HETS Online Journal
Volume 12, Issue 1, November 2021
ISSN 2693-9193

Cartografía conceptual: hacia la ciberseguridad proactiva para la educación, obligación de todos

Díaz-Rodríguez, Elizabeth
edrcc@yahoo.com

Resumen

Se presenta un análisis cartográfico del concepto de ciberseguridad en la educación a distancia desde un enfoque socioformativo. La principal conclusión es que como parte de las experiencias pedagógicas se busca capacitar a personas y equipos para resolver problemas del ciberespacio en la educación a distancia. La ciberseguridad es un problema de todos. Una intensa campaña de educación basada en la estrategia de solución de problemas aminora el daño de ciberataques y ciberamenazas.

Palabras claves: ciberseguridad, educación a distancia, proactiva

Abstract

An analysis of the concept of cybersecurity in distance education is presented from a socioformative approach based on conceptual cartography. The main conclusion is that as part of the pedagogical practices it seeks to train people and teams to solve cyberspace problems in distance education. Cybersecurity is everyone's problem. An intense education campaign based on a problem-solving strategy reduce the damage to cyberattacks and cyberthreat.

Keywords: cybersecurity, distance education, proacitve

Introducción

La sociedad busca la solución de problemas en la colaboración de las tecnologías de la información y la comunicación (TIC) (Deckard, 2020) y ha encontrado su catalizador en el azote de una epidemia a nivel global. La sensibilidad de los datos que se manejan en los ámbitos educativos hace que se requiera de soluciones de seguridad informática fiables y seguras de ataques (Lagua & Paul, 2018; Marchese, 2020). *La Ley de Derechos Educativos y Privacidad Familiar* de 1974 (FERPA), la *Ley de Oportunidades de Educación Superior* (2008) y *la Ley de Protección de la Privacidad Infantil* en Línea (1998) fueron creadas para proteger la privacidad de los datos de los estudiantes. Seguridad del perímetro de la red no es suficiente, es necesario proteger a los usuarios, los datos y los recursos de la red dondequiera que se encuentren (Aruba, 2021). Los atacantes son personas capacitadas para explotar vulnerabilidades, bandas criminales que buscan hacer producir dinero, buscando formas de violar los acuerdos de propiedad intelectual y derechos de autor (Hong, 2016; Lagua y Paul, 2018). Comprender los problemas y proporcionar métodos para evitar el riesgo es inminente.

La exploración sobre ciberseguridad está creciendo, sin embargo, la investigación empírica sobre las prácticas de seguridad es deficiente (Ulven y Wangen,2021). Se exhorta hacer disponible los datos de incidentes con la comunidad y trabajar hacia un marco común de clasificación de incidentes para la presentación de informes. Intrusiones, programas malignos (*malware)*, activos vulnerables, el escaneo, los ataques de ingeniería social y la divulgación accidental son los más comunes (Ulven y Wangen, 2020). Fuga y perdida de datos, fraude financiero, pérdida de disponibilidad, abuso y ataques a la integridad de los datos son las consecuencias afectando el funcionamiento y la logística comercial de las instituciones.

Ciberseguridad en LMS

Las instituciones educativas se han provisto de sistemas de gestión de aprendizaje (SGA; en inglés, *learning management system* o LMS), programas instalados en un servidor que se utilizan para administrar y monitorear actividades presenciales y en línea donde establecen políticas de mitigación (la más destacada es el establecimiento de roles de acceso) operando dentro de un proveedor de servicios, que tiene sus propios riesgos de seguridad (Broncano & Pesantez, 2021; Cruz Valencia, 2018). Las actividades de los estudiantes en la plataforma comprometen el sistema (alteración y distribución de contenido, cambios no autorizados, alteración de calificaciones, destrucción de bases de datos y robo de identidad) (Cruz Valencia, 2018). El medioambiente donde se desarrolla el programa propicia riesgos adicionales a manera de correo basura (spam), phishing, sitios falsos dedicados al robo de credenciales de acceso, *spyware*, *software* malicioso para recabar información del usuario, instalación de publicidad molestosa, *malware*, software creado con la intención de robar información o dañar y los *crackers* (expertos informáticos en intervenir sistemas) (Cruz Valencia, 2018).

Objetivos

El propósito de la siguiente cartografía era reunir y analizar medidas y datos de la ciberseguridad en la educación a distancia para describir su concepción, producción, diseminación y estudio. Los datos obtenidos trazaron el significado de la ciberseguridad en la educación a distancia desde una perspectiva humanista, con las referencias más recientes, estableciendo ejes claves, analizando sus características y explorando sus vínculos con otros campos utilizando las categorizaciones de la cartografía conceptual. Se espera contribuir a

fortalecer e impulsar los estudios en el área y sus relaciones con la educación, la sociedad y las organizaciones (Deckard, 2020; Ortega-Carbajal et al., 2015).

Metodología

La presente investigación ha seguido el análisis documental con un enfoque cualitativo para determinar los ejes claves del concepto de ciberseguridad en la educación a distancia. El análisis consistió en la búsqueda, recuperación, análisis, crítica e interpretación de datos obtenidos por otros investigadores en fuentes documentales y artículos (Ortega-Carbajal et al., 2015; Hernández-Sampieri & Mendoza 2018).

Tipo de estudio

El estudio es cualitativo basado en el análisis documental (Ortega-Carbajal et al., 2015; Tobón, 2015) utilizando la técnica de cartografía conceptual en torno al concepto ciberseguridad en la educación a distancia.

Técnica de análisis

La estrategia de análisis fue la cartografía conceptual, "una estrategia de construcción y de comunicación de conceptos basada en el pensamiento complejo, mediante aspectos verbales, no verbales y espaciales" (Requena, 2020. p.1 citando a Tobón, 2004, p.11). Requena sugiere añadir un eje adicional denominado causación ya que "gran parte de los constructos empleados en las ciencias humanas y sociales, como la psicología, están referidos a fenómenos o procesos, los cuales tienen existencia en redes de relaciones causales: son influidos e influyen a otros fenómenos" (Requena, 2020, p.2).

Criterios para la selección de los documentos

Se inició la investigación con la búsqueda y selección de los documentos en torno a la importancia de la ciberseguridad en la educación a distancia, utilizando estudios y artículos de producción científica. La selección de documentos se realizó a partir de las palabras claves que tuviesen elementos teóricos metodológicos para abordar los ejes de la cartografía conceptual.

Resultados

A continuación, los resultados presentan el análisis de cada una de las categorías de la cartografía.

Noción. ¿Cuál es la etimología del concepto ciberseguridad para la educación a distancia? ¿cuál es su desarrollo histórico y la definición actual?

El concepto de ciberseguridad responde a una época centrada en la informática, al auge de Internet y su amplia red de dispositivos (Dutton et al., 2019). La etimología del término se divide en dos partes, ciber-se origina del inglés cyber, y es el acortamiento de la palabra *cybernetic* 'cibernético'. Su elemento compositivo tiene relación con las redes informáticas (Dutton et al., 2019). Algunos términos derivados: ciberespacio, ciberespaciales, cibernauta y cibernético. Otro vocablo relacionado es seguridad que proviene del latín securĭtas*, -ātis*, de cualidad de seguro que proviene del latín *secūrus*., adjetivo de que implica libre, sin riesgo (Fundéu RAE, 2020). “La ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos” (Kaspersky Lab, 2020). ¿Cuáles fueron los comienzos de la ciberseguridad?

La civilización mesopotámica, 1.500 antes de Cristo (aC), utilizaban estenógrafos y cifrados. Felipe II guardaba los tesoros utilizando el método de cifrado con dos claves. Durante la Segunda Guerra Mundial, Hedy Lamarr, junto a Geroge Antheil crearon un sistema de comunicación secreta. En 1962, la seguridad consistía en la comunicación mediante la conmutación de frecuencias. Para el 2005, el término emerge ante amenazas del ciberespacio y ciberterrorismo (Jesús & Robledo, 2020). El objetivo consistía en cuidar, proteger, garantizar la confidencialidad, integridad y disponibilidad de la información anteponiéndose a los actos criminales (Roush, 2020). La ciberseguridad en la educación a distancia se concentró en la no presencialidad, relación docente-estudiante, la interactividad, las experiencias de aprendizaje (Ulloa Brenes, 2021) y el apoyo de una institución con funciones administrativas. Respondiendo a los eventos de la época se fue integrando dentro de la educación a distancia el concepto de ciberseguridad procedente de entornos militares y gubernamentales. La asignación de responsabilidades diarias para evaluar, gestionar e informar los riesgos de manera adecuada a todo el personal académico y grupo de apoyo componía el primer paso para enfrentar las emergentes amenazas yuxtapuesto con el cumplimiento de las medidas de la *Ley de Protección de Datos* (*Ciberseguridad en la educación a distancia eLearning*, 2021).

Categorización. ¿A qué clase inmediatamente mayor pertenece el concepto de ciberseguridad en la educación a distancia?

La ciberseguridad en la educación a distancia pertenece a la clase mayor de las Tecnologías de la Información y Comunicación (TIC) y a la Seguridad. Las TIC tienen una capacidad para almacenar enormes cantidades de información que facilitan el intercambio entre ordenadores, superando los obstáculos espaciales y temporales (Evaluando software, 2016). Su

empoderamiento radica en la diversidad de lenguajes, audiovisuales y el hipertexto, acomodados a la vida cotidiana. La Seguridad en la modalidad de ciberseguridad protege la información de riesgos, en sus diferentes formas digitales y los sistemas interconectados que la procesan, almacenan o transmiten (welivesecurity, 2015).

Caracterización. ¿Cuáles son los elementos centrales que le dan identidad a la ciberseguridad en la educación a distancia?

Los rasgos propios que le dan identidad a la ciberseguridad en la educación a distancia se fundamentan tres principios. Primero, confidencialidad para mantener los datos intactos frente a alteraciones o modificaciones. Disponibilidad para garantizar la integridad del control de flujo de datos (Grupo proyecta, 2019) e identidad. Los entornos político, económico y social (Deckard, 2020; Dutton al., 2019; Moreno, 2020) junto con la riqueza, el producto interno bruto (PIB), número de usuarios del Internet, centralidad del uso y el tamaño de las naciones (población total) son colaterales en la delineación de identidad (Dutton et al., 2019).

Diferenciación. ¿De cuáles otros conceptos cercanos se diferencia el concepto de ciberseguridad en la educación a distancia?

La ciberseguridad de la educación a distancia se relaciona con los conceptos de seguridad informática, sistemas informáticos y ciberseguridad. Son conceptos cercanos, pero a la misma vez diferentes. Las medidas de protección relativas a la seguridad informática y ciberseguridad son tecnológicas y se ponen en funcionamiento en los departamentos de tecnologías. La diferenciación de cada concepto lo determina en quien debe tomar las decisiones sobre el nivel de protección adecuado y quién debe garantizarlo mediante la implantación de medidas de seguridad tecnológicas. La confusión nace de la costumbre de asignar a los técnicos toda la

seguridad (Jesús & Robledo, 2020). La seguridad informática protege los activos de información en formato digital, los sistemas informáticos los procesan y almacenan, indistintamente si están interconectados o no y ciberseguridad, se orienta a proteger a los activos de información en formato digital (Jesús & Robledo, 2020). La seguridad de la información abarca todas las áreas de las organizaciones educativas, independiente del medio en que se encuentre la información (Jesús y Robledo, 2020).

El mundo de la ciberseguridad converge con otros conceptos cercanos. Por ejemplo, el IdC (Internet de las Cosas), la interconexión digital de objetos cotidianos, el acoso o la violencia física virtual, obscenidades, conflictos escolares en la red, rebeldía o mal comportamiento, exposición de datos personales, chantaje cibernético, intimidación (Gross et al., 2017) y el *Big data o* el gran volumen de datos que inundan la red utilizado por las organizaciones que los manejan interfiriendo con la ciberseguridad.

Clasificación. ¿En qué subclases o tipos se clasifica el concepto de ciberseguridad en la educación a distancia?

Los criterios para la clasificación pueden agruparse según el tipo de protección al equipo que se ofrece, los niveles de vulnerabilidad, el alcance del desarrollo de las capacidades en ciberseguridad, las categorías de personal, los tipos de seguridad, los puntos más críticos de protección a los usuarios, tipos de delitos y la potencialidad del daño a la seguridad. Al agrupar el concepto de ciberseguridad en la educación a distancia siguiendo el criterio de vulnerabilidad, se encasillan considerando las vulnerabilidades de día cero (acaba de ser descubierta y se presenta de forma desconocida), aplicaciones de la web y gestores de bases de datos (Molina et al., 2020). Cualquier análisis de vulnerabilidades debe der precedido por la determinación del

alcance. Primero se identifican todos los recursos que forman parte de los sistemas de información de la organización, mediante registros que contengan amenazas y vulnerabilidades para mantener un depósito central de acciones correctivas (*Los 5 principales escáneres de vulnerabilidades para patrullar las redes*, 2021). Luego se organizan según los criterios establecidos por la institución (Dutton et al.,2019). Finalmente, se subdividen basándose en la naturaleza de la agresión: espiar, acosar (*stalkear*); engaño pederasta por la red(*grooming*); bloquear o restringir (*banea*r); secuestro de datos (ransomwear), sobreexposición filial(*sharenting*) y falsificación de páginas para captar datos privados de los usuarios (*phishing)* entre otros (Fundéu RAE, 2014).

Agrafiotis (2018) fundamentó su clasificación de ciberseguridad en el potencial del daño: daño físico, digital, económico, psicológico y reputacional. La empresa Sophos agrupa los daños en provenientes del acceso remoto o del acceso a datos confidenciales para implementar capacidades avanzadas de protección teniendo en cuenta la capacidad del usuario, su concienciación y capacitación para contrarrestar los ataques de ingeniería social (Castañares,2020; Iberia, 2020; Sophos,2020). Los ciberataques exitosos son muy costosos. En junio de 2020, una universidad pública pagó a sus atacantes más de 1.1 millones de dólares. Esto no incluye ni el tiempo ni el esfuerzo necesario para determinar el alcance del ataque, negociar y luego asegurarse de que el sistema esté completamente restaurado (Aruba, 2021).

Vinculación ¿Cómo se relaciona el concepto ciberseguridad en la educación a distancia con determinadas teorías, procesos sociales, culturales y referentes epistemológicos que estén por fuera de la categoría?

Las teorías, los procesos sociales, culturales trascienden la ciberseguridad en la educación a distancia. Simultáneamente dan forma epistemológica al concepto. Históricamente, las teorías de la educación avanzaron de un enfoque conductista a uno cognitivo, constructivista y conectivista. Los modelos de aprendizaje a distancia son paralelos a las teorías emergentes que dan forma a su epistemología (Intermulticulturalidad, 2018; Ulloa Brenes, 2021). Los modelos heteroestructurales en la educación a distancia propician el aprendizaje por repetición, incitado por estímulos extrínsecos e intrínsecos. El fin del aprendizaje es una asociación de estímulo respuesta (Intermulticulturalidad, 2018; Ulloa Brenes, 2021). Los modelos autoestructurales consideran la actividad del estudiante en su propio desarrollo cognitivo, centralizándose en la socialización y el trabajo grupal (Intermulticulturalidad, 2018), influenciado por la teoría sociocultural de Vygostky (Intermulticulturalidad, 2018; Ulloa Brenes, 2021). El modelo interestructurante conocido como dialogante se centra en identificar dimensiones cognitivas, socioafectivas y práxicas. El aprendizaje es un proceso activo y mediado en el que se debe usar diversidad de estrategias que garanticen reflexión, aprendizaje y diálogo; condicionado por el contexto cultural y social en que se ha gestado (Intermulticulturalidad, 2018) para la transformación de la sociedad mediante el desarrollo de competencias que integren conocimientos (saber), habilidades (hacer) y valores (ser).

Prevalecen cuatro teorías (Ulloa Brenes, 2021). La teoría de autonomía e independencia donde sus principales expositores fueron Charles Wedemeyer y Michael Moore centrada exclusivamente en el aprendizaje. (Ulloa Brenes, 2021). La teoría de la industrialización por Otto Peters para una planificación estandarizada y racionalizada, sustentada en la tecnología como puntal de metas pedagógicas a gran escala y masificación, emulando la producción (Ulloa Brenes, 2021). La teoría de la interacción y de la comunicación de Börje Holmberg donde

predomina un sistema de enseñanza abierto y a distancia. El diálogo se concreta en la interacción y conversación que establece el alumno con los materiales didácticos y se complementa en la interacción educador-educando. La interacción es parecida a una conversación guiada. Fomenta la heterogeneidad, libertad de elección e independencia (Ulloa Brenes, 2021). Por último, la teoría de la equivalencia de Hilary Perraton, donde promueve cualquier medio en tanto éste sirva para una comunicación y un aprendizaje efectivo. El estudiantado, de acuerdo con sus características individuales, accede a estrategias de instrucción diferenciadas pero equivalentes, adaptadas a las características individuales o grupales, sin afectar la calidad y equidad de acceso a los recursos pedagógicos (Ulloa Brenes, 2021). Todas las teorías y los modelos se cobijan bajo la relación educador-educando, la interactividad facilitada por las tecnologías de comunicación y las experiencias de aprendizaje (Ulloa Brenes, 2021). Los cursos se realizan con un dispositivo electrónico con acceso a Internet; docentes certificados internacionalmente y protocolos en la certificación de asistencia de los participantes. Para lograr los objetivos, acoplarse a las teorías y modelos educativos y cumplir con los estándares y requisitos para ayudas económicas gubernamentales se recopilan una gran cantidad y variedad de datos. Los componentes del sistema educativo necesitan acceso a esta información alimentando una cultura abierta y colaborativa que propicia los ataques cibernéticos (Aruba, 2021).

El mundo virtualmente globalizado implementa modelos para el uso responsable de la tecnología en la educación a distancia. Los dos modelos más populares (Urvan & Wangen, 2021) lo constituyen el *ADDIE* (Análisis, Diseño, Desarrollo) y Aseguramiento de la Información (IA). Cada institución establece uno o varios modelos con políticas normativas, guías y estándares integrando los conceptos de diversidad funcional, diseño universal e inclusión en una delineación y pertinencia para la equidad.

La etimología del concepto como bien se discutió en la noción número uno responde a una época centrada en la seguridad informática (Dutton et al., 2019). Se centra en la protección del conocimiento. La epistemología acomoda significaciones que nos ayudan a entenderlo. El fundamento epistemológico explícito y específico del contexto es esencial para la conciliación de la variedad de perspectivas y dimensiones de la ciberseguridad organizacional, incluyendo su gestión y estrategia. La construcción epistémica del conocimiento en la ciberseguridad se relaciona con la comprensión del contexto y sus interrogantes (Sallos, et al. 2019; Williams, 2021). Las creencias individuales actúan de forma local, temporal y secundario al tomar cualquier acción (Sallos et al.,2021). Sallos et. al (2019) dirige la epistemología de la ciberseguridad a la respuesta de ¿qué es el conocimiento de la ciberseguridad?, ¿dónde encontrarlo? y ¿cómo debería utilizarse? El conocimiento de la ciberseguridad es naturalmente inferencial. Las vulnerabilidades y amenazas se basan en el comportamiento del sistema hacia estados futuros que no pueden observarse directamente (Sallos et al.,2019). Conocer es estar al tanto de estrategias de gestión para inferir el valor de los procedimientos con base en la evidencia disponible. Si el conocimiento es incompleto (incertidumbre epistémica) entonces inhabilita el conocimiento del verdadero estado de un sistema (Sallos et al.,2019). El conocimiento epistemológico de la ciberseguridad de la educacion a distancia se encuentra en la sociedad misma. La comprensión del conocimiento está anclada en una red coordinada (con múltiples subsistemas) de conocedores (Sallos et al.,2021) y en una metacognición colectiva análoga (Sallos et al.,2019). ¿Como utilizarlo? El conocimiento posibilita trazar las estrategias ante un descriptor de un contexto hostil. Si la estrategia no es una inferencia efectiva conlleva la ausencia de regularidades ontológicas observables, limitaciones en la capacidad para adquirir y utilizar información relevante sobre la base de vulnerabilidades, amenaza relevante y efectos potenciales

de los incidentes de ciberseguridad (Sallos et al.,2019). Sallos y colaboradores recomiendan una visión pragmática para lidiar y recuperarse de incidentes (Sallos, et al. 2019; Williams, 2021).

La educación a distancia, la educación virtual y otras epistemologías pedagógicas implican especular en el conocimiento; extendiéndose a los métodos de acceso y transferencia, a los formatos de creación y representación (Universidad Estatal a Distancia [UNED], 2017). La reflexión epistémica abarca un repertorio de experiencias culturales acumuladas y potenciadas de realidades e ideas en el entorno individual y comunitario. Cada experiencia real o conceptual forja sus propias capacidades de metacognición durante el proceso (UNED, 2017). Durante la experiencia cibernética la relación entre el sujeto y el objeto es recíproca y protagonista. El sujeto toma decisiones en torno a los objetos de conocimiento, estos asumen un papel retroalimentador. Los objetos de conocimiento inducen transformaciones en el propio sujeto, como resultados de las decisiones activadas por sí mismo. El sujeto conoce al objeto dinámicamente, aprende su esencia y experimenta la modificación de su propio yo, al constituirse en el receptor de una retroalimentación inmediata (UNED, 2017). La tecnología enriquece el sistema cognitivo, social y cultural, pero es el educando responsable de seleccionar sus propias herramientas de aprendizaje, ambientes, redes y comunidades virtuales (UNED, 2017). Ante la diversidad funcional, las inteligencias múltiples y las dificultades contextuales, se concreta la conexión epistemológica entre lo que se sostiene; lo que se profesa en el discurso; y, lo que se desarrolla tanto en la mediación pedagógica como en el diseño de entornos educativos virtuales. Para lograrlo es necesario recorrer el camino de la renovación de los esquemas instruccionales tradicionales por espacios de investigación, interés, motivación y curiosidad con el fin de desarrollar competencias más allá de la aplicación de teorías (UNED, 2017).

Teorías, procesos sociales y la cultura en la educación a distancia le dan vida al perfil de ciberseguridad educativa (Dutton et al., 2019 & Morán Blanco,2017). Los componentes del sistema utilizan redes sociales y tecnología con un exceso de confianza e inexperiencia (Delgado, 2019). Los datos estudiantiles son más fáciles de explotar porque tienen pocos antecedentes. Las sumas de dinero por la información son sustanciales (Delgado, 2019).

El cambio epistemológico que vive la sociedad de la información y el conocimiento está basado en el tránsito de un modelo centrado en la transmisión, la recursividad, el holograma y el protagonismo del usuario para generar y recrear contextos, además de recibir información, consumirla y aplicarla, lo que retumba en la necesidad de la ciberseguridad en la educación a distancia (Fainholc, 2007).

Metodología. ¿Cuáles son los elementos o ejes claves que conlleva la aplicación de ciberseguridad en la educación a distancia?

La aplicación de ciberseguridad en la educación a distancia conlleva parámetros, leyes y protocolos que se van aplicando según los eventos y ataques acontecen. En marzo de 2021, la división cibernética de la Oficina Federal de Investigaciones advirtió sobre un aumento en ataques cibernéticos a instituciones educativas. El Buró Federal de Investigaciones recomendó la segmentación de la red, deshabilitar el acceso remoto, evitar uso de wifi público, centrarse en la sensibilización y educación (Aruba, 2021). Se exhortó a los usuarios a crear contraseñas seguras, actualizadas con regularidad, cerrar la sesión de las aplicaciones antes de dejar su dispositivo desatendido y no abrir correos que pueden proporcionar a los piratas informáticos un punto de entrada a la red. Las prácticas de seguridad van más allá del mero hecho de educar (Aruba, 2021). La eficacia radica en fomentar la adopción de las ventajas del protocolo correcto (*IP, Internet Protocol)*, promover la privacidad por diseño, seguridad por defecto anticipando y

previniendo eventos de invasión a la privacidad (Proyecto Lawi, 2018). Identificar los dispositivos que se conectan a sus redes, aprovisionarlos con políticas de seguridad para evitar ser explotados en un ciberataque, un buen antivirus y el escaneo regular de los sistemas ante las vulnerabilidades dan forma a las herramientas de protección (Aruba,2021). Adoptar un enfoque de "confianza cero" para la seguridad de la red, unificar redes cableadas e inalámbricas bajo una única consola de administración, implementar autenticación basada en roles, control de políticas, segmentación de la red en forma más inteligente y protección avanzada basada en la inteligencia artificial complementan la ciberseguridad en la educación a distancia (Aruba,2021). El auge de los vídeos que parecen convincentemente reales(*deepfakes*) y el aumento de los estados de emergencia declarados en las ciudades por los ataques masivos de programas malignos(*malaware*) transmuta la ciberseguridad de los dispositivos y redes escolares, induciendo a acciones acertadas como el filtrado de información y la administración responsable de datos (Irons 1970).

La aplicación de ciberseguridad en la educación a distancia ha llevado a CoSN (*Consortium for School Networking*) a establecer ejes claves para mitigar las continuas violaciones a la ciberseguridad (ASCD, 2020). Comienza con la configuración de un sistema de videoconferencia que requiera que los estudiantes tengan su contraseña y nombre de usuario; proteger las grabaciones de audio y video de acuerdo con las leyes federales y evitar grabar las discusiones en el aula con los estudiantes. Se estimula a los maestros a grabar previamente sus lecciones sin la presencia de los estudiantes, minimizando los riesgos de privacidad y evitar enviar enlaces en los correos electrónicos. Añade que se debe informar las razones por las que se está usando la tecnología y cómo está protegiendo la privacidad de los datos de los estudiantes. Permitir a los padres la posibilidad de optar por la abstención de participación de sus hijos en las

sesiones de video y tener métodos de conexión alternativos disponibles para aquellos estudiantes que lo necesiten; revisar los procedimientos y pautas del país y la institución con respecto al uso de dispositivos. Recordar a los educadores, estudiantes y padres que el personal nunca les pedirá sus credenciales de inicio de sesión por correo electrónico ni los amenazará con desactivar el acceso a las cuentas de la escuela por no acceder a un enlace. Considere implementar la autenticación de dos factores o de múltiples factores siempre que sea posible y examinar las normas de privacidad tanto para estudiantes como para profesores de encender una cámara web en una casa privada.

Ejemplificación. ¿Cuál podría ser un ejemplo relevante y pertinente de la aplicación de ciberseguridad en la educación a distancia?

Los ejemplos de ciberseguridad en la educación a distancia exponen lo relevante y pertinente de su aplicación. A medida que surgen nuevas formas insidiosas de violar datos y vulnerar códigos maliciosos en sistemas y programas críticos, los administradores intensifican su trabajo en protección, protocolos y ciberseguridad para que el aprendizaje continúe ininterrumpidamente (Deckard,2020; Press, 2019b). También duplican el uso de análisis de seguridad y automatización para ayudar a los equipos de seguridad con poco personal y fatiga a proteger los sistemas y los datos confidenciales, creando posturas proactivas (Press, 2019b) y el desarrollo de competencias para distinguir entre el conocimiento falso y el verdadero (Morán Blanco, 2017).

Las plataformas educativas accionan por la proactividad en la ciberseguridad. Por ejemplo, utilizando SaaS (*Software as a Service*) facilitan la gestión diaria de cualquier centro educativo: accesibilidad, agilidad, flexibilidad, seguridad y reducción de costos. SaaS, es una forma de disponibilidad de softwares y soluciones de tecnología por medio del Internet. El acceso es fácil

y simple: solo es necesario conexión. Las aplicaciones SaaS también son llamadas softwares basados en Web, *softwares on demand* o *softwares* hospedados. SaaS ofrece la tecnología de seguridad TLS, protocolo criptográfico para comunicaciones seguras en Internet, ejecutados en los servidores de las empresas proveedores y responsables de gestionar el acceso y mantener la estructura, la conectividad y los servidores necesarios para el servicio (Cruz Valencia, 2018; Sales Force, 2017). La mayoría cumple con el ciclo de desarrollo de sistemas (SDC), o ciclo de desarrollo de un *software*, planificando, analizando, diseñando y ejecutando ajustes periódicos de intervención (Blackboard Inc., 2018, Cruz Valencia, 2018).

Otro ejemplo es *Moodle* que se caracteriza por el servicio LAMP (Linux + Apache + Mysql +PHP) convirtiéndose en uno de los ejes vertebrales de los servicios que pueden encontrarse en Internet. El servidor Apache se concentra en la gestión de páginas HTML. También pueden alojarse en sistemas Windows, donde se instala un *Socket Security Layer* (HTTPS) a fin de que las sesiones de los usuarios no se transfieran en modo abierto (Cruz Valencia, 2018). Blackboard aplica las prácticas de ciberseguridad aceptadas en la industria apoyadas en la ingeniería del *Open Web Application Security Project* (OWASP), la aplicación de contramedidas específicas para las principales vulnerabilidades. OWASP y SDC ayudan a fortalecer la seguridad del producto y el programa de *Blackboard Learn*.

Causación. ¿Qué relaciones de causa y efecto guarda la ciberseguridad en la educación a distancia con fenómenos, procesos, condiciones o variables subjetivas, psicológicas o del contexto?

La ciberseguridad en la educación a distancia guarda una relación de causa y efecto con la subjetividad, la ingeniería social y la naturaleza del hombre. ¿Por qué? La ciberseguridad

responde a fenómenos, procesos, condiciones o variables subjetivas inherentes en la naturaleza humana. Las vulnerabilidades tienen relación con errores de codificación o puntos débiles y provienen o son causadas por la propia víctima por elementos particulares o subjetivos. El arte del hackear al individuo es utilizar las debilidades, necesidades, pasatiempos o gustos de los individuos para maniobrar. La pandemia y la acelerada digitalización han provocado un incremento de los ataques cibernéticos. (Bermúdez Rezabala & Moreira Vera, 2020).

Engaño, los ataques de bajo perfil(*hunting*), dirigir a un sitio web falso atacando al servidor Dns(servidor de nombres), con el afán de obtener información mediante la introducción de credenciales(*pharming*), recolectar informacion con fin malicioso(*dumpster diving*), fraude a través de la line telefónica o VoIP(*vishing*), suplantación de identidad(*pretexting*), anucios e información falsa con códigos maliciosos(*spam*), extorsión y el engaño al usuario para que piense que el administrador del sistema solicita información con fines legítimos (*phishing)* forman los elementos con los que trabaja la ingeniería social de la ciberseguridad. Conservar los derechos humanos, y establecer controles para evitar el abuso del poder es la meta de las instituciones educativas (Morán Blanco,2017).

Los ataques en el ciberespacio han forjado un nuevo enfoque tecnológico futurista: el desarrollo de una mayor resiliencia a los riesgos de seguridad en línea y todos los contextos de uso de Internet (Dutton et al., 2019). El objetivo es desarrollar actitudes proactivas incitando a las comunidades e instituciones educativas a participar en programas que fomenten las medidas de protección frente a cualquier agente perturbador o adverso del ciberespacio. A la misma vez propulsar programas, equipos y sistemas capaces de recuperar su estado inicial luego de una perturbación (Dutton et al.,2019).

Infringir las normas de ciberseguridad en la educación a distancia, resulta en delitos que afectan los procesos cognitivos, psicológicos y sociales de las víctimas. El ciberacoso es uno de los delitos más frecuentes. Sánchez-Domínguez (2020, p.1) comenta que "es un tipo de violencia digital que rompe los límites de la agresión presencial…Las consecuencias psicológicas … pueden permanecer durante años. Afecta… su entorno familiar y de comunidad".

La categoría de causación expone el comportamiento de los usuarios como una de las causas principales de violaciones a la seguridad digital (Dutton et al., 2019). La variedad heterogénea que compone la comunidad cibernética precisa de gestiones y estrategias múltiples (Dutton et al., 2019). Aunque diseño, adquisición, utilización de la tecnología y el estudio de las características de seguridad únicas de cada individuo o grupo pertenece a la ingeniería social, no se pretende dejar la ciberseguridad exclusivamente a los expertos ni a las máquinas (Dutton et al., 2019). La comunidad educativa es un elemento ingénito de la ciberseguridad, cuyo objeto es la seguridad de forma general, necesaria para toda la sociedad.

Los mismos grupos que utilizan Internet para su beneficio, lo explotan con fines terroristas y delincuenciales (Morán Blanco, 2017), señalando hacia los procesos sociales. La capacitación en la sociedad prepara al individuo para resolver lo que conoce, mientras la educación prepara para resolver lo que no conoce mediante el desarrollo del pensamiento crítico y la capacidad de solucionar problemas (Deckard, 2020). La educación en ciberseguridad no es exclusiva para el Departamento de Defensa ni los administradores, se ha convertido en un asunto global, internacional y social (Dutton et al., 2019 & Morán Blanco,2017). Los conflictos familiares, educativos, en la comunidad y las naciones trascienden al mundo virtual (De Pedro, 2019). La dinámica de interacción de los individuos y los distintos grupos entablan y reajustan

sus patrones de conducta, respondiendo los unos a los otros de manera recíproca para dar forma al proceso de ciberseguridad (Dutton et al., 2019 & Morán Blanco, 2017).

Discusión de resultados y conclusiones

Durante la cartografía cada eje explicó los aspectos relevantes de la ciberseguridad en la educación a distancia. Los ejes de conocimiento(noción), categorización, caracterización, diferenciación y clasificación levantan y trazan el camino para el entendimiento del concepto. El concepto se centra en la seguridad de las redes sociales aplicada a la educación por Internet y esta fuertemente relacionada con las tecnologías de la información y la educación y sus derivados. Se caracteriza por renglones dinámicos de confidencialidad, integridad y disponibilidad. La ciberseguridad en la educación a distancia se clasifica en diferentes grupos. La clasificación guarda relación con el enfoque del sujeto(s) involucrado(s). El eje cartográfico vinculación muestra como la epistemología de la ciberseguridad en la educación a distancia enfoca sus esfuerzos en lograr el conocimiento, la centralidad y el protagonismo del educando, donde se promueve consumir, usar y recrear el conocimiento. La epistemología es moldeada por las teorías, filosofías, paradigmas y movimientos de la época e influenciadas por la economía, la política de las naciones y varían en tiempo y espacio. La metodología es un conjunto de elementos de tipo racional que se emplean para alcanzar objetivos. El eje cartográfico metodología describe el procedimiento, las técnicas y las estrategias de trabajo que conlleva la aplicación de ciberseguridad en la educación a distancia. Se recomienda las técnicas recomendadas por el FBI para alcanzar la ciberseguridad (Aruba, 2021). Para seguir la línea se revelan ejemplos relevantes y pertinente de situaciones a los cuales se ven expuestas las instituciones educativas. Además, se incluyen tres ejemplos de la acción tomada por algunas instituciones mostrando los ejes claves que conlleva la aplicación de

ciberseguridad en la educación a distancia. Por último, la categoría causación, establece la relación directa de la aplicación de ciberseguridad en la educación a distancia con la subjetividad, la ingeniería social y la naturaleza del hombre, pilares para su optimización. A mayor ciberseguridad menor son los efectos psíquicos, anímicos y mentales. La ciberseguridad no es exclusiva de los expertos ni las máquinas (Dutton et al., 2019).

Para concluir, la ciberseguridad en la educación a distancia responde a la acción de convertir los dispositivos electrónicos en herramientas seguras. El objetivo inmediato de las TIC y sus derivados está en educarnos durante el trabajo, el estudio, la diversión y el consumo. Estas están moldeadas por las exigencias sociales, económicas y políticas. No obstante, al mismo tiempo que utilizamos cada una de las herramientas, hay que considerar que la naturaleza individual y social es influenciada por elementos orgánicos, emocionales, fisiológicas, patológicos y externos. Las tendencias individuales repercuten en el mundo virtual. Las características ingénitas a la naturaleza humana hacen eminente la ciberseguridad en la educación a distancia.

Recomendaciones

Cartografiar la ciberseguridad en la educación a distancia devela la necesidad de una transformación y una coherencia con las expectativas sociales y la educación (Marchese,2020; Salazar-Gómez & Tobón, 2018). Los datos de los usuarios es información relevante. Para los delincuentes suculenta. Consiguientemente, precisa de la aplicación de gestiones y estrategias fuertes para su protección y castigos severos para los que violen la seguridad. Los aspectos legales de los sistemas jurídicos, las soluciones técnicas innovadoras y estructuras organizativas racionales forman parte activa de la transformación (Marchese, 2020; Morán Blanco, 2017). Los

ciberdelincuentes han evolucionado. Los ataques *wetware,* combinando la generación automatizada de contenido y el esfuerzo humano manual para personalizar los ataques contra objetivos, y evadir cualquiera de las defensas provistas está en avanzada (Press, 2019b). Técnicas de defensa, evaluaciones, nuevas implementaciones de infraestructura para manejar la conectividad en todas las escalas son cruciales para resolver los desafíos (Bonderud, 2020). Los ciberataques, las transgresiones y la penetración en los sistemas informáticos(*hacks*) dominan los titulares noticiosos, la adquisición de cuentas de protección está en aumento (Press, 2019b). Los riesgos planteados por los eventos cibernéticos accidentales y perjudiciales nunca pueden cuantificarse por completo. Con el fin de tomar decisiones informadas sobre el costo de los recursos públicos y privados que se dedican a la protección cibernética y la seguridad, las organizaciones educativas necesitan expertos y usuarios educados que comprendan vulnerabilidades potenciales para desarrollar estrategias convenientes con el fin de mitigar los riesgos (Catota et al., 2019; Deckard,2020; Katz, 2018; Marchese, 2020). La solución a la seguridad en el ciberespacio es de todos con el fin de suscitar la proactividad y la resiliencia.

La ciberseguridad en la educación a distancia transciende de enfoques mecánicos a enfoques humanistas. Los procesos de enseñanza y aprendizaje demandan implementar estrategias que mejoren la calidad (Deckard, 2020) abordando los problemas desde todas sus vertientes, inclusive la seguridad cibernética. Los educadores analizan las necesidades reales de los estudiantes aplicando los saberes (ser, hacer, conocer, convivir) en una síntesis de actividad y retroalimentación para que a través del trabajo colaborativo se desarrolle conciencia y control sobre los procesos de pensamiento y aprendizaje. Para que la experiencia tenga éxito no debe ser interrumpida por la intromisión de vulnerabilidades ni los ataques de seguridad a los sistemas o plataformas. Monitoreo, *pentesting* (atacar entornos informáticos con la intención de descubrir

vulnerabilidades) y contar con el personal capacitado son elementos esenciales (Molina et al., 2020).

La ciberseguridad en la educación a distancia no es una opción. Los ataques cibernéticos dejan huella en la personalidad y en las empresas. Una intensa campaña de educación basada en la estrategia de solución de problemas amortigua el daño de ciberataques y ciberamenazas. La consecución de una cultura de ciberseguridad no es posible a través de meras acciones de divulgación, sino que requiere de una ingente labor formativa especializada para todos los sectores de la sociedad. La eficiencia de la ciberseguridad en la educacion a distancia se sustenta positivamente en una cultura de seguridad, educación y defensa (Achundia-Betancourt, 2017).

Referencias

Achundia-Betancourt, C. (2017). *Ciberseguridad en los sistemas de información de las universidades*. Course Hero. https://www.coursehero.com/file/63634685/Dialnet-CiberseguridadEnLosSistemasDeInformacionDeLasUnive-6102849pdf/

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Aruba. (2021, May 1). Five Ways to Improve Higher Education Network Security. *Ecampusnews*, pp. 1–7. https://www.ecampusnews.com/pdfs/five-ways-to-improve-higher-education-network-security/

ASCD (2020). *Cybersecurity guidelines for remote learning*. Cybersecurity Guidelines for Remote Learning - Educational Leadership. http://www.ascd.org/publications/educationalleadership/summer20/vol77/num10/Cybersecurity-Guidelines-for-Remote-Learning.aspx

Bermúdez Rezabala, R. E., & Moreira Vera, K. A. (2020). Análisis de las incidencias e impactos de ataques de ingeniería social o ciberdelitos en la carrera de ingeniería civil de la facultad de ciencias matemáticas y físicas. *Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Networking y Telecomunicaciones*. http://repositorio.ug.edu.ec/bitstream/redug/48832/1/B-CINT-PTG-

N.526%20Berm%c3%badez%20Rezabala%20Ronny%20Eduardo%20.%20Moreira%20Vera%20Kevin%20Andr%c3%a9s.pdf

Blackboard Inc. (2018). *Seguridad | Ayuda de Blackboard*. Help.blackboard.com. https://help.blackboard.com/es-es/Learn/Administrator/SaaS/Security

Bonderud, D. (2020, August 24). *Tips on reducing key remote learning security risks*. Technology Solutions That Drive Education. https://edtechmagazine.com/higher/article/2020/08/tips-reducing-key-remote-learning-security-risks-perfcon

Broncano, M. P. E., & Pesantez, D. F. Á. (2021). Ciberseguridad en los sistemas de gestión de aprendizaje (LMS). *Ecuadorian Science Journal*, *5*(1), 46–54. https://doi.org/10.46480/esj.5.1.98

Castañares, I. (2020, septiembre, 25). Ciberseguridad, el otro gran desafío de la educación a distancia vía internet. *EL CEO.* TIC

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The ecuadorian environment. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz001

Cruz Valencia, G. I. (2018). *Ciberseguridad para la educación online | Revista .Seguridad*. Revista.seguridad.unam.mx. https://revista.seguridad.unam.mx/numero22/ciber-seguridad-para-la-educacion-online

De Pedro, S. (2019, enero 22). *La ciberseguridad como responsabilidad social*. Blog Educación Y Bienestar Digital. https://gaptain.com/blog/la-ciberseguridad-como-responsabilidad-social/

Deckard, G. M. (2020). *Organizational challenges and concretion of cybersecurity education, training, exercises, and performance predictors within the United* States Department of Defense (Publication No. 27835096). [Doctoral dissertation, Indiana University]. ProQuest Dissertations & Theses Global. https://search.proquest.com/docview/2404611270?accountid=41558

Delgado, P. (2019). *Aumenta número de ciberataques a alumnos, ¿cómo pueden prepararse?* Observatorio | Instituto Para El Futuro de La Educación. https://observatorio.tec.mx/edu-news/ciberataques-universidades

Dutton, W., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity capacity: Does It matter? *Journal of Information Policy, 9*, 280-306. doi:10.5325/jinfopoli.9.2019.0280

einzelnet. (2020, julio 5). *La importancia de la ciberseguridad en entorno escolar*. https://einzelnet.com/ciberseguridad-en-la-educacion/.

Evaluando software.com. (2016). Tendencias TIC relacionadas con la ciberseguridad. *Evaluando Software*. https://www.evaluandosoftware.com/tendencias-tic-relacionadas-la-ciberseguridad/

Fainholc, B. (2007). La relevancia de la Epistemología de la Educación a distancia para entornos de educación superior virtuales con TICs. *www.academia.edu*. https://www.academia.edu/4127281/La_relevancia_de_la_Epistemologia_de_la_Educacion_a_distancia_para_entornos_de_educacion_superior_virtuales_con_TICs

Fundéu RAE. (2014, octubre 7). *Seguridad en internet, claves de redacción*. https://www.fundeu.es/recomendacion/seguridad-en-internet-claves-de-redaccion/

Gridasova, A. (2019, January 25). *Los trucos psicológicos del spear phishing*. Kaspersky.com; Kaspersky. https://latam.kaspersky.com/blog/phishing-psychology/13978/

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: its effects on psychological well-being, public confidence, and political attitudes. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyw018

Grupo proyecta. (2019, diciembre 18). *Tres principios básicos de la ciberseguridad | CE Consulting*. Blog CE Consulting. https://blog.ceconsulting.es/los-principios-basicos-de-la-ciberseguridad/

Hernández-Sampieri R., & Mendoza C. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

Hong, J. (2016). Toward a safe and secure internet of things. *New America.* http://www.jstor.org/stable/resrep10509

Intermulticulturalidad. (2018, October 28). *EDUCACIÓN A DISTANCIA: MODELOS PEDAGÓGICOS Y TEORÍAS DEL APRENDIZAJE*. Educación a Distancia. https://intermulticulturalidadwordpress.wordpress.com/2018/10/28/educacion-a-distancia-modelos-pedagogicos-y-teorias-del-aprendizaje/

Iberia, S. (2020, julio 08). *Enseñanza a distancia: Los cinco principales problemas de ciberseguridad para la educación*. Sophos. https://news.sophos.com/es-es/2020/07/08/ensenanza-a-distancia-los-cinco-principales-problemas-de-ciberseguridad-para-la-educacion/

Irons, A. (1970, January 1). Delivering cybersecurity education effectively. *IGI Global.* https://www.igi-global.com/chapter/delivering-cybersecurity-education-effectively/225922.

Jesús, M., & Robledo, C. (2020). Proteger la información ha sido una constante a lo largo de la Historia. In *#64 Revista Española de Control Externo* | (pp. 90–103).

https://www.tcu.es/repositorio/96871f69-3af7-431c-b324-387eee6f0b7e/R64_ART%205%20MJ%20CASADO.pdf

Kaspersky Lab. (2020, mayo 26). ¿Qué es la ciberseguridad? *Latam.Kaspersky.Com.* https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?CJ_CID=2805960&CJ_PID=3637436&CJ_CID_NAME=Symbaloo.com&utm_source=CJ&utm_medium=affiliate&CJEVENT=cfe8016d0e6b11eb823a00be0a24060d

Katz, F. (2018). Breadth vs. depth: Best practices teaching cybersecurity in a small public university sharing models. *The Cyber Defense Review, 3*(2), 65-72. Retrieved October 14, 2020, from https://www.jstor.org/stable/26491224

Los 5 principales escáneres de vulnerabilidades para patrullar las redes. (2021). Ciberseguridad. https://ciberseguridad.com/herramientas/software/escaneres-vulnerabilidades/#Definir_el_alcance

Lagua, T., & Paul, B. (2018). Plan informático 2018- 2022, basado en la norma ISO/IEC 27032:2012 para mejorar la ciberseguridad de los recursos tecnológicos de información y comunicación (TIC´S) en la unidad educativa Alfredo Pareja Diezcanseco de la ciudad de Santo Domingo. *Dspace.Uniandes.Edu.Ec*. http://dspace.uniandes.edu.ec/handle/123456789/8990

Marchese, J. (2020). E*lementary and secondary school children: Vulnerabilities of online learning (*Publication No. 28092615). [Doctoral dissertation, Marchese, Jolan Utica College]. ProQuest Dissertations & Theses Global. (2448614148). https://search.proquest.com/docview/2448614148?accountid=41558

Molina, Y., Luis, & Orozco, G. (2020). *Vulnerabilidades de los Sistemas de Información: una revisión Information System Vulnerabilities: A review*. https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Morán Blanco, S. (2017). La ciberseguridad y el uso de las tecnologías de la información y la comunicación (TIC) por el terrorismo. *Revista Española De Derecho Internacional, 69*(2), 195-222. http://www.jstor.org/stable/26187882

Moreno, J. J. (2020). *A qualitative study of cybersecurity specialists' concerns in virtual reality in the United States of America* (Publication No. 27993858). [Doctoral dissertation, Colorado Technical University]. ProQuest Dissertations & Theses Global. https://search.proquest.com/docview/2416226402?accountid=41558

Orbegoso, P. (n.d.). *Teoría cognitiva y sus representantes*. https://tauniversity.org/sites/default/files/teoria_cognitiva_y_sus_representantes.pdf

Ortega-Carbajal, M. F., Hernández-Mosqueda, J. S., & Tobón-Tobón, S. (2015). Análisis documental de la gestión del conocimiento mediante la cartografía conceptual. *Ra Ximhai*, *11*(4), 141–160. https://www.redalyc.org/comocitar.oa?id=46142596009

Press, G. (2019 a, December 3). *141* Cybersecurity predictions for 2020. *Forbes*. https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/#1b1a8e1c1bc5

Press, G. (2019b, December 12). 42 more cybersecurity predictions for 2020. *Forbes.* https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/#559b80884a56

Proyecto Lawi (2018*). Plataforma digital de derecho, ciencias sociales y humanidades.* https://leyderecho.org/ciberseguridad/

Requena, M. (2020). *La cartografía conceptual: fundamentos, características y aportes. en análisis y reflexiones en torno a la metodología de la investigación y el desarrollo humano*. México. https://www.researchgate.net/publication/344306033_La_cartografia_conceptual_Fundamentos_y_caracteristicas

Roush, A. (2020, October 4). October is cybersecurity awareness month*. TechNotes Blog*. https://blog.tcea.org/cybersecurity-awareness-month/?utm_source=TCEA+Emails.

Salazar-Gómez, E., & Tobón, S. (2018). Análisis documental del proceso de formación docente acorde con la sociedad del conocimiento. *Revista Espacios*, *39*(53). https://revistaespacios.com/cited2017/cited2017-17.html

Salesforce. (2017). *What is Software as a Service (SaaS)?* https://www.salesforce.com/mx/saas/

Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organizational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*, *20*(4), 581–597. https://doi.org/10.1108/jic-03-2019-0041

Sánchez-Domínguez, J. P., Raymundo, L. M., & Osorio, M. cristel P. (2020, julio 2). *Estudio comparativo del Ciberacoso en escolares de secundaria y media superior*. https://www.ctes.org.mx/index.php/ctes/article/view/715.

Sophos. (May 2020). *Secure Remote Learning in Education.* https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-secure-remote-learning-education-wp.pdf.

Tobón, S. & Guzmán, C. & Hernández Mosqueda, S. & Cardona, S. (2015). Sociedad del conocimiento: Estudio documental desde una perspectiva humanista y compleja. *Paradigma.* 36. 7-36.

Tobón, S. (2012). El aprendizaje basado en *mapas. Instituto CIFE.* https://issuu.com/cife/docs/e-book_el_aprendizaje_basado_en_map

Ulloa Brenes, G. (2021). Reflexiones en torno a la evolución histórica del concepto de la educación a distancia. *Innovaciones Educativas*, *23*(34), 42–51. https://doi.org/10.22458/ie.v23i34.3364

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

Universidad Estatal a Distancia (UNED). (2017). *Fundamentos*. Multimedia.uned.ac.cr. https://multimedia.uned.ac.cr/pem/epistemologia_ed/paginas/concepto2.html

welivesecurity. (2015, June 16). *¿Ciberseguridad o seguridad de la información? Aclarando la diferencia*. WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Williams, T. D. (2020). Epistemological Questions for Cybersecurity. *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. https://www.academia.edu/44171826/Epistemological_Questions_for_Cybersecurity