Torres Jara[1]

Resumen

El objetivo de la presente investigación fue indagar sobre las actividades teóricas y prácticas que el director o directora debe cumplir para gestionar la ciberseguridad educativa y encontrar cuáles son dichas operaciones que propicien una mente abierta y critica en la manipulación de cantidades crecientes de datos característicos del personal, de las personas estudiantes y en general de información relacionada con la diversidad de proyectos y programas para registros, y a la vez procurar la privacidad y datos seguros para evitar las amenazas de softwares maliciosos, códigos dañinos y pérdida de identidad. El tipo de investigación aplicada en el artículo es la documental con medios aprovechados para obtener los datos a partir del análisis e interpretación de documentos. Las revelaciones encontradas expresan la necesidad de concientización articulada por parte de la persona administradora, en el uso de recursos tecnológicos y redes informáticas para potenciar la enseñanza y el aprendizaje.

Palabras clave: *Ciberseguridad educativa, privacidad, datos seguros, softwares maliciosos, códigos dañinos.*

Abstract.

The objective of this research was to investigate the theoretical and practical activities that principals must carry out to manage educational cybersecurity. Furthermore, to find out which operations promote an open and critical mind in the manipulation of increasing amounts of data characteristic of the staff, students, and general information related to the diversity of projects and programs for collecting personal information data. At the same time, ensure privacy and secure data to avoid the threats of malware, ransomware, and identity theft. The type of research applied in the article is qualitative documentary with means, used to obtain data from the analysis and interpretation of documents. The revelations found express the need for articulated awareness required to be made by the manager, focused on the use of technological resources and computer networks in order to enhance teaching and learning.

Keywords: *educational cybersecurity, privacy, secure data, malware, ransomware.*

[1]María Vanessa Torres Jara: Educadora de Informática Educativa y de robótica para I y II ciclo, en la Dirección Regional de Alajuela. Con formación y experiencia adicional en educación preescolar. Formación en redes y tecnologías en general. Con 13 años de experiencia docente. E-mail: mariavanessa.torres@gmail.com

La gestión del director en la ciberseguridad en los centros educativos

El presente artículo trata acerca del abordaje de la ciberseguridad en los centros educativos del contexto costarricense y la gestión tecnológica por parte de la persona administradora, se enfoca en la Escuela Timoleón Morera Soto, del Circuito 03 de la Regional Educativa de Alajuela, en el período 2024.

Según National Institute of Standards and Technology (2019) la gestión de la ciberseguridad se debe entender como "… en resumen, la ciberseguridad es un problema del negocio que solo se puede resolver con una visión holística de Personas, Procesos y Tecnología" (p.20). Al tomar en cuenta la posición de la instancia mencionada, en el contexto de la presente publicación se comprende el concepto de gestión de la ciberseguridad en entornos educativos como el análisis y aplicación de estrategias para proteger los datos y la identidad de la personas estudiantes, personal administrativo-docente e infraestructura de redes y softwares utilizados para la enseñanza-aprendizaje y control administrativo; al integrar elementos de evaluación de riesgos informáticos, políticas, protocolos, capacitación, concientización, necesidad de monitoreo continuo y gestión de accesos seguros.

Las personas directivas deben encontrarse al tanto de las herramientas actualizadas de análisis de riesgos, contingencia y aprovechamiento de recursos para salvaguardar la identidad y los datos referentes a información sensible, la cual necesita de sistemas de bloqueo y organización acorde a las características de la institución; tomar en cuenta el uso de las aplicaciones pertinentes y vincularlas con las capacitaciones y conciencia a la comunidad educativa.

El desarrollo del articulo plantea una visión general de los términos relacionados a la temática, con el objetivo de darle a la audiencia lectora la claridad y guiarla en el entendimiento de las etapas constructoras en un proceso de ciberseguridad, y unirlo con el resguardo de quienes son parte del ambiente educativo ante posibles amenazas cibernéticas que pueden causar robo de información personal e institucional, para proporcionar conclusiones formadoras de recomendaciones, con el fin de impulsar la puesta en práctica de estrategias de conocimiento y acción tecnológica en la organización en la Escuela Timoleón Morera Soto, del Circuito 03 de la Regional Educativa de Alajuela.

Dada la relevancia de establecer bases bajo una disciplina de informarse para asumir la responsabilidad de luchar contra las vulnerabilidades del medio informático sin aislarse, sino utilizando los apoyos existentes a nivel de hábitos, materiales especializados y profesionales

certificados; seguidamente la publicación iniciará con la muestra de los referencias para inducir el reconocimiento del panorama dado por la experiencia de autores y las proposiciones con un carácter de familiaridad con el tema tratado.

A raíz de la búsqueda documental sobre la ciberseguridad y la gestión de la figura directiva institucional se identificaron investigaciones prácticas a nivel nacional e internacional en relación con la influencia directa en el manejo del tema en las personas estudiantes y en el entorno, donde se enlaza con los componentes de políticas de control y la orientación a manos de los mayores de edad en contacto con los y las discentes; dentro de las referencias se presenta el detalle de cada una:

En la exploración nacional realizada acorde a la materia se encuentra el estudio titulado: "Peligro en redes sociales, educando en ciberseguridad", en el año 2020 los siguientes autores abordaron el tema con sustento de la Universidad Nacional de Costa Rica: Cristel Ivannia Astorga, Rodolfo León Anchia, Alcides López Cascante, Jorge Manuel Luna Angulo e Ileana Schmidt Fonseca. La población meta se estableció en padres de familia y menores de edad de II y III Ciclo de Educación Básica y Diversificada de la región rural de Horquetas de Sarapiquí, en Heredia, con el objetivo de fomentar una cultura y desarrollar un plan de formación ante los peligros de las redes sociales en línea.

En este caso las conclusiones surgieron al detectar que la mayoría de jóvenes y niños tiene contacto con teléfonos celulares y WhatsApp, convirtiéndolos en vulnerables al compartir discriminadamente información, también se recalcó en los porcentajes relevantes: en general se conoce sobre los lineamientos de privacidad, pero menos del 20% las aplica, en cuanto a las instituciones solo el 33% se preocupa por enseñar normas; el 91% de los encargados han conversado con los hijos, pero solo el 40% aplica controles. Lo anterior permite a los gerentes de escuelas y colegios analizar los resultados para fijarse el rol integrador en la gestión de seguridad.

El avance internacional indagatorio es el llevado a cabo acerca del uso y riesgo del internet en adolescentes, particularmente analizando la explotación sexual en línea. Elaborado por Graciano (2021) apoyada por el Fondo de las Naciones Unidas en la Infancia (UNICEF), en República

Dominicana en el año 2021. Corresponde a una población de estudiantes de doce a diecisiete años, con el propósito de perfeccionar las acciones institucionales en las fases de investigación relacionados con posibles riesgos y daños causados por la interacción dentro del internet. Los resultados expresan de un 86% a 88 % en edades de 12 a 14 las redes se aprovechan para asignaciones y luego para socializar, lo cual va aumentando con los adolescentes de 15 a 19 años. Se evidenció de manera general en la muestra seleccionada, los docentes subestiman las situaciones de ciberacoso.

La ciberseguridad se ha retomado de diversas perspectivas y con elementos ubicados desde la enseñanza del tópico en niños y jóvenes hasta juntarlo con el uso de conexiones seguras y el compromiso formación, supervisión y orden de programas para limitar la utilización de dispositivos y proteger contra agresiones, como robo de identidad, virus o ataques cibernéticos. Tanto en hogares como en los centros de aprendizaje; lo cual invita a reflexionar cuestionándose sobre las implicaciones para la administración educativa en el centro de trabajo, el personal, discentes y representantes legales; por eso se da paso a la presentación de las preguntas generadoras y el planteamiento del problema en cuestión.

El problema de investigación que fundamenta el tema de este artículo es la identificación de las aristas claves que se desarrollaran como punto de enfoque para obtener resultados, con el fin de enmarcar la gestión del director y establecer los cuestionamientos a los cuales se investiga para encontrar respuestas, toma en consideración desde la forma de cuidar los informes, expedientes, softwares privados, proteger correos, fiscalizar el compartir fotos o videos con grados de privacidad; hasta la concientización fundamentada teórica y prácticamente de los administradores y colaboradores, incluyendo las etapas de formación a los menores de edad.

En la actualidad la exposición a las opciones digitales es la realidad en la que se desenvuelven las personas, trae situaciones positivas de acortar distancias y propiciar recursos para la vida cotidiana, estudiantil y laboral; pero también presenta peligros con espacios donde existen relaciones con individuos, empresas o programas no identificados cara a cara. Los niños y jóvenes son parte del movimiento de la era tecnológica, en interacción constante con el mundo cibernético, cada vez con más posibilidades de conexión, por ejemplo, según Graciano (2021)” A mayor edad, mayor es el

uso de tenencia y celular propio: el 82% entre los 15 y 17 años tienen celular propio en mayor proporción que los adolescentes entre 12 y 14 años (58%)" (p.14). Incluso en edades menores se evidencia, aunque en menor cantidad la utilización de dispositivos.

La pregunta generadora es ¿Cuáles son acciones teóricas y prácticas que el director debe cumplir para gestionar la ciberseguridad del centro educativo y los miembros que conforman la comunidad estudiantil? La interrogante se subdivide en: ¿Cuáles son los términos relacionados con ciberseguridad, riesgos y vulnerabilidad?, ¿Cuáles son las etapas para establecer protocolos de seguridad en instituciones educativas?, ¿Cuáles se consideran elementos para procesos de capacitación y formación en el tema para menores y mayores de edad?, ¿Cuáles son las recomendaciones teóricas para concienciar? y ¿Cuáles son las recomendaciones prácticas para ejecutar en las máquinas y entornos de redes?

Las causas del problema se centran en la carencia de guías concretas y claras que encamine al gerente de la organización para transformar la escuela en un habitad seguro concerniente con amenazas digitales, el derecho y deber de estimular la inserción de todos involucrados para alcanzar el compromiso y acatamiento de las alternativas, con el estudio se conseguirá la enumeración de tácticas para lograrlo, y luego interiorizarlo al ser practicado con regularidad.

Si la situación de la temática no se atiende, la población participante se puede convertir en una sociedad pasiva manipulada por entidades superiores nacional e internacionales que inspeccionan y acumulan los datos cuando se identifican sin protección, además del riesgo de desfalco de identidad y atentados contra la integridad del cuerpo y emocional; la creación de rutinas para evitar ser víctimas se logra desde tempranas edades, como cita The Edron Academy (2022) "Comenzar a abordar estos temas desde temprana edad y mantener constante comunicación sobre las nuevas tecnologías" (p.7)

La falta de ciberseguridad en centros educativos puede dar paso a contrariedades significativas, según la literatura revisada y apoyo del motor de búsqueda de inteligencia artificial, tomando en cuenta que la generación de texto fue asistida por el modelo lenguaje ChatGPT de OpenAI (OpenAI,2024). los principales riesgos se pueden resumir de la siguiente forma:

1.**Pérdida de datos confidenciales:** La carencia de medidas de seguridad podría poner en riesgo la privacidad de los datos confidenciales como información personal de estudiantes y personal colaborador que almacenan los centros educativos, lo cual podría tener consecuencias legales y ataques físicos y cibernéticos graves.

2.**Amenazas de malware y virus**: Sin una protección adecuada, los sistemas informáticos de los centros educativos son vulnerables a ataques de malware y virus, los cuales pueden causarles daño al robar información sensible o interrumpir las operaciones normales de los equipos y afectar la normalidad de funcionamiento de trámites.

3.**Falta de integridad en la información:** La manipulación no autorizada de información, como calificaciones o registros académicos, podría ocurrir sino se aplican medidas de seguridad adecuadas a la infraestructura de red y a la cantidad de datos manipulados.

4.**Acoso cibernético y ciberbullying:** La falta de seguridad en línea puede exponer a las personas estudiantes a amenazas como el acoso cibernético y el ciberbullying. Esto puede afectar negativamente el bienestar emocional y psicológico.

5.**Robo de propiedad intelectual:** Los centros educativos realizan investigaciones y desarrollan contenido educativo con derechos de creación y edición. La falta de seguridad podría exponer esta propiedad intelectual a riesgos de robo o piratería.

6.**Interrupciones en la enseñanza:** Ataques cibernéticos, como ransomware o códigos maliciosos, podrían afectar a la infraestructura tecnológica de un centro educativo, lo que trascendería en interrupciones en la enseñanza y la administración.

7.**Exposición a contenido inapropiado:** La falta de controles de seguridad podría permitir el acceso a contenido en línea inapropiado o peligroso.

8.**Desconfianza y pérdida de reputación:** La falta de seguridad puede socavar la confianza de las personas encargadas legales, los y las estudiantes o del personal en la capacidad de la institución para proteger la información y proporcionar un entorno educativo seguro.

El problema se explica en la importancia de organizar el conjunto de partes que conceptualizan y conforman la ciberseguridad las repercusiones en los centros educativos y los miembros de la comunidad educativa; por tanto se involucran variables que necesitan ser examinadas y vinculadas para beneficio del proceso de crecimiento mental, físico, de enseñanza y aprendizaje de los estudiantes en una realidad de contexto tecnológico; las siguientes ideas enriquecerán la misión justificadora del presente artículo.

La investigación aportará sobre la ejecución de conceptos e ideas sobre la ejecución de ciberseguridad en centros educativos, Al partir de un entendimiento de los riesgos latentes de los recursos y servicios en línea; para tomar decisiones informadas y reducir la oportunidad de ser víctimas de usurpaciones cibernéticas, pone a disposición de los directivos de educación y de la población en general rasgos del tópico clasificados y organizados para hacer comprendidos con facilidad, porque en gran medida se maneja en escritos dirigidos a personas que conozcan del tema y sin términos que puedan ser comprendidos por profesionales educativos y afines.

Al analizar las referencias estadísticas acerca de la temática se refleja la necesidad de implementación de la ciberseguridad en las instituciones educativas, donde se evidencia el aumento de ataques con códigos e intenciones maliciosas, según el estudio realizado por la empresa Sophos reconocida por las encuestas anuales del estado del ransomware en el sector educativo a nivel de España, Europa en general y América, citada por el instituto Digital Security (2023) “En el 2023 el 79% de las organizaciones de educación superior encuestadas informaron haber sido atacadas por ransomware, mientras que el 80% de las organizaciones de educación primaria encuestadas fueron atacadas¨”(p.1); aumentando un 15% y un 24% respectivamente desde el año 2022; en tales ataques se explica que roban datos administrativos y personales de personas estudiantes y quienes laboran en los centros, además de causar daños como virus informáticos dañando servidores y afectando emocional y académicamente a los involucrados, a lo que se adiciona la solicitud de recompensa, en el año 2022 se pidieron en España 64% de rescates de información en estas instituciones y para el 2023 creció en un 64%.

Los organismos internacionales como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura **(**UNESCO) establecen referentes para comprender la importancia de

entornos digitales seguros, según UNESCO (2023) “Aboga por políticas nacionales que protejan el bienestar digital de docentes y estudiantes, reduzcan y neutralicen la huella de emisión digital y eviten el tecnosolucionismo” (p. 2), se complementa con la visión de Organización de Naciones Unidas que apoya su conceptualización en la llamada Agenda 2030 sobre ciberseguridad al evocar a la educación digital inclusiva, paralelo a ello se percibe la trascendencia del respaldo recibido para divulgar la protección de recursos digitales a altura mundial por parte de la Organización para la Cooperación y el Desarrollo Económicos (OECD), la Agencia Europea de Ciberseguridad (ENISA), Consejo de Europa (CDE) y la Unión Internacional de Telecomunicaciones (ITU).

Dichas organizaciones en conjunto concluyen que el aspecto clave de la gestión de ciberseguridad a manos de quien administra es el desempeño del liderazgo escolar y el fortalecimiento de la cultura de seguridad y facilitar las medidas para proteger la información y los recursos digitales en el ámbito educativo. Al enlazar la teoría del tópico se resume que el personal administrativo debe desarrollar elementos como: políticas de ciberseguridad, educación y concientización, gestión de incidentes, integración de profesionales, ejecución de herramientas y tecnologías e implementación normativa.

A nivel costarricense el Ministerio de Ciencia, Innovación, Tecnología y comunicaciones apoya el enfoque del crecimiento de las amenazas en el área cibernética, incluyendo el sector educativo, por lo cual manifiesta el requerimiento de estrategias, por eso, el Gobierno de Costa Rica junto ministerio respectivo implementa La Estrategia Nacional de Ciberseguridad 2023-2027 (2023) “se centrará en principios orientadores, pilares, objetivos de trabajo y líneas de acción; que guiarán nuestras acciones y nos ayudarán a lograr nuestros objetivos; los cuales se encuentran enfocados a reforzar la gobernanza de ciberseguridad nacional” (MICITT,2023). Se recalca en lo analizado la función de la Directriz N° 133-MP-MICITT, enfocándose en el 1° del Decreto Ejecutivo número 37052-MICIT del 9 de marzo de 2012, donde se dice que el Estado costarricense cuenta con el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) y se suscita en los artículos 1° y 2° de la Ley de la Administración Pública a desempeñar las recomendaciones, medidas técnicas y originar de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica para robustecer la ciberseguridad en el país.

Sumado a lo anterior se requiere la formación en leyes las cuales protegen la identidad y la información de los y las estudiantes y del personal, donde el Ministerio de Educación Pública unido a la comunidad educativa debe concientizar el respeto a: Código de la Niñez y la Adolescencia (Ley N°7739) Art. 5 menciona el "…respeto de sus derechos en un ambiente físico y mental sano…"; resolución MS-DM-2592-2020 MEP-00713-2020 de la protección de la imagen de la persona menor de edad y la confidencialidad de sus datos personales; Código Civil (Ley N°63) Art. 47 menciona que "las fotografías o imagen de una persona no pueden ser reproducidas, expuestas o vendidas en forma alguna sino es con su consentimiento"; el derecho a la intimidad establecido en la Constitución Política, en su Art. 24, limita la observación y captación de la imagen y documentos de la población en general, la cual específicamente en personas menores de edad dispone del Código de la Niñez y la Adolescencia, en el Art. 27 "… derecho a la imagen. Prohíbase publicar, reproducir, exponer, vender o utilizar, en cualquier forma, imágenes o fotografías de personas menores de edad …".

El documento del Ministerio de Educación Pública indica que el incumplimiento de los principios y disposiciones en atención al Art. 47 del Código Penal (Ley N°4573) y el Art. 27 del Código de la Niñez y la Adolescencia, nombradas anteriormente, faculta el acatamiento de posibles sanciones a las personas que lo irrespeten, conteniendo las fuentes disponibles en el ambiente de violación de seguridad cibernética que permitan la propagación de datos en la red online.

Por tanto, el objetivo del presente estudio documental es la indagación de acciones teóricas y prácticas que el director o directora debe cumplir para gestionar la ciberseguridad del centro educativo y los miembros que conforman la comunidad estudiantil; para propiciar el cambio hacia la dicha colectividad pedagógica y posterior en la sociedad con las herramientas para enfrentar el flujo digital y de pensamiento computacional, con mente abierta y critica de utilizar la agilidad de la actualidad sin incurrir en incidentes que podrían causar violaciones de seguridad individual y grupal.

La responsabilidad de los gerentes educativos se enlaza con la práctica y transmisión de valores, entre ellos los relacionados con los comportamientos digitales; respeto a la privacidad propia y de los demás, complementándose con la disciplina para acatar normas básicas de seguridad, por

ejemplo, el no ingresar a correos o enlaces de dudosa procedencia. La información del artículo servirá para ser analizado y ejecutado para cumplir el objetivo propuesto.

La publicación es relevante por la actual época donde se da el crecimiento de las tendencias a las actividades e interacciones virtuales. Otros estudios hablan sobre la terminología y estrategias de ciberseguridad a nivel extenso o enfocados en el uso de Internet en la niñez y la adolescencia, se toman como base para formular ideas concretas enriquecidas con líneas del tema en estudio expuestas desde el siguiente marco referencial.

La publicación se orienta desde lineamientos, conceptos, teorías y debates expuestos a continuación, por ejemplo:

El termino ciberseguridad pauta el proceso de enganche para del resto del estudio, datos recopilados por el Fondo de las Naciones Unidas en la Infancia la unen con las palabras de ciberacoso, noticias falsas, robos de información, protección de datos y sexting o compartimiento de fotos de menores con contenido sexual; donde la noción de malware es primordial, según el planteamiento López (2021) para este instituto se entiende malware como

> Es un código malicioso diseñado para infiltrarse en tu dispositivo cuando lo instalas o descargas, aunque no necesariamente te das cuenta3. Cuando hay uno en tu computadora, teléfono o tableta, puede: acceder a toda tu información, incluyendo ubicación en tiempo real y lista de contactos. acceder a tus fotos y archivos y publicarlos en internet o en páginas maliciosas y tu ni en cuenta, hackearte contraseñas, email, redes sociales y demás. (p.139)

La exaltación de limites generalmente son llevados a cabo por personas con identidades ocultas o perfiles inexistentes con características que llamen la atención para después del primer contacto ganar la confianza y solicitar datos personales o credenciales para facilitar el ingreso a cuentas o para extorsionar usando la táctica de la amenaza, la práctica de la desconfianza para corroborar la veracidad de las personas o recursos se debe enmarcar en pasos de verificación, al formar nodos de enlace entre entidades conocidas que puedan proporcionarla.

La evolución histórica muestra que cuando surgió la computación no se trataba el tema en cuestión, luego se le da un matiz de ficción al relacionarlo con video juegos o el ciberespacio, nace como tal con el auge de redes informáticas, por eso con la explosión de la virtualidad a nivel mundial se vuelve necesaria; para Prieto (2023) "La Ciberseguridad no nació hasta que se comenzaron a conectar los equipos y a desarrollarse redes de computadoras, lo cual ocurrió en 1950, cuando se crearon las primeras redes informáticas y módems."; (párr.3); en 1960 se moviliza la cantidad de archivos digitales, lo cual aumenta la propagación. En el ambiente educativo es hasta después del 2000 que se hace más evidente con el uso de las computadoras con internet en las instituciones.

Las teorías que dan origen a la pregunta generadora van ligadas a las clasificaciones de la seguridad informática, según el proyecto sustentado por la Universidad Piloto de Colombia, se expresa por Gamboa (2020) "Las categorías son seguridad de red, de las aplicaciones, de la información, operativas, recuperación de desastres y la continuidad de funcionamiento, capacidad de usuario final, en el cual se desglosa la habilidad de reacción, integridad, confidencialidad y autenticación" (p. 1); puntos clave para la visión tecnológica de sus implicaciones y de la forma de abordarse para el diseño de la gestión.

El estudio realizado por el experto y profesor de ciberseguridad de la universidad de Cenfotec, al analizar los resultados de las condiciones que tienen las escuelas y colegios en costa Rica, presenta el marco teórico de apoyo que habla sobre los ataques en situaciones reales a centros educativos, sirve de referencia para la visualización de los alcances, peligros y contingencias acordes a la publicación. Las Cámaras de Tecnologías de Información y Comunicación (CAMTIC) (2021) acota "Ese porcentaje es ligeramente mayor al 54% de incidencia que en el resto de los sectores empresariales del mundo. Es decir, cuando los atacantes propagan sus ataques tienen más éxito con las escuelas que con otras empresas" (párr.4). El articulo enfatiza en que los cibercrímenes dirigidos a las instituciones están en aumento, debido a las vulnerabilidades y falta de inversión en las distribuciones se seguridad.

La controversia en el tema seda al reflexionar si parte de las vulnerabilidades son a consecuencia de descuidos humanos o de las destrezas tecnológicas de los agresores digitales, al respecto se cita en la investigación sobre la ciberseguridad en cadenas de suministros inteligentes realizada

por La Comisión Económica para América Latina y el Caribe (CEPAL), a manos de Díaz (2022) el cual menciona

> En estudios recientes de CEPAL se ha encontrado que dos tercios de los incidentes de ciberseguridad registrados tienen su origen en errores o distracciones cometidas por los integrantes de la organización a través de la utilización de contraseñas débiles y/o repetidas para las cuentas utilizadas en diferentes servicios (p.13)

Formar en hábitos en la actuación cibernética minimiza la posibilidad de equivocaciones de seguridad y complementan la cimentación y colocación de la infraestructura de software y organizaciones de los capitales reservados para tal efecto. Las normas o lineamientos se deben bosquejar con protocolos integrales desde la perspectiva informática, pedagógica, psicológica, social y cultural; con ayuda de la motivación para asumirlos con conciencia.

MÉTODO

El tipo de investigación que se aplica en el presente artículo es la documental cualitativa según los medios aprovechados para obtener los datos, como menciona la enciclopedia digital Concepto (2024)" En general, las investigaciones documentales aplican el método de cita o citado, ya sea textual o de cualquier otro tipo, para indicarle al lector de dónde provienen las aseveraciones y/o las informaciones que muestra"(p.342), se centra en el análisis e interpretación de documentos; en este caso se utilizó el tipo hemerográfico porque se revisó material proveniente de revistas y publicaciones del tema ubicados en la Web de organizaciones y autores nacionales e internacionales, reflejándose lo que cita la autora del Consejo Nacional de Investigaciones Científicas de España, Gaitán (2022)"En este sentido, nos centraremos en el abordaje de la investigación hemerográfica, es decir, del estudio de testimonios de diversa índole recogidos en una fuente primaria como son los periódicos, diarios, revistas o medios similares" (p. 14)

La metodología de la investigación documental con la cual se efectuó este artículo se basa en el aspecto abordado por referentes de este tipo de investigación, según Baena (1985) "la investigación documental es una técnica que consiste en la selección y recopilación de información por medio de la lectura y crítica de documentos y materiales

bibliográficos"(p.4), también para Rojas (2011) "En general, las fuentes de información utilizadas en la investigación se denominan, genéricamente, unidades conservatorias de información, y se trata de personas, instituciones, documentos, cosas, bibliografías, publicaciones,…, bases de datos, fuentes electrónicas situadas en la Web,…" (p.4) complementada con la exposición de Ávila (2006) "la investigación documental es una técnica que permite obtener documentos nuevos en los que es posible describir, explicar, analizar, comparar, criticar entre otras actividades intelectuales, un tema o asunto, …" (p.4); citados por Universidad Nacional Autónoma de México(2017)

El proceso se lleva a cabo con un orden lógico, se mantiene una secuencia para permitir el vínculo entre la investigación con los espacios de organizar y exponer lo extraído, mantener un orden como menciona la Universidad Autónoma de México (UNAM) "Elegir con claridad el tema a investigar, definir la bibliografía básica acerca del tema, elaborar fichas de información bibliográficas o hemerográficas, hacer lecturas rápidas del material seleccionado, filtrar la utilidad, Definir una organización, redacción final"(párr.6); los pasos deben de dirigir la revisión y discusión para llegar a los resultados y conclusiones a partir de la problemática definida identificando y seleccionando conceptos y tendencias acordes a la ciberseguridad en instituciones de educación para luego proponer estrategias que respondan a los objetivos definidos.

Los elementos de la investigación documental en el proceso de la presente producción se clasifican en fuentes de información, apoyo de motor de búsqueda de inteligencia artificial y fichas de estudio; en el primer caso se procura identificar las fuentes relacionadas directamente con la temática y analizar la procedencia con el fin de tener la confianza en la aportación de los contenidos sustentados en los sitios de análisis de teoría aclaratoria y en la visualización de estadísticas, antecedentes y referentes teóricos para luego fundamentar la importancia, protocolos y leyes concernientes a aplicar la ciberseguridad en centros educativos, basándose en los aportes de Organismos y autores reconocidos por la veracidad como universidades o la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura **(**UNESCO).

En cuanto al elemento de la inteligencia artificial que apoya lo anterior como recurso para determinar puntos clave de búsqueda relacionados con autores principales, información más actualizada e ideas generales para guiar el proceso, el utilizado fue el ChatGPT por ser considerado

acorde a las posibilidades y la necesidad del tema; en cuanto a las fichas de estudio contribuyen a tener a la mano un respaldo de los sitios (enlaces), autores y contenidos básicos para luego ser retomados a la hora de hilar las ideas.

En las fuentes de investigación primarias y secundarias que se utilizaron se aprovechó el recurso digital para hallarlas, en el caso de las primarias que tienen información directa con el tema se usaron por ejemplo las conceptualizaciones de la UNESCO, la UNICEF, The Edron Academy, Digital Secury, National Institute of Standards and Technology, CENFOTEC, la Universidad Nacional de Costa Rica, la Universidad de Costa Rica, y otras instituciones educativas internacionales ;en las secundarias que citan información referente a autores de otros textos o con ideas secundarias a las preguntas generadoras se utilizaron por ejemplo los documentos del Ministerio de Educación Pública que menciona las leyes encontradas en el Código Penal, la Constitución Política y en el Código de la Niñez y la Adolescencia referentes a la temática, y los aportes de Ministerio de Ciencia y Tecnología y Telecomunicaciones con su propuesta hacia la ciberseguridad a nivel nacional. Las técnicas de la investigación documental que se ejecutaron son: extracción de datos teóricos y estadísticos con la guía de fichas de registro de datos bibliográficos(autor, tema tratado, enlace) de las fuentes y posterior edificar una lluvia de ideas de conceptos y estadísticas; por tanto, se procedió a identificar las fuentes pertinentes al tema, organizarlas en dichas fichas para proceder a revisar la información y priorizar el desglose de las ideas significativas a la materia para seguidamente enriquecerlas con el apoyo teórico y desarrollarlas.

La selección de la información se rigió por los principios de: pertinencia, exhaustividad y actualidad; la pertinencia se enfatiza en el significado y relación directa de los contenidos con los objetivos determinados, capaces de ofrecer refuerzo para justificar la problemática y alcanzar soluciones; la exhaustividad se resume en la profundidad de las aristas retomadas y la actualidad se requiere al buscar fuentes actuales y a la vez responder a una necesidad emergente por la época de masividad de datos y recursos digitales, en la cual se desempeña la población, en específico la educativa; y recordar lo que se recalca en el sitio web de la Biblioteca Centro de Recursos para el Aprendizaje y la Investigación (CREI) por parte de Grela (2018) “En este sentido, un documento pertinente es un documento que resulta ser oportuno a las necesidades individuales de información,

necesidades que deben ser precisadas con anterioridad a la búsqueda de información" (párr. 2); donde cada principio debe ligarse a la coherencia y claridad del texto presentado.

A continuación, se enmarcan las etapas o fases de la investigación documental realizada:

1. Se selecciona el tema según la actualidad y afinidad, se delimita el problema de estudio ¿Cuáles son acciones teóricas y prácticas que el director debe cumplir para gestionar la ciberseguridad del centro educativo y los miembros que conforman la comunidad estudiantil? Se realiza búsqueda de antecedentes teóricos nacionales e internacionales para delimitar el problema según la necesidad expuesta por los autores y elaborar las preguntas generadoras que sirven para abarcar la problemática general.

2. Definir el objeto de estudio y escoger una metodología adecuada al mismo: Paralelo al paso anterior acorde al tema se identifica el objeto de estudio para estructurar el planteamiento del problema y abarcarlo en los objetivos por desarrollar. El objeto de estudio de la temática es la ciberseguridad en centros educativos, luego se delimita la metodología acorde donde se utiliza la investigación documental hemerográfica, tomando en cuenta lo mencionado por Cortés y González (2021)" el investigador debe decidir cuál es el paradigma más apropiado para responder dicha pregunta y, así, acercarse a la realidad por medio de una metodología específica que indique cómo recopilar datos y cómo tratarlos." (párr19); demás se requiere articular el objeto de estudio en la redacción de los objetivos.

3. Recuento de fuentes: se indaga sobre el material electrónico que podría ser útil para la investigación documental. Se organizan las fuentes para luego extraer la información acorde al problema y los objetivos, se descartan las que no cumplen con los propósitos de actualidad, pertinencia y exhaustividad; y se realizan fichas resumen de las fuentes elegidas para facilidad de identificarlas cuando se amerite ubicándolas en primarias y secundarias.

4. Revisión y comparación documental: partiendo de las fuentes seleccionadas se revisa el contenido. Se realizan lluvia de ideas de la información relacionada con los objetivos de la investigación y la contestación de las preguntas generadoras. Luego se compara el material seleccionado para obtener sustento textual. Se enlazan las ideas, conceptos y teorías de las

diferentes personas y organismos autores, se extrae citas textuales que fundamenten los antecedentes, la planeación del problema, la justificación, el referente teórico y la metodología; y sustenten la interpretación y el análisis por parte de la persona investigadora.

5. Interpretación, análisis y conclusiones: se analiza el material comparado y se elabora la propuesta crítica, complementándola con la opinión y las deducciones de quien investiga. Se realiza lectura critica de los documentos basándose en el sustento teórico, se desarrollan los contenidos resultantes de la comparación de información unida con el análisis y la interpretación para exponer la redacción de las ideas. Luego se elabora el cierre general enumerando los resultados de la investigación y se desglosan las conclusiones de la temática, se trazan estrategias que respondan a las interrogantes planteadas y otorguen posibles soluciones.

El contexto en el cual se requiere aprovechar los resultados obtenidos de la investigación se basa en el entorno de la comunidad educativa, tanto para las personas estudiantes como para el personal docente y administrativo de la Escuela Timoleón Morera Soto, de la Regional de Alajuela, circuito 03; la cual cuenta con trescientos discentes y treinta y cuatro entre quienes administran y dan lecciones. La institución se ubica en una zona urbana donde las familias se mantienen en un nivel socioeconómico medio; en el ambiente escolar se percibe el menester de activar alternativas de cuido de la identidad y de la información manipulada por medio del internet, tanto para los menores de edad como para los mayores de edad, se observa el uso indiscriminado de la red y sus opciones a la hora de utilizar correos o compartir datos gráficos o de carácter administrativo.

RESULTADOS Y DISCUSIÓN

RESULTADOS

Los siguientes resultados se basan en la pregunta general y el referente objetivo sobre la indagación de acciones teóricas y prácticas que el director o directora debe asumir para gestionar la ciberseguridad del centro educativo y de los miembros que conforman la comunidad estudiantil.

El primer resultado obtenido a partir de la investigación documental acerca de la interrogante de los principales términos relacionados con la temática de ciberseguridad, riesgos y vulnerabilidad surge con el aporte del autor López (2021) en la colaboración para el Fondo de las Naciones Unidas en la Infancia (UNICEF) en la publicación titulada Ciberseguridad en el 2021, ubicada en el Sitio Web Oficial del instituto, donde se extrajo que los conceptos relacionados con la problemática y los cuales deben ser manejados por las personas gerentes de la educación se vinculan con malware (software maliciosos con virus incrustados en archivos de orígenes no confiables o verificables), ransomware (códigos infiltrados provenientes de personajes mal intencionados que dañan los sistemas informáticos), hackeos de datos e identidad, y se complementaron con términos acerca del ciberacoso y propagación de noticias falsas.

El segundo resultado se encontró conexo con la pregunta de cuáles son las etapas para establecer protocolos de ciberseguridad en instituciones educativas, según el estudio las Cámaras de Tecnologías de Información y Comunicación (CAMTIC), las fases comienzan con la identificación de vulnerabilidades en cada institución, por medio de profesionales en analítica de datos y sistemas, que analicen los comportamientos y la infraestructura de red de los centros, como punto de partida para el diseño de lineamientos con el fin de evitar y enfrentar los posibles riesgos de perdida de información o atentados contra el robo de datos personales e institucionales. Paralelo se encontró el planteamiento del experto Gamboa (2023) de la Universidad Piloto de Colombia, se enfatizó que en un protocolo de ciberseguridad debe respetar los principios de reacción, integralidad, inclusividad, integridad, confidencialidad y autenticación, y mantenerse acorde a las normativas de las autoridades nacionales y locales.

En cuanto al resultado tres sobre los elementos que componen los procesos de capacitación y formación en el tópico investigado, los escritores de National Institute of Sanders and Technology

apuntaron en la fuente llamada “Un abordaje Integral de la Ciberseguridad”, la delimitación de concienciar y la relevancia de capacitarse en el tema, tanto los dirigentes de las instituciones como los participantes miembros activos de las entidades, por ejemplo las educativas, incluyendo en el proceso de información a mayores y menores de edad, lo que ellos catalogaron como la disminución de la brecha sobre ciberseguridad.

El resultado cuatro acorde a las recomendaciones teóricas para concienciar y las prácticas para ejecutar en máquinas o entornos de red expuso Prieto (2023) de la Saint Leo University en la obra referente a la Historia de la Ciberseguridad, que el punto focal para crear alternativas para protegerse como individuo y cuidar los sistemas informáticos y a la vez aumentar la concientización es centrarse en el aumento del movimiento de redes, tanto en la perspectiva de redes sociales y el compartir datos, como en la relacionada con las conexiones de equipo mediante la internet a nivel mundial como la intranet de carácter local; además del uso y actualización de software y herramientas para detectar errores en el aprovechamiento de cada red y sus nodos.

DISCUSIÓN

En las fuentes revisadas expuestas en los resultados se retomaron los conceptos en vinculación con la ciberseguridad particularmente enfocándolas al sector de centros educativos, los hallazgos encontrados responden a la realidad actual y a los peligros que deben enfrentar las instituciones al manipular cantidades crecientes de datos característicos del personal, de las personas estudiantes y en general de información relacionada con la diversidad de proyectos, programas para registros, entre otros, según la envergadura de dichas instituciones.

En las diferentes referencias convergen la mayoría de los términos que necesitan ser claros para las involucrados como, por ejemplo, las palabras riesgo y vulnerabilidad, unida a los ataques cibernéticos, por medio de códigos dañinos. También la repercusión del surgimiento del acoso cibernético o la transmisión de noticias no reales por la red, lo cual puede repercutir a nivel físico y psicológico.

Según la experiencia en centros educativos, en el Ministerio de Educación Pública, en los últimos años, se ha mostrado la tendencia de diseñar protocolos para tener guías de actuación en

circunstancias determinadas para resguardar la integridad de los y las dicentes e incluyen medidas formativas, pedagógicas o de apoyo psicológico y social, dichos protocolos se visualizan a través de pasos concretos y acordes a casos particulares, pero en el asunto de la ciberseguridad en dichos lugares, se observa un sesgo en cuanto a la implementación e identificación de riesgos y opciones para enfrentar la problemática. El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones como se evidencia en el análisis de la Agenda 2023-2027 sobre la Estrategia Nacional de Ciberseguridad propone alternativas a nivel país, e inclusive promueve cursos de protección de los niños y niñas en línea donde utiliza el MEP para difusión; pero directamente en el Ministerio de Educación Pública se requiere crear por etapas una ruta de acción sobre la seguridad cibernética que se adicione al ya existente lineamiento de protección a la identidad de la niñez y la adolescencia y se lleve a cabo en el contexto de cada institución.

Otra de las tendencias en el aspecto nacional y de ciberseguridad es la proliferación de cursos sobre el tema en institutos y universidades públicas y privadas; se evidencia el aumento de trato de estos tópicos en redes sociales y demás medios de comunicación, donde resalta la trascendencia de que en la actualidad se interactúe con estrategias para abordarlos en un entorno cotidiano y profesional; en las instituciones de educación se empieza a incluir la temática de seguridad cibernética en la materia de formación tecnológica, se busca que a mediano plazo se comience a formar una cultura entre la comunidad educativa, donde la persona directora y quien es parte del entorno se responsabilicen de fomentar hábitos de protección individual y grupal.

Según lo puesto en las fuentes consultadas, se da la necesidad de una infraestructura de red eficaz y eficiente que apoye el objetivo de seguridad en las entidades donde se manipula información de carácter privado de personas menores y mayores de edad; entre las prácticas que se recomiendan en la mayoría de bibliografía examinadas inician por el uso de valores como la cautela y el aprovechamiento de aplicaciones como antivirus, cortajuegos, herramientas de gestión de identidad de accesos, escáneres de vulnerabilidad y sistemas de prevención y detección de instrucciones; para lo cual en las organizaciones, incluyendo las de educación, se debe realizar la proyección del presupuesto para ejecutar las acciones de seguridad digital.

CONCLUSIONES

En el proceso se logró responder a las preguntas generadoras, pero debido a la extensión y el tipo de la presente investigación se podría ampliar la misma en siguientes indagaciones enumerando ampliamente los protocolos de asesoramiento por parte de empresas especialistas en ciberseguridad, y describir a profundidad los software existentes en el mercado para la protección de instituciones públicas y privadas, donde se delimite las características informáticas de los recursos y se enlacen a la infraestructura de red de las escuelas y colegios, tomando en cuenta el filtrado de contenidos acorde a los establecimientos. Y en cuanto a la suma de términos trascendentes para ser tratados en apartados posteriores serían el phishing conocido como el "pescar víctimas", por ejemplo, al mandar enlaces atractivos que luego lleven a sitios falsos; smishing que son mensajes provenientes de delincuentes; qrshing que es la simulación de códigos QR de marcas suplantadas, entre otros.

A partir de la investigación realizada pueden surgir nuevas interrogantes para estudios posteriores como ¿Cuál es el papel del Ministerio de Educación Pública en la formación en ciberseguridad en administradores educativos?, ¿Cuáles son alternativas para que el Gobierno asigne presupuesto para el abordaje teórico y práctico de la ciberseguridad en cada institución educativa? o ¿Cómo gestionar el apoyo de organizaciones internacionales para los centros educativos nacionales a nivel de equipamiento y capacitación?

Los resultados extraídos y los requerimientos en los centros educativos se pueden proyectar a la necesidad de protección cibernética en las familias del personal y los y las discentes, aplicándose los hallazgos a un nivel más amplio de la comunidad y luego de la sociedad, para luego unirse a la visión de seguridad digital que se busca en el país, al responder a características de un mundo conectado y formado en hábitos de respeto a la identidad y a la información privada, se recomienda avanzar en el acompañamiento de los y las menores de edad en el fortalecimiento de la reflexión antes de dar a conocer imágenes, textos, contraseñas y demás datos sensibles, donde reconozcan el alcance de las acciones y las consecuencias legales y emocionales que podrían enfrentar como participantes directos o a un ser querido, donde se incluyen las amenazas y extorsiones.

En el campo académico se dio el aporte al impulsar el reconocimiento de la incidencia de riesgos cibernéticos en el ambiente cercano donde se desenvuelven diariamente los miembros de la comunidad educativa, no exentos de sufrir robos virtuales de información personal, familiar o financiera, a través de páginas web no seguras, descargas indiscriminadas, instalación de programas no verificados con autenticidad de originalidad, dispositivos como computadoras, tabletas, celulares, cámaras de vigilancia u otros artículos los cuales poseen conexión a internet; y se deben considerar.

Según las fuentes consultadas en la investigación documental las personas informadas al respecto con la ciberseguridad y las aplicaciones del tema, adicionado al establecimiento de redes confiables ayuda a detener un porcentaje de más de 50% de estos ataques en escuelas y colegios; donde el sector educativo ocupa el tercer lugar a nivel mundial de dichas vulnerabilidades con hackers que se adentran en las cuentas, correos o sistemas de control de pagos escolares.

La importancia de las revelaciones encontradas radica en preocuparse y ocuparse de la de concientización, contar con planes de interacción, ciclos donde se hable y se trasmita rutinas y conocimientos de los padres, madres o encargados hacia los hijos e hijas, de las personas docentes hacia los y las discentes, entre colaboradores de las instituciones y de estos hacia quienes son encargados o encargadas legales y viceversa; además debe darse una formación articulada sustentada con estrategias diseñadas por especialistas en el campo. Es relevante referir para las calificaciones a profesionales con habilidad informática y con destreza pedagógica para que se logre la asimilación de los procesos.

El director o directora de una organización educativa debe asumir la responsabilidad de articular junto con el personal las medidas aprovechamiento digital y avalar el tratamiento de los recursos de tal forma que se potencie el beneficio integral para el proceso de enseñanza aprendizaje y del quehacer docente-administrativo, sin caer en peligros propios del uso inadecuado de la tecnología, internet, espacios virtuales para compartir o para investigar.

REFERENCIAS

CAMTIC. (2021). Estudio internacional revela que centros educativos son los más afectados por cibercrimen. CAMTIC. https://www.camtic.org/actualidad-tic/estudio-internacional-revela-que-centros-educativos-son-los-mas-afectados-por-cibercrimen/

Cervera, J. (2023). El 80% de los centros educativos han sufrido algún ciberataque en 2023. The objetive. https://theobjective.com/tecnologia/2023-09-17/ciberataques-centros-educativos/

Comisión Económica para América Latina y el Caribe. (2022). Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe. https://repositorio.cepal.org/server/api/core/bitstreams/2b53c8ee-380e-47de-b115-298e8e06eeaa/content

Camarillo, M., T. (2024). Investigación documental. Concepto. Boletín del IIb, vol. xx, núm. 1 y 2, México, primer y segundo semestres del 2015http://publicaciones.iib.unam.mx/index.php/boletin/article/viewFile/790/761

Cortes, M. y González, M. (2021). *Delimitación del problema y la pregunta de investigación* https://www.librosoa.unam.mx/bitstream/handle/123456789/3295/Delimitacion_final.pdf?sequence=1&isAllowed=y

Digital Security. (2023). El sector educativo, el más castigado por el ransomware en 2023. It. Digital Security. 11 setiembre 2023. https://www.itdigitalsecurity.es/actualidad/2023/09/el-sector-educativo-el-mas-castigado-por-el-ransomware-en-2023

Edron (2022). Por una cultura de ciberseguridad. Edron blog. 08 abril, 2022. https://edron.edu.mx/es/por-una-cultura-de-ciberseguridad/

Gaitán, C. (2022). *Arte y género en la homografía: fuentes primarias para el Siglo XX*. https://digital.csic.es/bitstream/10261/283318/1/Introducci%C3%B3n_Arte_g%C3%A9nero_hemerograf%C3%ADa.pdf

Gamboa, J. (2023). Importancia de la Seguridad Informática. Universidad Piloto de Colombia, Gamboa, Seguridad Informática y Ciberseguridad http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%C3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y

Graciano, C. (2021). *Adolescentes y el uso de internet. Fondo de las Naciones Unidas Republica Dominicana.* https://www.unicef.org/dominicanrepublic/media/5771/file/Adolescentes%20y%20el%20uso%20de%20Internet%20-%20PUBLICACI%C3%93N.pdf%7D

Grela, L. (2018). Criterios para evaluar la pertinencia de las fuentes de información. Biblioteca CEU-CRAI https://blog.uchceu.es/biblioteca/criterios-para-evaluar-la-pertinencia-de-las-fuentes-de-informacion/

León, R. Astorga, C. Luna, J. Schmidt, I. López, A. (2020). Peligro de las redes sociales: educando en ciberseguridad. Universidad Nacional de Costa Rica. Ponencia. https://repositorio.una.ac.cr/handle/11056/19261?show=full

López, R. (s.f.). Ciberseguridad. UNICEF, México https://www.unicef.org/mexico/ciberseguridad

MICITT. (2023). Estrategia Nacional de Ciberseguridad 2023-2027. MICITT. Gobierno de Costa Rica. https://www.micitt.go.cr/el-sector-informa/micitt-presenta-la-estrategia-nacional-de-ciberseguridad-2023-2027

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (2023). Gobierno de Costa Rica. https://www.micitt.go.cr/gobierno-digital/ciberseguridad#:~:text=El%20Centro%20de%20Respuesta%20de,del%20Estado%20todo%20lo%20relacionado

Ministerio de Educación Pública. (2020). *Criterio con respecto al uso de la imagen de personas menores de edad*. Gobierno de Costa Rica https://www.mep.go.cr/sites/default/files/proteccion-imagen-persona-menor-edad.pdf

National Institute of Standards and Technology. (2019). Ciberseguridad marco NIST. Slideshare. https://es.slideshare.net/franco592473/ciberseguridad-marco

OpenAI. (2024). ChatGPT (versión del 10 de enero 2024) [La falta de ciberseguridad en centros educativos] https://chat.openai.com/chat

Prieto, E. (2023). ¿Cuál es la historia de la ciberseguridad? Saint Leo University https://worldcampus.saintleo.edu/noticias/historia-de-la-ciberseguridad#:~:text=La%20Ciberseguridad%20no%20naci%C3%B3%20hasta,que%20conocemos%20en%20la%20actualidad.

Prosic (2010). *Ciberseguridad en Costa Rica.* Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.prosic.ucr.ac.cr/sites/default/files/documentos/ciberseguridad_2010.pdf

Syed, Z. (2021). Cómo ayudar a proteger su escuela de los ataques de ransomware. https://calmatters.org/calmatters-en-espanol/2021/07/como-ayudar-a-proteger-su-escuela-de-los-ataques-de-ransomware/

UNESCO (2023). Directrices para la formulación de políticas y planes maestros de TIC en educación. Biblioteca digital. https://unesdoc.unesco.org/ark:/48223/pf0000385091

Universidad Nacional Autónoma de México (2017). Unidad de apoyo para el aprendizaje. SUayED. UNAM. https://repositorio-uapa.cuaieed.unam.mx/repositorio/moodle/pluginfile.php/1516/mod_resource/content/3/contenido/index.html

Universidad Veracruzana. (2014.). Tipos de investigación. Biblioteca general de humanidades. https://www.uv.mx/apps/bdh/investigacion/unidad1/investigacion-tipos.html

Universidad Veracruzana. (2014.). Introducción a la investigación: guía interactiva. Biblioteca general de humanidades https://www.uv.mx/apps/bdh/investigacion/index.html

ANEXO N°1

Declaración Jurada.

Yo, María Vanessa Torres Jara, cédula de identidad 205750691, alumna de la Universidad Internacional San Isidro Labrador, declaro bajo fe de juramento y consciente de las responsabilidades penales de este acto, que soy la autora intelectual del Artículo Especializado para obtener el grado de Maestría Profesional en Administración Educativa, titulado:

La gestión de la ciberseguridad en los centros educativos del contexto costarricense: la gestión de un director.

Por lo que libro a la Universidad de cualquier responsabilidad en caso de que mi declaración sea falsa.

Alajuela, Naranjo, Naranjo a los 10 días del mes de abril del año 2024

Vanessa Torres

María Vanessa Torres Jara

205750691