Caracterización de Ciberataques en Universidades: Análisis de una muestra por conglomerados de Cobertura Mediática

Characterization of Cyberattacks on Universities: Analysis of a Clustered Sample of Media Coverage

http://doi.org/10.17981/culteducsoc.15.2.2024.5393

Recibido: octubre 8 de 2023 Aceptado: agosto 23 de 2024 Publicado: octubre 25 de 2024

Aura M. Torres-Reyes
Grupo de Investigación OPIICS, Universidad de Zaragoza (España)
auramtorresreyes@gmail.com

Para citar este artículo:
Torres-Reyes, A.-M. (2024). Caracterización de Ciberataques en Universidades: Análisis de una muestra por conglomerados de Cobertura Mediática. *Cultura, Educación y Sociedad, 15*(2), e34465393. http://doi.org/10.17981/culteducsoc.15.2.2024.5393

Resumen

Introducción: La digitalización progresiva de las instituciones educativas ha experimentado un notable incremento en los últimos años, este avance está acompañado de nuevos desafíos, entre ellos la ciberseguridad, dado que a medida que las instituciones aumentan el uso y la oferta de servicios en línea también aumentan la exposición de sus datos e información a situaciones relacionadas con cibercrimen. **Objetivo:** Caracterizar los ciberataques a universidades mediante una revisión sistemática de la cobertura mediática encontrada mediante una muestra por conglomerados en diferentes combinaciones de búsqueda online. **Metodología:** Este estudio de enfoque mixto llevó a cabo una revisión sistemática de diferentes combinaciones de recuperación online, mediante el Método de siete pasos. El análisis incluyo técnicas cualitativas y cuantitativas. El muestreo intencional por conglomerados, generó 560 resultados directos y 8 resultados por rastreo. La muestra final a partir del criterios del estudio se estableció en 66 coberturas mediáticas de ciberataques realizados a instituciones universitarias. **Resultados:** Se caracterizaron 45 ciberataques a instituciones educativas dentro del periodo 2008-2023, permitiendo establecer una caracterización general a partir de 11 categorías de análisis, estableciendo correlaciones moderadas entre el autor y el tipo de información expuesta durante el ciberataque. **Conclusiones:** Los ciberataques de la muestra, se caracterizan por ser de autoría desconocida, intencionales, concentrándose en países europeos. Según el tipo de ataque suelen ser por Ransomware o Filtración de datos, e integrar otros a modo de puertas traseras. Su impacto incluye, entre otros: pérdidas económicas, exposición de datos, el daño en el prestigio institucional y cierre de la institución.

Palabras clave: Educación superior; Tecnología educativa; Tecnologías de la Información y Comunicación, Seguridad Informática

Abstract

Introduction: The progressive digitalization of educational institutions has experienced a remarkable increase in recent years, this progress is accompanied by new challenges, among them cybersecurity, given that as institutions increase the use and offer of online services, they also increase the exposure of their data and information to situations related to cybercrime. **Objective:** To characterize cyberattacks on universities through a systematic review of media coverage found through a cluster sample in different combinations of online search. **Methodology:** This mixed-approach study conducted a systematic review of different combinations of online retrieval, using the Seven-Step Method. The analysis included qualitative and quantitative techniques. Purposive cluster sampling generated 560 direct results and 8 crawl results. The final sample from the study criteria was established in 66 media coverage of cyber-attacks on university institutions. **Results:** 45 cyberattacks on educational institutions within the period 2008-2023 were characterized, allowing to establish a general characterization from 11 categories of analysis, establishing moderate correlations between the author and the type of information exposed during the cyberattack. **Conclusions:** The cyberattacks in the sample, are characterized by being of unknown authorship, intentional, concentrating in European countries. Depending on the type of attack, they are usually Ransomware or Data Leakage, and integrate others by way of backdoors. Their impact includes, among others: economic losses, data exposure, damage to institutional prestige and closure of the institution.

Keywords: Higher Education; Educational Technology, Information and Communication Technologies, Computer Security

INTRODUCCIÓN

Si bien la digitalización de las instituciones educativas ha sido un proceso lento y paralelo a lo largo del tiempo con diversas experiencias (Ugur, 2020; Grosseck, Malita y Bunnoiu, 2020), la situación generada por las medidas tomadas a propósito de la declaración de pandemia, generaron una serie de restricciones que obligaron a todas las instituciones educativas a nivel mundial a realizar procesos digitales (Funk, 2021; UNESCO, 2023), para generar procesos educativos alternativos (Ali, 2020; Lei y Medwell, 2020; Morgan, 2020)

Con ello, las plataformas de mensajería (Azfal y Abdullah, 2020), redes sociales (Anggoro y Rueangrong, 2020; Insorio y Olivarez, 2021), videoconferencia (Al-Samarraie, 2019), además de las plataformas educativas comenzaron a implantarse de forma masiva, sin haber tenido tiempo para realizar un tránsito adecuado en la mayoría de los casos (Le, 2022; Bojovic, 2020, Yusuf, 2020), tal como lo manifestaba un análisis en México sobre la ausencia de políticas de ciberseguridad en instituciones educativas (Chávez, 2020).

Esto repercutió no solo en la profundización de las brechas digitales (Anaya, 2021; Fernández et alt., 2022; Kuric y Sanmartín, 2021) sino también en la exposición y vulnerabilidad de las comunidades educativas en cuanto a su información y datos personales digitales, introduciendo de pleno las problemáticas relacionadas con la ciberseguridad en los sistemas educativos (Harrel et al., 2018; Kaspersky, 2020)

Estas problemáticas podrían resumirse de forma general en cinco temáticas claves: la computación en la nube, la computación móvil, la convergencia tecnológica, las redes sociales y la asimetría de los ciber-conflictos (Cano, 2020:82), en donde cualquier vulnerabilidad o riesgo da lugar a la cibercriminalidad.

Aunque de forma específica en instituciones educativas es un tema poco abordado en publicaciones, tal como lo evidencia la revisión sistemática realizada por Ulven y Wangen (2021), que hallaron un total de 18 documentos académicos que abordaban el tema de riesgos de ciberseguridad en educación superior, de los cuales sólo 9 se correspondían con artículos de revistas especializadas y sólo el estudio de Kwaa-Aido y Agbeko (2018) es del último lustro. Esto puede deberse a situaciones que relacionan seguridad institucional y prestigio (Bjorge y Wangen, 2021), así como al proceso de secreto sumarial que acompañan los procesos judiciales y limitan la información que se pone en circulación (González, 2010)

En este contexto, el enfoque se centró en la problemática de los ciberataques dirigidos a universidades, utilizando información disponible en la cobertura mediática. Siendo el objetivo principal: caracterizar los ciberataques experimentados por las universidades a través de una revisión sistemática de artículos publicados en los medios de comunicación (Diarios de difusión nacional, portales universitarios, medios especializados). Este enfoque permitió contribuir con nueva información, que amplió el conocimiento sobre la situación de ciberseguridad dentro del entorno universitario y visibilizó la importancia de su abordaje en escenarios educativos.

Revisión de la literatura

Se podría asegurar que la cibercriminalidad es tal vez el lado de la misma moneda que se inicia con la digitalización, a medida que se aumenta la exposición de la información y los datos, también se aumenta la vulnerabilidad y el riesgo de ser víctima de un cibercrimen, y de forma paralela también aparecen las regulaciones que tratan proteger a la ciudadanía, la más significativa de ellas es el Convenio sobre cibercriminalidad firmado en Budapest en 2001 ratificado por varios países entre ellos España en 2014 (BOE-A-2010-14221, 2014). Este convenio establece cuatro grupos de ciberdelitos: a) Contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, b) Delitos informáticos, c) Delitos relacionados con el contenido y d) Delitos relacionados con infracciones de la propiedad intelectual.

Estos delitos son articulados a las normativas nacionales, por ejemplo, las vinculadas a dar garantía al derecho a la intimidad y la privacidad, las relacionadas con la protección de datos e información personal, la propiedad intelectual. Que junto a otras permiten regular procesos de ataque y delito contra la intimidad, derechos de autor, falsedad, fraude informático, acceso a información, entre otros. Al respecto, cada país ha desarrollado regulaciones específicas, en el caso español se encuentra el plan de contingencia y evaluación del alcance previsto en el Esquema Nacional de Seguridad (Real Decreto 3/2010) y los protocolos de actuación y notificación de la Agencia Española de Protección de Datos en concordancia con el Reglamento General de Protección de Datos (RGPD, 2016), a fin de limitar el riesgo derivado del ciberataque.

A pesar de ello, existe una economía paralela que se deriva del ejercicio de la cibercriminalidad, algunos de ellos se han establecido como un servicio (CaaS- Cybercrimen as a Service), que ya se proyecta y puede llegar a costar 10.5 trillones de dólares anuales para 2025 (Morgan, 2020). Lo cual no es desproporcionado si se observa el incremento sostenido en el tiempo de la cibercriminalidad, para 2021 en España se registraron 305.477 casos conocidos, siendo el 87,4% correspondientes con Fraude informático (López et alt., 2022, p.43), sobre la respuesta policial se encuentra que en general se logró el esclarecimiento de 46.141 casos y hubo 13.801 Detenciones/Investigaciones (López et alt., 2022:45), que en conjunto implicarían el esclarecimiento de menos de la sexta parte de los casos reportados.

Sin embargo, esta tendencia es global, tal como lo menciona el informe de la IOCTA (Internet Organised Crime Threat Assessment), que menciona como hechos recientes que el aumento del Ransomware está relacionado con: teletrabajo, incremento del comercio online, actividades intrusivas, acceso de la población infantil provocado por la covid-19 y el mercado floreciente de la venta y comercio de datos privados (Internet Organised Crime Threat Assessment-IOCTA Europol, 2021). Estás situaciones continúan presentes y en aumento debido en parte, a los usos indebidos de tecnologías como Inteligencia Artificial (IA) que van saliendo a flote de forma paralela a nuevas modalidades de ciberdelincuencia.

En general, una vulnerabilidad es explotada por los cibercriminales a partir de ataques, tanto activos como pasivos, tal como lo mencionan Romero y otros (2018), los ataques pasivos están orientados a obtener información a través de Monitorización de tráfico, OSINT (contraseñas o fuentes abiertas) e ingeniería social; y los ataques activos son acciones directas para penetrar la infraestructura, que puede incluir sabotaje, robo de información, malware, secuestro de equipo (Romero et alt. 2018, p. 37), en donde las redes sociales juegan un papel importante en las brechas de seguridad.

Si bien los ataques van evolucionando con el tiempo, la revisión de literatura de Cando y Medina (2021) nos da una idea de los ciberataques más comunes, entre ellos se encuentran: Ransomware, Ataques a dispositivos loT, Phishing e ingeniería social, Ataque a redes LAN inalámbricas, Ataque de denegación de servicio (DOS o DDOS), Suplantación de Identidad y Sybil, y otros Malware (Cando y Medina, 2021, p.29), aunque en la actualidad la convergencia de tecnologías puede suscitar una gran diversidad.

Algunos ciberataques corresponden con: virus tipo thingbots que atacan al internet de las cosas y por ende a las interacciones con la educación (Rueda et alt. 2017), ciberataques a los asistentes virtuales con el tipo ataque delfín (Zhang et alt., 2017), filtraciones de datos exponenciales a través de ataques a Inteligencias artificiales (Terán, 2023) e incluso a antivirus que expusieron a organizaciones gubernamentales como la NASA, el FBI, entre otras (Hoppenstedt, 2023), lo cual hace de cualquier enlace o correo un potencial desencadenante de un ciberataque.

De esta forma, a medida que aumenta la digitalización de los procesos, los datos incrementan su valor de mercado, dando lugar a la aparición de nuevos modelos económicos en las economías legales. Entre estos modelos destacan el Big Data, Gig data, Human Data, la economía de la atención, Open Data, la economía del like y el Pop-up, entre otros. Estas tendencias se suman al crecimiento de la economía en el sector tecnológico, que soporta los servicios fundamentales para la digitalización.

Aunque de otro lado, también emergen nuevos modelos económicos desde el cibercrimen que se suman a las conocidas redes de piratería, tales como: el CaaS (Cibercrimen como un servicio- Cybercrimen as a Service) (Akyazi, 2021), el franquiciado (licenciamiento) de malware y “programa de afiliados” (Erard, 2021), la implantación de chips espías (Sánchez, 2018), malware que secuestra equipos/información a cambio de un “rescate” (cuyo creador fue curiosamente un biólogo investigador del VIH) (Rus, 2021). De esta forma el lucro y el ciberataque forman un binomio potencialmente peligroso.

Este último da lugar a bandas de ransomware (LocBit, Hive, Black Basta, Royal), algunas de ellas especializadas en el sector educativo como Vice Society (Constantin, 2023), también se observan grupos dedicados al hacking delictivo como The Equation Group, Shadow Brokers, Bureau 121, Fancy Bear, DarkSide, La Unidad 8200, Unidad 61398 y Machete (Regan, 2021) o al pshinsing como Oktapus, que a su vez se conectan con otras cadenas del mercado ilegal teniendo portales de venta en la Dark web, en donde cada dato adquiere un valor económico.

Con respecto a quienes son los ciberdelincuentes, si bien se encuentran diferentes estudios a lo largo del tiempo que intentan ofrecer un perfil (Shaw, 2006; Fernández, 2019; Cámara, 2020), la tendencia del cibercrimen como un CaaS, podría influir en la distribución de roles al interior de los equipos de cibercrimen dificultando el establecimiento de un perfil único. De esta forma el objetivo del "cibercrimen" agrupa los diferentes roles para su comisión, y por tanto el estudio del móvil causante comienza a cobrar importancia en el ciberdelito como lo menciona González y Campoy (2018) en relación a la función de los precipitantes situacionales en su estudio del ciberacoso.

Dentro de las manifestaciones de delitos mediados por tecnología que son frecuentes en el entorno educativo, tales como: el ciberacoso, el plagio, la falsificación de documentos, la piratería, el hackeo a sistemas en busca de información privilegiada como exámenes o alteración de registros como por ejemplo las notas. También se han identificado casos de falsificación de expedientes o titulaciones, así como suplantación de identidad para presentar exámenes, entre otras situaciones.

Aunque muchas de estas situaciones, son prolongaciones a problemáticas ya existentes en la presencialidad, otras son propias de los entornos digitales trascendiendo a demandas nacionales o institucionales suscitando debates alrededor de la protección de datos personales y recopilación de información personal en niños-as como lo han reportado titulares de medios en relación a las prácticas de empresas tecnológicas por ejemplo YouTube y Google (Gibbs, 2018; Sánchez, 2020).

Aun así, es innegable el aporte que las TIC pueden hacer en combinación con la experticia docente y la organización de la comunidad educativa, especialmente en cuanto a la atención de la diversidad (Ochoa y otros, 2019), procesos de inclusión (Cabero y Valencia, 2019) y adaptación a metodologías activas (Daher et alt., 2022), entre otras, que han permitido mejorar la atención y los procesos que se realizan al interior de las instituciones educativas.

En este camino emergen dos posiciones que comienzan a polarizarse, la tecno-optimista que puede observarse en organismos multilaterales como UNESCO que fomentan la inclusión de todo avance incluyendo ChatGPT generando cursos y guías específicas para la educación superior (Bastidas, 2023), y la tecno-pesimista que ha comenzado a prohibir el uso de tecnología, como Italia que han prohibió Chat GPT o Suecia que luego de los resultados del informe PIRLS, con sus 544 puntos aún por encima de la media de la OCDE (533) ha decidido terminar con 15 años de impulso a las pantallas dentro del aula y volver a los libros de texto (Farreras, 2023).

Este camino tecno-pesimista, ha tomado un curso especial en instituciones educativas de nivel básico (Juste, 2024), obteniendo una mejora en habilidades sociales, disminución de acoso escolar, entre otras situaciones que van ganando cada vez más instituciones restrictivas de los dispositivos en aulas, especialmente de los móviles.

Ciberseguridad en educación superior

Específicamente en cuanto a Ciberseguridad en Educación superior la revisión de Bongiovanni (2019) establece la necesidad de ampliar la investigación sobre de seguridad de la información en educación superior, dado que sus flujos de información generan diferentes brechas de seguridad.

Estas brechas son comunes a diferentes organizaciones, por ello la educación como proceso, es un componente importante en la Ciberseguridad (Cayón y García, 2014), dando lugar a un incremento en los programas académicos que abordan la temática de Ciberseguridad, con sus respectivos desafíos (Payne et alt., 2021), entre ellos la necesidad de mantener un nivel prestigio frente a los ciberataques de los que son víctimas.

Aunque en el día a día dentro de la Universidad puede percibirse como una tarea del departamento técnico tal como lo encontraron, Bjorge y Wangen, quienes realizaron una revisión sistemática de la literatura existente al respecto de la ciberseguridad en Educación superior concluyendo la falta de estudios, como lo mencionó Bongiovanni (2019), y adicionalmente establecieron tres grandes bloques de vulnerabilidades comunes: 1) las administrativas y culturales, 2) las vulnerabilidades técnicas, 3) la seguridad física (2021); mencionando la falta de datos de los estudios que podrían ser explicados por la probabilidad de perdida de prestigio de la institución al dar a conocer dicha información (Bjorge y Wangen, 2021), que bien podrían ser fundamentadas en el análisis de los comentarios de estudiantes posterior a un ciberataque, que llegan a cuestionar la credibilidad del programa, especialmente en temáticas de ciberseguridad.

No obstante, el estudio de Microsoft Security Intelligence de 2018 muestra que el sector de la educación fue más afectado recibiendo el 80,25% de los ataques (Microsoft Security Intelligence, 2018), y durante pandemia el estudio de BlueVoyant mencionada que los ataques de Ransomware a universidades se había duplicado (BlueVoyant, 2021), una situación esperable luego del incremento no planeado en el uso de herramientas digitales.

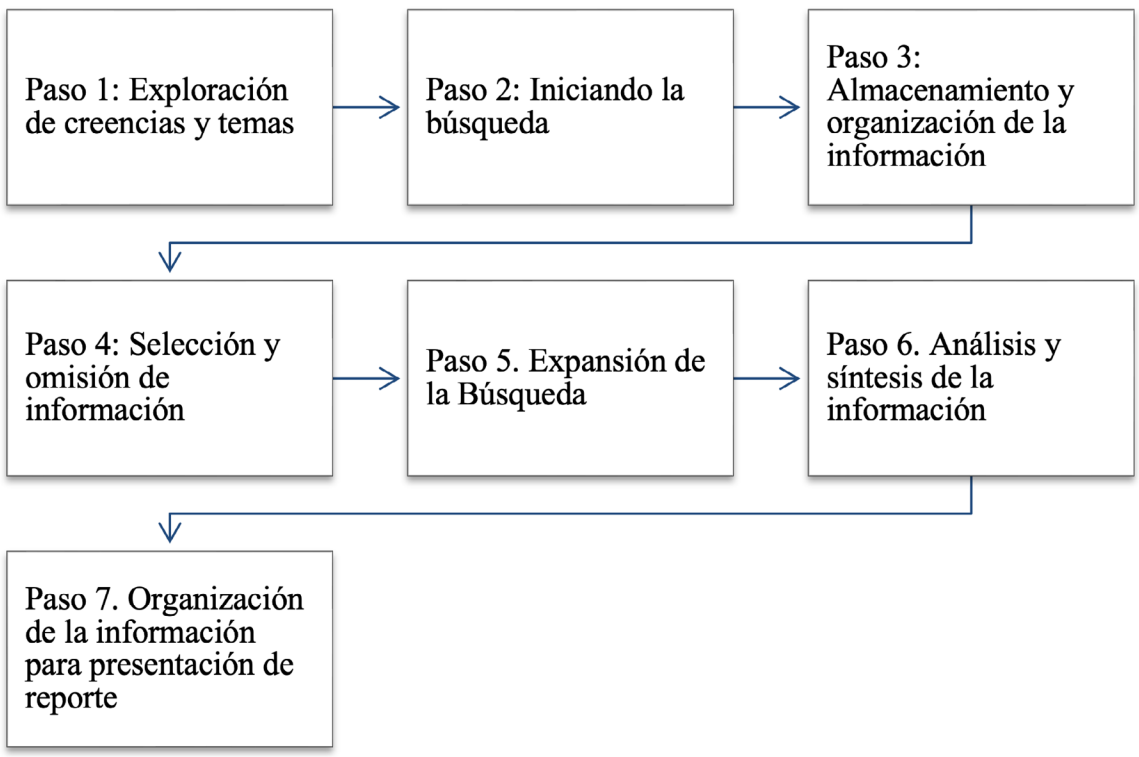
Al respecto, en el Reino Unido durante 2020-2021 se encontraron picos de ataques de ransomware en el sector educativo que en tendencias generales atacaban a través del acceso remoto (protocolo de escritorio remoto y redes privadas virtuales) explotando vulnerabilidades como: contraseñas débiles, falta de autenticación multifactor y ausencia de parches en software (Nacional Cyber Security centre, 2023), algo que sigue siendo un común denominador de los usuarios-as digitales.

Aunque de forma paralela a esta explosión de ataques, se han ido desarrollando diferentes herramientas de diagnóstico de seguridad de la red, algunos testeados específicamente en Universidades (Zheng et alt., 2021), en donde como lo expresa Hazay en la presentación de su aplicación “nos enfrentamos al reto de compartir datos mientras se aseguran secretos” (Hazay, 2017), más aún cuando se realizan esfuerzos de integración, alianzas e internacionalización institucional.

METODOLOGÍA

Para alcanzar el objetivo, se realizó un estudio de enfoque mixto llevó a cabo una revisión sistemática mediante el método de siete pasos propuesto por Onwuegbuzie y Frels (2016, p. 58), a fin de analizar la cobertura mediática de ciberataques dirigidos a universidades. Este método se ilustra en la figura 1, y la selección de la muestra de análisis siguió el flujo recomendado por la declaración PRISMA, representado en la figura 2. Adicionalmente, se llevó a cabo un análisis correlacional entre las variables categóricas resultantes del estudio a fin de profundizar sobre las relaciones entre las categorías obtenidas a partir del estudio.

Figura 1. Método de siete pasos.



Fuente: Elaboración propia a partir de la propuesta de Onwuegbuzie y Frels (2016, p.58).

Muestra

Se realizó un muestreo a partir de información online debido a la escasa publicación académica sobre ciberataques a instituciones de educación superior, constituyendo a los medios de comunicación una de las pocas fuentes que registran estos ciberataques tanto en el ámbito nacional como internacional, que debido a sus repositorios online, hacen de los navegadores/motores de búsqueda un mecanismo accesible de recuperación. Otros estudios que han analizado cobertura mediática para indagar fenómenos poco estudiados con enfoque mixto en la literatura académica son por ejemplo: el estudio sobre corrupción en España y su impacto en la opinión pública (Palau y Davesa, 2013) que tomó como referencia diarios o el trabajo de Malianos (2023) sobre la Agenda medioambiental que se basó en la

monitorización de noticieros de Nicaragua utilizando técnicas cuantitativas de tabulación de frecuencias.

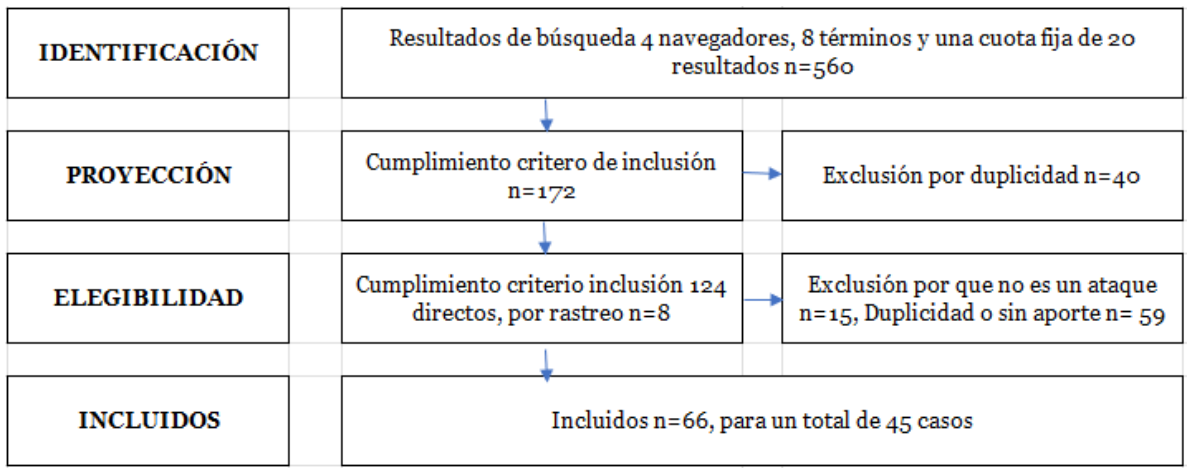
En el caso del estudio, a fin de evitar los sesgos de los navegadores y motores de búsqueda se realizó un muestreo de conglomerado de cuota fija obteniendo 560 resultados directos y 8 resultados indirectos por rastreo de muestra inicial. La muestra se tomó en el periodo del 19-30 de junio de 2023 y estuvo constituida por una cuota fija de 20 primeros resultados online en español, que se recopilaron a través de conglomerados formados por una combinación dentro de: 1) cada término de búsqueda (Ciberseguridad, Hacking, Phishing, Ransomware, Vulnerabilidad, Filtración de datos y Ciberataque), 2) mezcla de Navegador/Motor de búsqueda (Chrome: Google; 2. Microsoft Edge: Bing; 3. Opera: Google; 4. Brave: Brave), y 3) el término Universidad.

La recuperación se realizó en cada combinación de navegador/motor de búsqueda, así: "termino de búsqueda" "Universidad" se omitieron operadores boléanos (And, Or, Not), reemplazándolos por comillas directas en los términos, a fin de obligar al navegador/motor a generar resultados específicos. Este operador garantizó que la información se obtuviera en idioma español y generará resultados específicos, acotados por el límite de cuota en cada buscador y filtrados por los siguientes criterios de inclusión y exclusión:

1. **Fuente:** Criterio proveniente de medio de comunicación (El País, La Vanguardia, El Tiempo, BBC, entre otros.), Sitio web institucional (portal online de la universidad), Sitio web especializado (Computer Hoy, Business Insider, We live security, entre otros), no se tuvieron en cuenta blogs personales, redes sociales, foros.
2. **Tipo de documento:** Artículo, se excluyeron: cursos, información promocional, comentarios en redes sociales o similares.
3. **Contenido:** Contenido original (no duplicado en otro medio), específico (aborda un ciberataque a una Universidad), aporta información adicional del ciberataque a una universidad. Se excluyeron artículos no relacionados con ciberataques a una universidad o aquellos duplicados que no aportaban información adicional.
4. **Rastreo:** Se incluyeron 8 artículos que eran mencionados en artículos que cumplieron los criterios de inclusión, pero que no habían sido listados por el buscador, los cuales cumplían con los criterios de inclusión y exclusión.

En total, se obtuvieron 560 resultados de búsqueda, resultado de multiplicar 7 términos de búsqueda por 4 navegadores/buscadores por 20 resultados de búsqueda directa y 8 resultados por rastreo. Posteriormente, se aplicó el protocolo de la declaración PRISMA (Matthew et al., 2021), como se muestra en la figura 2, lo que condujo a una muestra final de sesenta y seis registros mediáticos (n=66) de ciberataques en instituciones universitarias que cubrían 45 casos.

Figura 2. Diagrama de Flujo PRISMA.



Fuente: Elaboración propia

Selección de términos de búsqueda

A fin de garantizar la calidad de los datos del estudio se tuvieron en cuenta tres atributos: Transparencia, Persistencia y Obsolescencia, tal como lo sugiere el libro Blanco de Data (IAB, 2019), en cuanto a la transparencia se incluyó dentro del criterio de inclusión la fuente. Para garantizar la Persistencia se realizó una exploración de términos asociados a ciberataques a través de IA (ChatGPT) validados según su contenido a través de triangulación de información proveniente del INCIBE (Instituto Nacional de Ciberseguridad en España) y en cuanto a Obsolescencia se tuvieron en cuenta primeras posiciones de listado en motores y buscadores con mayor representatividad dentro del mercado.

Se seleccionó para realizar la exploración inicial IA debido a su capacidad para realizar análisis de grandes volúmenes de datos en menos tiempo a través del modelo de inteligencia artificial generativa Chat GPT3 acorde con las recomendaciones de Unesco de la inclusión de Inteligencia Artificial en Educación superior (Unesco, 2023), bajo el prompt: "Cómo experto en ciberseguridad genera un listado de ciberataques que suelen estar asociados a noticias sobre seguridad de información o protección de datos en coberturas mediáticas de ciberataques a universidades". Los términos arrojados fueron: Ciberseguridad, Hacking, Phishing, Ransomware, Vulnerabilidad, filtración de datos y Ciberataque.

No se realizaron búsquedas en otros modelos de IA debido a que al momento de la búsqueda (junio 2023), no había otra IA que tuviese el respaldo de un organismo multilateral, y ya se habían encontrado estudios que demostraban algunas dificultades como el sesgo o la falta de actualización de estos modelos.

Técnicas de validación de términos de búsqueda

Para la validación de términos de búsqueda se realizó una validación de contenido de los términos arrojados en la revisión realizada mediante ChatGPT 3, se trianguló la información obtenida a través de los datos de expertos en ciberseguridad

recopilados en la Guía de ciberdelitos (INCIBE, 2020), este procedimiento permitió establecer los siete términos de búsqueda del estudio: Ciberseguridad, Hacking, Phishing, Ransomware, Vulnerabilidad, Filtración de datos y Ciberataque.

Representatividad de los Navegadores/buscadores utilizados

Las cuatro combinaciones de navegador/buscador del estudio se obtuvieron teniendo en cuenta las estadísticas de penetración de mercado de los navegadores y motores de búsqueda más utilizados, a fin de dar representatividad a los resultados de búsqueda (W3Counter: Global Web Stats, 2023). Se eligieron aquellas combinaciones con mayor y menor cuota de mercado, así: 1). Chrome: Google; 2). Microsoft Edge: Bing; 3). Opera: Google; 4). Brave: Brave.

Análisis y sistematización de los datos

Para el análisis de datos se utilizaron técnicas cualitativas como la categorización y codificación abierta (Vives y Hamui, 2007), teniendo como criterio general responder a preguntas básicas que responde un texto periodístico: qué, quién, cómo, dónde, cuándo, por qué, qué dijeron (Universidad Nacional de Asunción, 2020), esto permitió establecer las 11 categorías de análisis de la información: 1) Fecha del ciberataque (año, mes, día de la semana y número de día), 2) Autor del ciberataque, 3) País de origen, 4) Tipo de ciberataque, 5) Tipo de información atacada, 6) Sector afectado, 7) Impacto percibido del ciberataque, 8) Momento de detección del ciberataque, 9) Proceso jurídico relacionado, 10) Condena en casos correspondientes y 11) Comunicación de los ataques. La relación entre la cobertura mediática y las categorías de análisis se encuentran resumidas en la Tabla 1.

Tabla 1. Relación entre cobertura mediática y Categorías de análisis.

Pregunta de la noticia	Categoría de análisis del Ciberataque
Cuando	Fecha del ciberataque (año, mes, día de la semana y número de día), Momento de detección del ciberataque
Quién	Autor del ciberataque
Dónde	País de origen
Cómo	Tipo de ciberataque
Por qué	Tipo de información atacada, Sector afectado,
Qué	Impacto percibido del ciberataque,
Qué dijeron	Proceso jurídico relacionado, Condena en casos correspondientes y Comunicación de los ataques.

Fuente: Elaboración propia a partir de datos del estudio

Estas categorías permitieron sistematizar la información que se encontraba en cada una de las coberturas mediáticas incluidas, en aquellos casos en los cuales el texto en sí mismo no respondió a las preguntas, se amplió la búsqueda online del caso tanto en inglés como en español a fin de completar la información que caracterizará el caso. Para validar la categorización se hicieron análisis de frecuencia y durante la discusión de resultados se realizó examen sistemático de los datos obtenidos (Munarriz, 1992).

El análisis cualitativo se amplío a través del análisis cuantitativo, en donde se emplearon técnicas de obtención de variables cuantitativas a partir de variables cualitativas asignando un código numérico (Bologna, 2019). Obtenidas las variables cuantitativas, se realizó una análisis correlacional a través del Coeficiente de correlación de Pearson (Hernández, 2018) para establecer posibles asociaciones entre las variables obtenidas.

Para la sistematización de los resultados, se generaron inicialmente matrices en Excel que permitieron recopilar y filtrar la información obtenida de las búsquedas, para luego conformar una única matriz con los datos finales que contenía los casos y las categorías relacionadas.

La matriz establecida permitió tabular los resultados y establecer frecuencias de resultados, que a su vez fueron la base para generar variables categóricas y realizar el análisis cuantitativo de los datos.

Procedimiento

Se siguió la metodología de los siete pasos, que fue complementada con el protocolo PRISMA. Los pasos de la metodología se describen a continuación:

Paso 1: Exploración de creencias y temas. Durante este paso se exploró sobre la recuperación de información online y los algoritmos de recuperación, por lo cual se establecieron alternativas de navegadores y buscadores, a fin de obtener mayor representatividad de la muestra, seleccionado tanto los que lideran el mercado (Chrome: Google, Microsoft Edge: Bing), como aquellos con menor cuota de mercado (Opera: Google, Brave: Brave).

Para la definición de los términos de búsqueda se tuvo en cuenta la clasificación de ciberdelito del INCIBE, teniendo en cuenta ataques a contraseñas, por ingeniería social, a conexiones y por malware (INCIBE, 2020), y se apoyó la revisión inicial con la IA ChatGPT bajo el prompt mencionado en Selección de términos de búsqueda.

Esto llevó a obtener un listado de términos relacionados con la temática y que se ajustaban a la designación utilizada en medios, obteniendo la Tabla 2.

Tabla 2. Términos asociados a noticias en Ciberseguridad según IA.

Término asociado a noticias según ChatGPT
Ciberseguridad: Se refiere a la protección de sistemas informáticos, redes y datos contra ataques cibernéticos
Brecha de seguridad: Ocurre cuando se produce una vulnerabilidad o exposición de datos confidenciales debido a una falla en las medidas de seguridad.
Hacking: Es el proceso de acceso no autorizado a sistemas o redes informáticas, con el fin de robar, dañar o manipular datos.
Ataque de phishing: Es un intento de engañar a las personas para que revelen información confidencial, como contraseñas o detalles de tarjetas de crédito, haciéndose pasar por una entidad de confianza.
Ransomware: Es un tipo de malware que cifra los archivos de una computadora o sistema, y exige un rescate económico a cambio de su liberación.
Vulnerabilidad: Se refiere a una debilidad o fallo en un sistema que podría ser aprovechado por atacantes para comprometer la seguridad
Fuga de datos: Ocurre cuando la información confidencial se divulga sin autorización, ya sea debido a un error humano, una brecha de seguridad o un ataque.
Protección de datos personales: Se refiere a las medidas y regulaciones destinadas a garantizar la privacidad y la seguridad de la información personal de los individuos.
Reglamento General de Protección de Datos (GDPR): Es una ley de la Unión Europea que establece normas para la protección de datos personales de los ciudadanos de la UE y regula su procesamiento y transferencia.
Seguridad de la información: Se refiere al conjunto de medidas y prácticas que buscan proteger la confidencialidad, integridad y disponibilidad de la información.
Filtración de datos: Se refiere a la exposición de información confidencial sin autorización debido a una acción intencional
Ciberataque: Se refiere a una acción que tiene por objetivo exponer, robar, cambiar o destruir datos sensibles o dañar una red mediante un acceso no autorizado.

Fuente: Elaboración propia a partir de datos de ChatGPT

Paso 2: Iniciando la búsqueda. A partir de la información obtenida en el paso 1, se definió un muestreo intencional por conglomerados de cuota fija de 20 resultados por búsqueda, a través de la recopilación de los resultados obtenidos en cada buscador/navegador acorde con los siguientes términos: a) Ciberseguridad universidad caso, b) Hacking universidad caso, c) Phishing universidad caso, d) Ransomware universidad caso, e) Vulnerabilidad digital universidad caso, f) Filtración de datos universidad caso, g) ciberataque universidad caso.

Paso 3: Almacenamiento y organización de la información. En un libro Excel se recopiló la muestra de cada navegador/buscador y término, para un total de 560 muestras iniciales, y se retomaron adicionalmente 8 por rastreo.

Paso 4: Selección y omisión de información. Este proceso de selección resumido en el diagrama de flujo de PRISMA (figura 2), incluyó dos etapas de selección a través de una codificación por color se aplicaron los criterios de inclusión y exclusión. En la primera etapa se evalúo el título del artículo en correspondencia con el criterio de inclusión n= 172 y criterio de exclusión n=40, para un total de n=132.

En la segunda etapa se revisó el contenidos de los artículos, aplicando de nuevo los criterios del estudio, y a su vez que realizó la identificación de nuevos casos por rastreo a través de artículos; obteniendo acorde con los criterios de inclusión: 124 Resultados directos y 8 Resultados por rastreo. Al aplicar los criterios de exclusión, se eliminaron 15 resultados debido a que no eran un caso de ciberataque, 59 resultados debido a duplicidad o sin aporte. Obteniendo finalmente un Total de 66 resultados, que se constituyeron en 45 casos, a fin de proteger la identidad de las instituciones se anonimizaron, sustituyendo los nombres reales por una numeración de caso.

Paso 5. Expansión de la búsqueda. A partir de cada caso se realizó una búsqueda de información dentro del articulo o adicional que permitiera caracterizar el ciberataque, teniendo en cuenta las siguientes categorías de información: Fecha del ataque (mes, año), autor del ataque, país, tipo de información o datos objetivo del ataque, tipo de ataque, Sector afectado, Impacto del ataque, Detección del ataque, proceso jurídico, Tipo de condena y Afectación a comunicación.

Paso 6. Análisis y síntesis de la información. Para el análisis se utilizó análisis de contenido por categorización y análisis estadístico descriptivo, teniendo en cuenta los 45 casos y las categorías preestablecidas, adicionalmente a través de la técnica de asignación de puntuación se transformaron en variables categóricas las variables cualitativas: Autor, País, Tipo de información, Afectados y tipo de Ciberataque, en donde emergieron códigos nuevos, dando lugar a la figura 5. Una vez se tuvieron las variables categóricas, se procedió a realizar un análisis del coeficiente de correlación y se continuó hacia el séptimo paso.

Paso 7. En este paso se organizó la información para la presentación del reporte.

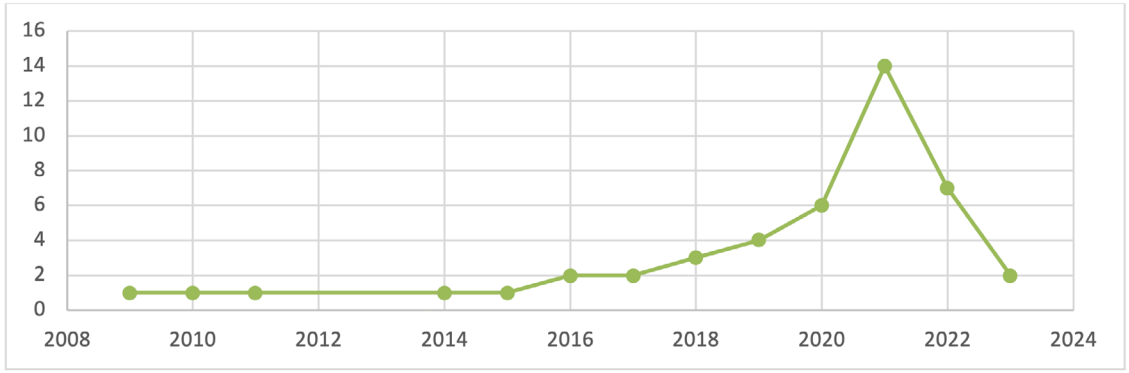
RESULTADOS

Para la presentación de resultados se tuvieron en cuenta las categorías de análisis presentadas en el apartado de metodología, iniciando con la fecha de ciberataque.

Fecha de ciberataque

Los casos del estudio comprenden ciberataques ocurridos entre 2008 y 2023. Acorde con la figura 3, se encuentra una tendencia al alza desde el 2015 hasta alcanzar su pico en 2021. El 2021 concentra el 31% del total de casos del estudio, para volver a decrementar al 4% en lo corrido del 2023 (fecha de corte 30 junio de 2023).

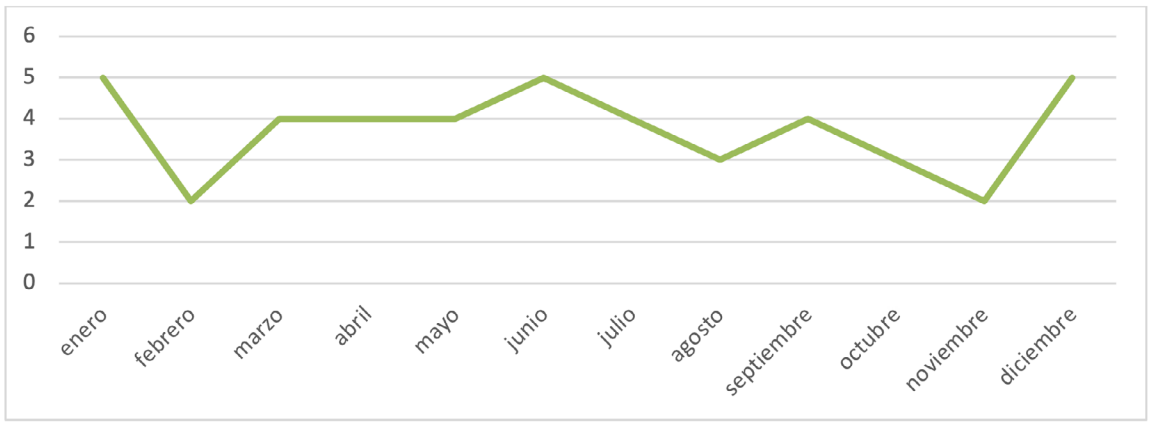
Figura 3. Ciberataques con cobertura mediática periodo 2008-2023



Fuente: Elaborada por el autor.

De otra parte, al observar solo los meses en que se realizan los ciberataques, se observa según la figura 4, que existen tres meses (enero, junio, diciembre) con altos picos concentrando el 33% de los ataques, y los meses con menor número de ciberataques son dos (febrero, noviembre) con el 8% del total de ciberataques.

Figura 4. Ciberataques según mes



Fuente: Elaborada por el autor

Según el día no se encuentran picos, de domingo a miércoles cada día participa en la distribución con un 13% que se incrementa de jueves a sábado a un 16%. Si se tiene en cuenta el número de día, se presentan picos acorde con el número del día así: 1 (13%), 8 (11%) y el 22 (9%).

Autor del ciberataque

Con relación al autor se encuentra que un 67% de los ataques son realizados por desconocidos, en un 13% se logra identificar el país de conexión o se presume por hallazgos de investigación relación con espionaje de países como: Rusía, Norcorea o China, el 11% se atribuye a grupos/bandas cibercriminales entre ellos el ejercito eléctronico de un país y grupos como DoppelPaymer y Conti, el 4% son adjudicados a estudiantes, el 2% se presume que fue un funcionario y en 2% de los casos se identifica a un funcionario.

País

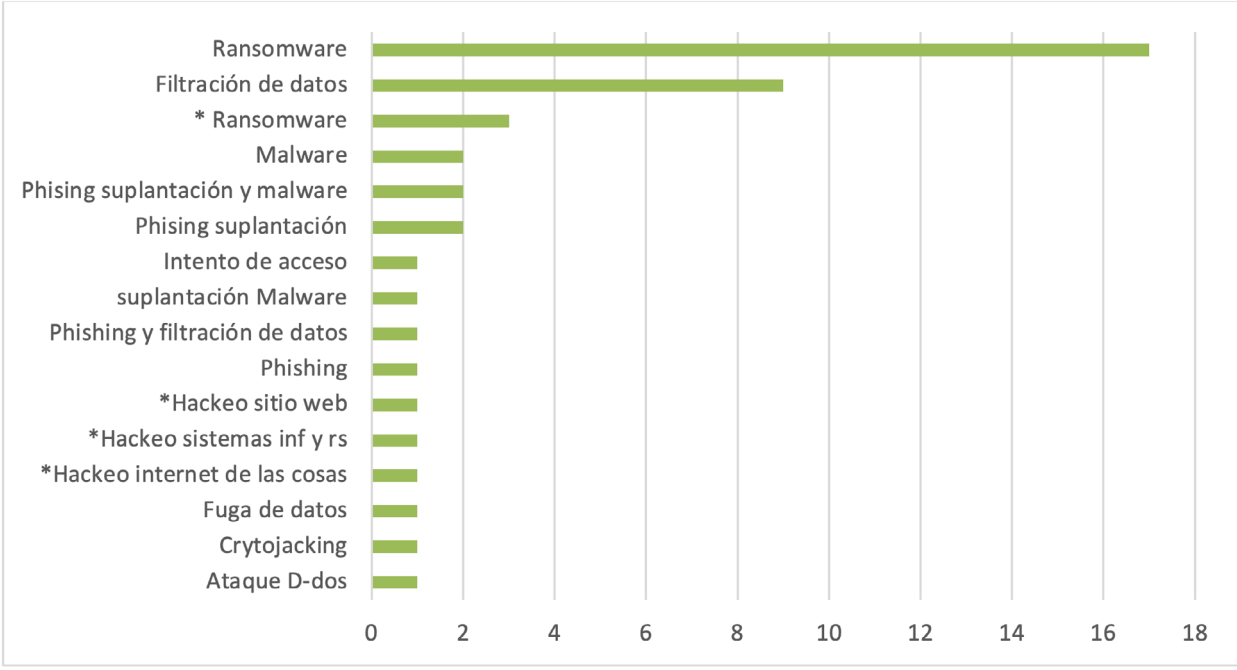
El 41% de los ciberataques se realizaron en España, seguido por el 20% de Estados Unidos, el 15% de Reino unido, el 7% en Colombia, 4% en Canadá y otros países participan con un 2% cada uno (Chile, Israel, Países Bajos, Uruguay y Venezuela). Por continentes la distribución porcentual es: Europa 61%, América 37%, Asia 2%

Tipo de ciberataque

En la figura 5, se observa la clasificación aquellos identificados con asterisco, son clasificaciones inferidas del autor sobre el tipo de ciberataque, las otras son literales de las fuentes consultadas. De esta forma, se encuentra que el ransomware suma un 45% del total de los casos, aunque en los artículos solo se nombra como tal un 38% y se evita dar información sobre el 7%, que infiere el autor es ransomware por la similitud del ataque con otros ciberataques denominados como ransomware.

El ransomware es seguido por la Filtración de datos del 20% y el Phishing 12% (sólo o acompañado de filtración de datos, suplantación, malware), otros ciberataques como Suplantación, Fuga de datos y Malware poseen menor cobertura mediática. Se encuentra de forma general que un ataque de suplantación puede conllevar Malware o Phishing, y a su vez el Phishing puede generar una suplantación para lograr ampliar el impacto del Phishing, o incluir malware, y a su vez el malware puede desencadenar una filtración de datos, ransomware, cryptohacking o alteración de la información (notas). Por tanto, existe una interacción entre los ciberataques, aunque cada uno puede darse por separado.

Figura 5. Tipos de Ciberataques según frecuencia en cobertura mediática



Fuente: Elaborada por el autor

Tipo de información que es atacada

El 44% de los ciberataques tienen como objetivo los sistemas de información de la Universidad, seguidos por el 24% que se dirigen hacia información y datos personales de miembros de la comunidad educativa, las notas (7%) y los exámenes (7%) son más codiciados que las credenciales (4%), mientras que otra información como Datos de la facultad (2%), Documentos confidenciales (2%), Acta de grado (2%), Sistema operativo Windows (2%) y sitio web (2%), son menos representativos al interior de la muestra.

Sector afectado

Acorde con la muestra la afectación en su mayoría es Toda la universidad (40%), seguidos por un Área específica (24%), o por Personal y estudiantes (9%) o solo Estudiantes (9%). El ataque también puede centrarse en un software o Programa informático (7%) o afectar solo a Aspirantes (7%), siendo menos frecuentes Personal de la universidad (2%) o los ciberataques que no dan información al respecto (2%).

Impacto percibido del ciberataque

En general desde la cobertura mediática no se da información que permita cuantificar o vislumbrar el impacto del ciberataque en un 29% de las instituciones, el 20% lo manifiesta en relación a la exposición de datos o información, el 16% lo cuantifica en relación al tiempo que ha quedado sin operación, el 11% no da valores al respecto mencionando frases como: estudiantes, otro 11% manifiesta un impacto económico ya sea por gastos de recuperación o por pago de extorsión, un 7% mide el impacto en número de personas que han sido afectadas, un 2% manifiesta no percibir afectación, un 2% considera que el impacto se encuentra en la perdida de prestigio y finalmente un 2% lo menciona en relación a la perdida de hardware que sobrevino con el ciberataque.

Al dimensionar en cifras a partir de los 45 casos analizados que incluían información cuantificables, se estableció que el impacto económico asciende a un total de 1.704.041,10 euros correspondientes al pago de extorsión o dinero invertido en reposición de equipos. En tanto que el impacto por exposición se encuentran 6.072.241 datos e información de personas y 76.000.003 documentos expuestos. En personas alrededor del mundo afectadas 197.795 y en infraestructura 1.200 servidores y 10.000 ordenadores. Cuyo impacto cuantificado en tiempo equivale desde unas 30 horas paralizados, hasta tres meses, ocasionando en este último caso el cierre de la institución.

Darse cuenta del ciberataque

La mayoría de las instituciones realizan una detección interna del ataque (60%), otras lo saben cuando llega la demanda de pago (13%), otras son alertadas por estudiantes (11%), por mensajes ajenos (7%), otras por un medio de comunicación (4%), son los docentes quienes se dan cuenta (2%) o no ofrecen información al respecto (2%).

Proceso Jurídico

Desde la cobertura mediática se establece que el 44% realiza denuncia ante el organismo respectivo, otro 44% no menciona información al respecto, el 9% informa de un proceso judicial en curso contra atacantes más allá de la denuncia institucional y un 2% corresponde a una cobertura de una demanda interpuesta por estudiantes a raíz de la filtración de datos.

Condena

En la mayoría de la cobertura mediática (89%) no existe información al respecto, se encuentran absoluciones (4%), Se recupero el dinero pagado de la extorsión en 2% y en 2% no se llegó a culminar el ataque.

Comunicación

Finalmente, se encuentra que las comunicaciones no fueron afectadas en un 47%, un 33% de los casos no realizó una mención al respecto, un 9% se apoyó en redes sociales o App de mensajería (WhatsApp), 7% logró restaurar el correo, un 2% generó Correos temporales, un 2% menciona afectación parcial.

Correlación entre variables categóricas de información

En la tabla 3, se resumen todas las correlaciones tenidas en cuenta, se resaltan una correlación moderada entre autor y tipo de información, y entre afectados y ciberataque, algunas correlaciones débiles entre afectados y ciberataque/tipo de información/ año que se corresponden con los hallazgos obtenidos de concentración de ataques en el 2021, siendo afectadas las universidades con ciberataques de Ransomware.

También se encuentran correlaciones negativas débiles entre país y ciberataque/afectados, y entre tipo de información y ciberataque, lo cual se corresponde con las concentraciones de la muestra con relación al país, ciberataque y tipo de información. En las otras variables la correlación es inexistente.

Tabla 3. Correlaciones entre categóricas

Correlación	Vr.
Correlación autor y tipo de información	0,49
Correlación afectados y ciberataque	0,30
Correlación año y afectados	0,23
Correlación afectados y tipo de información	0,20
Correlación año y país	0,13
Correlación año y tipo de información	0,07
Correlación autor y país	0,07
Correlación año y autor	0,00

Correlación	Vr.
Correlación año y ciberataque	0,00
Correlación afectados y autor	-0,05
Correlación autor y ciberataque	-0,07
Correlación país y ciberataque	-0,17
Correlación tipo de información y país	-0,20
Correlación tipo de información y ciberataque	-0,20
Correlación afectados y país	-0,23

Fuente: Elaborada por el autor

Esta información sobre las correlaciones entre variables categóricas del estudio, permiten observar correlaciones positivas, negativas y neutras que serán discutidas en el siguiente apartado. Aunque es probable que a medida que aumente la digitalización, también incrementen las economías delictivas como servicios (Fraude, Ataque, Cibercrimen y Desinformación como servicio), así como las nuevas relaciones al interior de la red.

Haciendo que estas correlaciones evolucionen mostrando nuevas correlaciones en ciberdelitos que ganan peso, como aquellos que aprovechan brechas de seguridad sin parches, los basados en la computación cuántica, el internet de las personas, el pretexting, los ataques multicanales, el burnout, entre otros, que estarán presentes en el futuro cercano.

Discusión

Para cada sector económico existen unas fechas de mayor impacto, en el caso de la Universidad si se tiene en cuenta el año, se observa que a mayor uso de sistemas de información conectados a la red mayor probabilidad de ataque, como se evidencia con las primeras medidas que la OMS sugiere en 2020 (Interpol, 2020). En el caso específico de la Universidad el pico más alto se encuentra en 2021.

Sin embargo, si se dejan de lado las consecuencias de las decisiones tomadas durante pandemia, y se observa la categoría mes, se encuentra un patrón de frecuencia relacionado con los meses de cierre diciembre-enero y junio, siendo más habituales en fin de semana, lo cual puede incrementar el impacto, al ser días en que no está operativa la institución disminuyendo la probabilidad de la una respuesta rápida.

En cuanto al día seleccionado según el número se podría inferir cierta superstición ligada al ciberataque, dado que dentro de los seguidores de la numerología los números 1, 8 y 22 poseen un significado especial tanto en la tradición de occidente como en oriente (Instituto Confucio, 2019; Méndez, s.f.).

Con relación al autor, el porcentaje de Desconocidos puede estar relacionado con la protección de datos que se deriva de un proceso judicial en curso (secreto de sumario), en donde la autoría de grupos tipo ransomware señala un nuevo perfil de ciberdelincuente basado en el Lucro, como lo señala el estudio de tipología de Navarra (Gobierno de Navarra, s.f) que es cimentada en una organización criminal.

De otra parte, su relación con ciberespionaje señalado como autoría, es algo plausible dentro del escenario actual, que: 1) acentúa la hiperconectividad (Puime, 2009), 2) las diferencias entre Europa – Rusia y China en relación a ciberseguridad como se dejó entrever en la Convención de Ciberdelincuencia celebrada por la ONU en 2023 o, 3) el escenario tenso con estos países (Colom, 2020). De esta forma, la autoría se constituye en una estrategia de guerra tanto en el reconocimiento como en la ocultación, emergiendo el terrorismo tecnológico (Francisco, 2021), aunque otros autores consideren este proceso como una evolución de los servicios preexistentes de inteligencia nacional (Kravetz, 2023), lo cierto es que el ciberespacio se constituye en un nuevo escenario de juegos de poder individuales y colectivos.

En el caso de autoría de estudiantes, que en otros tiempos se consideraban como autores de ataques a universidades (Molist, 2014), su disminución en la participación podría relacionarse con las sanciones y penalizaciones que actualmente existen, así como en el desarrollo de la ciberseguridad. En cuanto a la autoría de funcionarios, se evidenciaron dos tipos: una que se relaciona con un fallo humano– una característica común de los ciberataques hacia la industria- (Ayerbe, 2018) y el fallo intencional que, en el caso de estudio se relacionaba con una situación que afectaba a personajes políticos, en donde el ciberataque se constituye en una estrategia política y el prestigio de la Universidad en un daño colateral.

Al respecto del país, si se contrastan los resultados del estudio por regiones con relación a los resultados de la encuesta mundial de la Interpol (INTERPOL, 2020), se encuentran tendencias similares lideradas por Europa, sin embargo, en el informe de INTERPOL era seguida por Asia y luego América, mientras en el estudio se encuentra primero América y luego Asia. Aunque es importante resaltar que dada la perdida de prestigio que podría implicar el ser víctima de un ciberataque, más aún en aquellas instituciones que poseen programas de formación relacionados con ciberseguridad, los hechos dados a conocer mediáticamente sean inferiores a los reales, y que sólo hayan trascendido por situaciones relacionadas con el impacto de la normativa que obliga en algunos países a comunicar el incidente o se oculte la información como estrategia de inteligencia nacional.

Esta situación de obligatoriedad podría explicar los altos porcentajes de casos de países como España, Estados Unidos y el Reino Unido, aunque también pone de manifiesto el deber del Estado ante los ciberataques, es decir la “ciberdiligencia debida” (Cocchini, 2021), más aún en un contexto que prevé presentación de ciberataques importantes en el futuro inmediato incrementado por la exposición del internet de las cosas (Piernas, 2024), el emergente internet de las personas; la necesidad de colaboración entre estados (Barreiro, 2024) en contextos disruptivos que no obedecen a lógicas de sobre conceptos arraigados como el efecto de proximidad (Gómez y Shandler, 2024) o se fundamentan en tecnología de punta como la Inteligencia artificial apoyando tareas de ciberataques (Bas et al., 2024), que podrían presentar desafíos importantes para personas, instituciones. Sociedades y Estados-Nación.

Si se observan los tipos de Ciberataques que emergieron en la muestra desde la clasificación del INCIBE (INCIBE, 2020), se encuentra una mayoría de ciberataques por Malware (Virus, troyanos, Ransomware, Cryptohacking, keyloggers, spyware, Filtración de datos), seguido por ataques a Conexiones (Suplantación, Intento de acceso, Ataque DDos) y ataques por Ingeniería Social (Phishing), teniendo mayor cobertura mediática aquellos que poseen mayor impacto y exposición social (Ransomware y Filtración de datos), que pone de manifiesto la necesidad de las universidades como lo expresa Hasay de asumir el reto de "compartir datos mientras se aseguran secretos" (Hazay, 2017), en donde la prevención individual de cada miembro de la comunidad hace más fuerte la institución y refuerza su cultura de ciberseguridad.

Acorde con el Tipo de información y el Sector afectado, se puede inferir que el móvil apunta al lucro, por tanto, los ataques a los sistemas de información que dejan inhabilitada la institución podrían ser más persuasivos para forzar el pago de la extorsión, así como la exposición de los datos e información personal, que pueden acarrear demandas tal como se encontró en la muestra del estudio. Aunque también es importante resaltar que en un entorno digital la hiperconectividad conlleva a que las vulnerabilidades y riesgos informáticos de los proveedores también se conviertan en los propios, como se evidenció en la muestra a través de software informático o servicios de Cloud, y a nivel mundial se vivió con el colapso de los sistemas generado por la actualización de CrowdStrike (Venegas, 2024), que de forma reciente, puso en la mira el papel de los proveedores de servicios digitales dentro de la ciberseguridad.

En relación al impacto, desde la cobertura mediática se encuentra que no existen datos concretos y específicos dentro de todos los casos, esto se explica porque el momento en que se da a conocer la noticia (poco tiempo después del ciberataque) no se pueden tener datos concretos del impacto general. Aun así, se pudo establecer seis tipos de impactos: 1) económicos, 2) exposición, 3) tiempo de cese de actividades, 4) infraestructura, 5) personas afectadas y 6) prestigio.

En aquellos que se encuentran datos cuantitativos como el impacto económico, se encuentra que el impacto mencionado es igual a la suma de siete de los diez estados top víctimas de ciberataques durante el 2021 en Estados Unidos (FBI, 2021), con lo cual el impacto dentro de los presupuestos institucionales, tal como se encontró en el estudio, puede conducir al cierre de la institución.

En cuanto al tiempo se encuentra que es una variable importante dentro de la continuidad de la institución universitaria, por ello parte de los procesos de prevención incluyen la elaboración del plan de contingencia y continuidad del negocio (INCIBE, s.f), además de incluir información que permita soportar el ataque con estrategias de comunicación que según el estudio encuentran apoyo en aplicaciones de mensajería, restauración de servicios o correos temporales. En donde la rápida respuesta institucional juega a favor, sobre todo en un sector que sufre más ataques internos que cualquier otro sector (Protectdata, 2023), con lo cual la educación en ciberseguridad y ética es más que imprescindible.

En relación con la afectación de personas, con las cifras del estudio se calcula que los afectados sumarían el equivalente a la población total de diez países pequeños -con sólo 45 instituciones- y si se dimensionan los datos e información expuesta la afectación podría llegar a la población entera de Portugal, España, Viena y Holanda sumadas.

Por tanto, si bien la digitalización permite disminuir el espacio/tiempo necesario para procesar y almacenar información, también expone dramáticamente la magnitud de impacto y afectación dentro de una institución y su comunidad, que podría prolongarse o mantenerse en el tiempo llevando al cierre de la misma, sin que ello permita resarcir la exposición de sus comunidades, y por el contrario podría tener un impacto superior al incluirse el internet de las cosas y los sistemas inteligentes dentro de las instituciones tal como sucedió con la Universidad de Frankfurt durante 2024 (INCIBE, 2024), poniendo de manifiesto la fragilidad de la hiperconectividad.

Por ello el "darse cuenta" es un evento significativo, en el caso del estudio la detección interna fue importante para limitar el impacto y trazar estrategias para hacer frente al ataque, así como construir alianzas con instituciones del Estado y la empresa privada a fin de sumar sinergias (Jiménez, 2020), mejorando su resiliencia interna.

Adicionalmente, al informar a terceros (Estado, Empresa privada, Comunidad educativa), se siguen los protocolos normativos, que evitan futuras sanciones o demandas por daños derivados del ciberataque a terceros, y se da lugar a procesos de investigación policial y judicialización que podrían llegar a posibilitar la recuperación del daño en un futuro, como se encontró en el estudio. A la par que deja entrever las necesidades de adopción de protocolos de seguridad, cifrado de datos, sistemas de autenticación y educación del usuario final (Ciberpyme, 2024), entre otras medidas que garanticen la seguridad, integridad y confiabilidad de los datos individuales y sociales que son depositados en custodia de las instituciones de educación superior.

Conclusiones

En conclusión, el comercio de la información, en sincronía con un contexto de hiperconectividad y alta tendencia a la digitalización convierten a las universidades en un objetivo de ciberataques. Estos ciberataques a partir de la muestra del estudio se caracterizan por tener un incremento significativo durante el año 2021, que podría ser explicado por un mayor uso de la virtualidad dentro de los escenarios educativos, especialmente en los meses de enero, junio y diciembre que suelen tener mayor incidencia dentro de los calendarios escolares.

A pesar de la autoría desconocida en su mayoría, pueden atribuirse a grupos al margen de la ley, estudiantes y funcionarios de forma generalizada. Cuya motivación pasa desde el fallo humano, la alteración (notas, titulaciones), hasta el lucro económico, que son congruentes con la correlación moderada obtenida en el estudio entre las variables: a) Autor y tipo información, b) Afectados y tipo de ciberataque, y c) Tipo de ciberataque e información.

Es importante tener en cuenta que los ciberataques se incrementan con el nivel de digitalización presente dentro de las comunidades educativas, y su impacto se agudiza exponencialmente con sistemas hiperconectados integrados a través del internet de las cosas o sistemas inteligentes presentes en la institución educativa.

En cuanto a su localización geográfica, se caracterizan por concentrarse en Europa, (especialmente en España, Reino Unido y Países Bajos), seguido por América (Estados Unidos, Colombia, Canadá, Uruguay, Chile y Venezuela), y finalmente Asia (Israel). Aunque es importante tener en cuenta que los datos pueden estar sesgados por regulaciones locales (por ejemplo: obligación de dar a conocer), geoposicionamiento de los navegadores/motores de búsqueda, idioma en el que se realizó la búsqueda, entre otras variables.

De otro lado, los ciberataques por Malware y Filtración de datos suelen ser más comunes, dado que poseen mayor impacto y exposición de datos. Aunque no todos los ciberataques son resultado de una acción directa de un externo, puesto que también se relacionan con fallas en los proveedores de servicios informáticos como programas, sistemas o almacenamiento en la nube, haciendo más vulnerable los alcances de las instituciones educativas en cuanto a su protección online.

En cuanto a los tipos de impactos, según la percepción de las instituciones universitarias, se identificaron seis tipos: 1) económicos, 2) exposición, 3) tiempo de cese de actividades, 4) infraestructura, 5) personas afectadas y 6) prestigio; que al ser cuantificados evidencian un impacto negativo importante en los presupuestos del sector educativo.

De otro lado, variables como: 1) el tiempo para “darse cuenta”, 2) el tiempo requerido para la recuperación y, 3) las sinergias con los diferentes sectores de apoyo pueden ser vitales para la continuidad institucional, constituyéndose en factores decisivos de resiliencia institucional.

En cuanto a la judicialización, se establece que inicia con la denuncia, y conlleva un proceso que puede desencadenar en absolución, condena o recuperación de las pérdidas acarreadas según la muestra del estudio, aunque de forma general desde la cobertura mediática no se encuentra información que permita hacer seguimiento de todo el proceso de un ciberataque.

Adicionalmente, de acuerdo con los datos de los estudios sobre ciberataques al sector educativo en contraste con los casos recuperados desde la cobertura mediática, se encuentra una infra cobertura del fenómeno de ciberataques contra las instituciones de educación superior, que conlleva a que la muestra no sea representativa estadísticamente y por tanto, a pesar de compartir tendencias con otros estudios, los resultados no son generalizables a la situación general del sistema universitario, que se considera debe ser muy superior y probablemente de extremada gravedad con el auge confluyente del uso delictivo de la IA, y las economías que hacen del ciberdelito un servicio lucrativo.

Por tanto, los resultados obtenidos se circunscriben específicamente al escenario de cobertura mediática de ciberataques a universidades tenidos en cuenta dentro de la muestra. Aun así, permiten visibilizar una situación que viven las instituciones universitarias en silencio, debido a situaciones que podrían estar

relacionadas con la necesidad de: conservar del prestigio institucional, minimizar el impacto del ciberataque dentro de la opinión pública, mantener margen de maniobra de la problemática de forma interna, atender a las reservas del proceso legal, entre otras, reguladas por la diversidad de afrontamiento legal de los ciberdelitos en cada país.

En este camino, es probable que exista una infravaloración social de los ciberataques a comunidades educativas, que puedan contribuir negativamente con una posición generalizada de invisibilización de la probabilidad de ciberataque, lo cual afecta la preparación individual y colectiva de las instituciones educativas y sus comunidades, ante los ciberataques existentes y los emergentes en confluencia con nuevas formas de digitalización, automatización y servicios basados en la nube.

En consecuencia, se recomienda: 1) Fomentar un tejido de apoyo intra e interinstitucional interuniversitario local y transfronterizo, que facilite el intercambio de experiencias relacionadas con ciberataques, tanto en los casos exitosos como en aquellos que no lo son. Este intercambio podría incluir los mecanismos de respuesta, las instituciones de apoyo efectivo y las medidas adoptadas, constituyéndose en la base de una colaboración sólida que fortalezca la protección de las comunidades educativas y sus sociedades en su conjunto frente a los ciberataques, y 2) Realizar estudios posteriores que permitan ampliar el conocimiento sobre los ciberataques dentro de los sistemas de educación superior, a fin de mejorar la prevención y mitigación de sus efectos.

Financiación

No se recibió financiación externa para la realización de la investigación.

Declaración de conflicto de intereses

Esta investigación no posee ningún conflicto de interés propio, con la revista, la entidad editora y/o las entidades financiadoras.

Contribución de Autores

Aura-M Torres-Reyes: Conceptualización; curación de datos; supervisión, análisis formal; investigación; metodología; escritura–borrador original, revisión, corrección y edición del documento final.

Referencias

Agencia Española de Protección de Datos. (2016). Reglamento General de Protección de Datos, RGPD. EUR-Lex–32016R0679–EN–EUR-Lex. Europa.eu. https://acortar.link/l6LPTB

Akyazi, U. (2021). Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum. https://acortar.link/7c3JSQ

Ali, W. (2020). Online and remote learning in higher education institutes: a necessity in light of COVID-19 pandemic. Higher Education Studies 10(3), 16–25. https://acortar.link/GC94tw

Al-Samarraie, H. (2019). A Scoping Review of Videoconferencing Systems in Higher Education: Learning Paradigms, Opportunities, and Challenges. *Int. Rev. Res. Open Distrib. Learn.* 20 (121). https://acortar.link/UEh12w

Álvarez, D. y Enríquez, J. (2023). *La digitalización de las masas y los riesgos del dataísmo. Análisis Jurídico-Político.* 2(3) 63-91. https://doi.org/10.22490/26655489.3913

Anaya, T., Montalvo, J., Ignacio, A y Arispe, C. (2021). Escuelas rurales en el Perú: factores que acentúan las brechas digitales en tiempos de pandemia (COVID-19) y recomendaciones para reducirlas. *Educación XXX.* (58). 11-33. http://dx.doi.org/10.18800/educacion.202101.001.

Anggoro, K., y Rueangrong, P. (2020). Facebook: An alternative learning platform for online English as a foreign language instruction in the time of COVID-19. *Journal of Education Naresuan University,* 23(1), 413-423. https://acortar.link/gEs2eG

Ayerbe, A. (2018). La ciberseguridad de la industria 4.0: Un medio para la continuidad del negocio. *Revista Economía Industrial*. 410 (2018). 37-46. https://acortar.link/ix7LdF

Azfal, I. y Abdullah, N. (2020). Role of WhatsApp in teaching and learning process in schools in Pakistan. *Journal of Educators online.* https://files.eric.ed.gov/fulltext/EJ1363787.pdf

Barreiro Santana, K. (2024). Crimen organizado, conflictos fronterizos, lavado de activos y ciberespacio: desafíos actuales en la región. *Estado & Comunes, 1(18), 203–208. DOI:* https://doi.org/10.37228/estado_comunes.v1.n18.2024.343

Bas Graells, G., Tinoco Devia, R., Salinas Leyva, C., y Sevilla Molina, J. (2024). Revisión sistemática de taxonomías de riesgos asociados a la Inteligencia Artificial. *Analecta Política, 14(26). DOI:* https://doi.org/10.18566/apolit.v14n26.a08

Bastidas, Y. (2023). ChatGPT, inteligencia artificial y educación superior: ¿Qué deben saber las instituciones de educación superior? – UNESCO-IESALC. https://acortar.link/M81GBs

Bjorge, J. y Wangen, G. (2021). A systematic review of Cybersecurity Risks in Higher Education. *Future Internet, MDPI.* 13(2). 1-40. https://doi.org/10.3390/fi13020039

BlueVoyant. (2021, febrero). Cybersecurity in Higher Education Report. BlueVoyant. https://acortar.link/WgYOWQ

BOE-A-2010-1330 (2022). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE. https://acortar.link/RVMAGG

BOE-A-2010-14221. (2014). Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. BOE. https://acortar.link/9nlynm

Bojović, Ž., Bojović, P.D., Vujošević, D. y Šuh, J.(2020). Education in times of crisis: Rapid transition to distance learning. *Comput. Appl. Eng. Educ*. 28, 1467–1489. https://doi.org/10.1002%2Fcae.22318

Bologna, E. (2019). Capítulo 1 Los datos estadísticos | Un Recorrido por los Métodos Cuantitativos en Ciencias Sociales a bordo de R. Rbind. https://acortar.link/TCUQh2

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. Comput. *Secure.* 86, 350–357. https://doi.org/10.1016/j.cose.2019.07.003

Cabero, J., y Valencia, R. (2019). TIC para la inclusión: una mirada desde Latinoamérica. Aula Abierta, 48(2), 139–146. https://doi.org/10.17811/rifie.48.2.2019.139-146

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*. 60 (abr-jun), 471-512. https://dialnet.unirioja.es/descarga/articulo/7524987.pdf

Cando-Segovia, M. R., y Medina-Chicaiza, P. (2021). Prevención en ciberseguridad: enfocada a los procesos de infraestructura tecnológica. 3C TIC. *Cuadernos de desarrollo aplicados a las TIC,* 10(1), 17-41. https://doi. org/10.17993/3ctic.2021.101.17-41

Cano, J. (2020, 6 de agosto). Seguridad y ciberseguridad 2009-2019: Lecciones aprendidas y retos pendientes. 155. 4-7. *Revista Sistemas.* https://doi.org/10.29236/sistemas.n155a1

Cayón, J., y García, L.A. (2014). La importancia del componente educativo en toda estrategia de Ciberseguridad. *Estudios en seguridad y defensa*, 9(18), 5-13. https://doi.org/10.25062/1900-8325.9

Chávez, G. (2020, 26 de agosto). Las universidades en jaque informático. *Expansión.* https://acortar.link/0RT5nz

Ciberpyme. (2024, abril). Los mayores ciberataques y vulneraciones de datos, ataques de ransomware: marzo de 2024–*Revista de Ciberseguridad y Seguridad de la Información para Empresas y Organismos Públicos.* https://acortar.link/endsMN

Cocchini, A. (2021). Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados. *Revista UNISCI*. 55 (Enero). 69-98. https://acortar.link/h4xnV3

Colom, G. (2020). China y Rusia en las zonas grises del ciberespacio. Amenaza híbrida: la guerra imprevisible. Ministerio de Defensa. https://acortar.link/EeFZ9n

Constantin, L. (2023, 3 de enero). El ecosistema del 'ransomware' se diversifica de cara a 2023. *CSO Computer España*. https://acortar.link/MJLgBQ

Daher, M et alt. (2022). TIC y metodologías activas para promover la educación universitaria integral. *Revista electrónica de investigación educativa*, 24, (e08).https://doi.org/10.24320/redie.2022.24.e08.3960

Erard, G. (2022, May 18). Un médico venezolano, en el punto mira de EE. UU por crear los ransomware Thanos y Jigsaw. Hipertextual. https://acortar.link/HnO4uO

España, Jefatura del Estado. (2010, 8 de enero). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado, núm. 25, de 29 de enero de 2010, páginas 1 a 12. https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf

Farreras, C. (2023, June 2). Las escuelas suecas dan marcha atrás en el uso de pantallas y vuelven a los libros de texto. *La Vanguardia*. https://acortar.link/3FbK45

FBI. (2021). Internet Crime Report 2021. FBI. https://acortar.link/7lydmy

Fernández, J., López, M., Pérez, Á., Hortigüela, D. y Manso, J. (2022). La brecha digital destapada por la pandemia del coronavirus: una investigación sobre profesorado y familias. *Revista Complutense de Educación*, 33 (2). 351-360. https://doi.org/10.5209/rced.74389

Fernández, J., Miralle, F., y Millana, L. (2019). Perfil psicológico en el ciberdelincuente. *Revista Iberoamericana de las Ciencias Sociales y Humanísticas*. 8(16). 1-22. https://doi.org/10.23913/ricsh.v8i16.179

Francisco, S. (2021). La digitalización del miedo: del terrorismo "clásico" al terrorismo "tecnológico". *El criminalista digital: papeles de criminología*. 10 (2021). 1-19. https://acortar.link/jaVo4z

Funk, R. L. (2021). Challenges for higher education in times of COVID-19: How three countries have responded. *Higher Learning Research Communications*, 11, 106–111. https://doi.org/10.5590/10.18870/hlrc.v11i0.1242

Gibbs, S. (2018, April 9). YouTube illegally collects data on children, say child protection groups. The Guardian*; The Guardian*. https://acortar.link/XstoxE

Gobierno de Navarra (s.f.). *El delincuente: Tipología delictiva. Delincuente común. Delincuente violento.* Delincuente sexual. Delincuentes juveniles. Responsabilidad penal del menor. Ciberdelincuencia. Gobierno de Navarra. https://acortar.link/viSqi2

Gómez, M. A., y Shandler, R. (2024). Trust at Risk: The Effect of Proximity to Cyberattacks. *Journal of Global Security Studies*, 9(2). DOI: https://doi.org/10.1093/jogss/ogae002

González García, A., y Campoy Torrente, P. (2018). Ciberacoso y cyberbulling: diferenciación en función de los precipitadores situacionales. *Revista Española de Investigación Criminológica*. DOI: https://doi.org/10.46381/reic.v16i0.149

González, T. (2010). El secreto sumarial y el derecho a informar. *Cuadernos de periodistas.* Marzo (2010), 124-129. https://acortar.link/v059uS

Grosseck, G., Maliţa, L., y Bunoiu, M. (2020). Higher education institutions towards digital transformation-The WUT case. In: European Higher Education Area: Challenges for a New Decade. Cham: Springer, 565–581. https://acortar.link/KbszIu

Harrell, C. R., Patton, M., Chen, H., y Samtani, S. (2018, noviembre). Vulnerability assessment, remediation, and automated reporting: Case studies of higher education institutions. In 2018 I*EEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 148-153). IEEE. https://acortar.link/htRAEw

Hazay, C. (2017). *Sharing Data While Securing Secrets* | The Alexander Kofkin Faculty of Engineering. Biu.ac.il. https://acortar.link/D6wgjT

Hernández, J. et al. (2018). Sobre el uso adecuado del coeficiente de correlación de Pearson. *AVFT.* 37(5), 587-595. https://acortar.link/GVjrC3

Hoppenstedt, M., Rosenbach, M., y Hakan Tanriverdi. (2023, 17 de julio). *Kritische Schadcode-Bibliothek: Datenleck offenbart Kunden der Google-Sicherheitsplattform VirusTotal.* DER SPIEGEL. https://acortar.link/NrVbtf

IAB (2019). Libro blanco de Data. IAB. https://acortar.link/WkIA5p

INCIBE. (2020). *Guía de ciberataques*. INCIBE. https://acortar.link/ZO6ZT7

INCIBE. (2024, 6 de julio). *Ciberataque a la Universidad de Frankfurt.* INCIBE. https://acortar.link/gkbe2B

INCIBE. (s.f.). *Plan de contingencia y continuidad de Negocio*. INCIBE. https://acortar.link/hCkPFP

Insorio, A. O. y Olivarez, J. A. (2021). Utilizing Facebook and Messenger Groups as Platforms for Delivering Mathematics Interventions in Modular Distance Learning. International Journal of Professional Development, Learners and Learning, 3(1), ep2109. https://doi.org/10.30935/ijpdll/11290

Instituto Confucio. (2019). Numerología: Hacer números en China es cuestión de suerte. *Universidad de Valencia*. https://acortar.link/KFi4Nr

Internet Organised Crime Threat Assessment (IOCTA) 2021 | Europol. (2021). Europol; Europol. https://acortar.link/Q5nOQf

Interpol (2020). *Ciberdelincuencia: Efectos de la Covid-19*. Interpol. https://acortar.link/7uF8VD

Jiménez, M. (2020, 20 de marzo). Empresas de ciberseguridad colaboran con el CNI para blindar los servicios críticos. *Cinco Días.* https://acortar.link/Pir5pH

Juste, M. (2024, 7 de febrero). Así regula España el uso que hacen los menores de la tecnología. Expansion. https://acortar.link/2nhAvM

Kaspersky. (2020, 4 de Septiembre). Digital Education: The cyber risks of the online classroom. Securelist.com; Kaspersky. https://acortar.link/j7cAYs

Kravetz, J. (2023). Operaciones especiales en el ciberespacio: espionaje, sabotaje y subversión en el siglo XXI. *Revista de la Escuela Nacional de Inteligencia. 3 (2023).* 35-64. DOI: https://doi.org/10.58752/1PVI0VZ2

Kuric K, S., Calderón, D. y Sanmartín, A. (2021). Educación y brecha digital en tiempos del COVID-19. Perfiles y problemáticas experimentadas por el alumnado juvenil para afrontar sus estudios durante el confinamiento. *Revista de Sociología de la Educación RASE,* 14 (1). 63-84. https://doi.org/10.7203/RASE.14.1.18265

Kwaa-Aidoo, E.K.; Agbeko, M. An Analysis of Information System Security of a Ghanaian University. Int. J. Inf. Secur. Sci. 2018, 7, 90–99. https://acortar.link/CAaJeN

Le, N. (2022). Literature Review on the Barriers to Online Learning during Covid-19 Pandemic. Open Access Library Journal, 9, 1-9. https://doi.org/10.4236/oalib.1109219

Lei, M. y Medwell, J. (2021). Impact of the COVID-19 pandemic on student teachers: how the shift to online collaborative learning affects student teachers' learning and future teaching in a Chinese context. Asia Pacific Education Review. 22(2), 169–179. https://doi.org/10.1007/s12564-021-09686-w

López, J., et. Alt. (2022). *Informe sobre la cibercriminalidad en España*. Ministerio del Interior. España. https://acortar.link/85Zw

Malianos, R. (2023). La agenda medioambiental: el rol de los medios de comunicación en Nicaragua. *Revista Humanismo y Cambio social.* 22(10). 48-60. https://doi.org/10.5377/hcs.v21i21.17662

Matthew J. et al. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. *Revista Española de Cardiología,* 74 (9), 790-799 https://doi.org/10.1016/j.recesp.2021.06.016.

Méndez, M. (s.f.). El significado de los números en su aplicación a la numerología. https://acortar.link/EnB6Ua

Microsoft Security Intelligence. (2018). *Cyberthreats, viruses, and malware.* Microsoft.com. https://acortar.link/K6Jz9o

Molist, M. (2014, 26 de julio). De cuando las universidades eran nidos de "hackers." *EL MUNDO.* https://acortar.link/0FVjwU

Morgan H (2020). Best practices for implementing remote learning during a pandemic. The Clearing House. *A Journal of Educational Strategies.* 93(3): 135–141. https://doi.org/10.1080/00098655.2020.1751480

Morgan, S. (2020, 10 de noviembre). Cybercrime To Cost the World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://acortar.link/5Y3wTb

Munarriz, B. (1992). Técnicas y métodos en Investigación cualitativa. Universidad del País Vasco. Jornadas de Metodología de la Investigación educativa. https://acortar.link/JXVnV3

Nacional Cyber Security centre. (2023). *Alert: Further ransomware attacks on the UK education sector by cyber criminals.* Ncsc.gov.uk. https://acortar.link/Z4NC6N

Ochoa, B., Correa, J., Gutiérrez, A. (2019). Las TIC en la atención a la diversidad educativa: el caso de la Comunidad Autónoma Vasca. *RED. Revista de Educación a Distancia.* 61, (07). http://dx.doi.org/10.6018/red/61/07

Onwuegbuzie, A. y Frels, R. (2016). *7 Steps to a comprehensive literature review: A multimodal & Cultural Approach*. SAGE

Palau, A. y Davesa, F. (2013). La cobertura mediática de los escándalos de corrupción en España y su impacto en la opinión pública (1996-2009). *Revista Española de Investigaciones sociológicas (REIS)*. (144). 97-126. https://dialnet.unirioja.es/servlet/revista?codigo=1106

Payne, B. et. Alt. (2021). Impact of articulation agreements on student transfer between Higeher Education Institutions: a case study of a Cybersecurity program. Community college *Journal of research and practice*. 46(8), 573-588. https://doi.org/10.1080/10668926.2021.1887007

Piernas, J. (2024). The international law principle of due diligence and its application to the cyber context. Anales de Derecho, 41(1), 66–95. DOI: https://doi.org/10.6018/analesderecho.594441

Protectdata. (2023, 29 de diciembre). *Retos en ciberseguridad para el sector educativo en 2024*. Protectdata. https://acortar.link/UmdkGM

Puime, J. (2009). *El ciberespionaje y la ciberseguridad*. La violencia del siglo XXI. Nuevas dimensiones de la guerra. https://acortar.link/gQYTBh

Regan, J. (2021, 27 de julio). Los hackers más peligrosos y famosos del momento. Los Hackers Más Peligrosos Y Famosos Del Momento; Avg. https://acortar.link/kpOJEa

Romero, M. et alt. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. *3Ciencias.* http://dx.doi.org/10.17993/IngyTec.2018.46

Rueda et alt., (2017). *Internet de las Cosas en las Instituciones de Educación Superior*. Congreso Internacional en Innovación y Apropiación de las Tecnologías de la Información y las Comunicaciones – CIINATIC (1). https://acortar.link/2vFHgA

Rus, C. (2021, June 5). La curiosa historia del primer ransomware del mundo, su inventor y la víctima que consiguió eludirlo. *Xataka.* https://acortar.link/4zCggO

Sánchez, C. (2018, 14 de noviembre). El enemigo está en el interior... de tu ordenador. *XLSemanal*. https://acortar.link/3mLSA6

Sánchez, J. (2020, 25 de febrero). Nuevo México demanda a Google por recopilar sin permiso información de niños. *Diario ABC*. https://acortar.link/PGUYjs

Shaw, E. D. (2006). The role of behavioral research and profiling in malicious cyber insider investigations. *Digital investigación*, 3(1), 20-31. https://doi.org/10.1016/j.diin.2006.01.006

Terán, M. (2023, 28 de marzo). OpenAI reconoce un fallo en ChatGPT que filtró los datos y métodos de pago de los usuarios. *El Economista*. https://acortar.link/Mq0IWx

Ugur, N.G. (2020). Digitalization in higher education: A qualitative approach. *International Journal of Technology in Education and Science (IJTES),* 4(1), 18-25. https://acortar.link/XssxEJ

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

UNESCO (2023). *Education: From COVID-19 school closures to recovery*. Unesco.org. https://acortar.link/5tDoIC

UNESCO. (2023). *ChatGPT and Artificial Intelligence in higher education*. IESALC. https://acortar.link/gbjF25

Universidad Nacional de Asunción (2020). Las preguntas básicas de una noticia. Universidad Nacional de Asunción. https://acortar.link/M8Xc8A

Venegas, P. (2024, 19 de julio). *Cómo solucionar el problema del pantallazo azul de Windows por el fallo de CrowdStrike*. Computer Hoy. https://acortar.link/7kqSqm

Vives, T. y Hamui, L. (2007). La codificación y categorización en la teoría fundamentada, un método para el análisis de los datos cualitativos. *Metodología de la investigación Médica.* 10(40) octubre-noviembre, 97-104. https://doi.org/10.22201/fm.20075057e.2021.40.21367

W3Counter. (2023). Global Web Stats–December 2023. W3counter. https://acortar.link/qQ2npW

Yusuf, B.N. (2020). Are we prepared enough? A case study of challenges in online learning in a private higher learning institution during the covid-19 outbreaks. *Adv. Soc. Sci. Res.* 7, 205–212. https://doi.org/10.14738/assrj.75.8211

Zhang, G. et alt. (2017). *Dolphin Attack: Inaudible Voice Commands*. Association for Computing Machiner. October, 103-117. https://doi.org/10.1145/3133956.3134052

Zheng, R., et alt. (2021). Assessing the Security of Campus Networks: The Case of Seven Universities. *Sensors.* 21(1), 306. https://doi.org/10.3390/s21010306

Aura María Torres Reyes: posee un doctorado en Ciencias de la Educación y didácticas Específicas, así como una especialización en Economía Social por la Universidad de Zaragoza y un Máster europeo TIC para la educación y el aprendizaje. Su amplia experiencia en el sector privado y estatal, junto con su dedicación a la docencia y coordinación universitaria, le han permitido participar en escenarios de política social, educativa y tecnológica. Es autora de ponencias, artículos, capítulos de libros de investigación. Siendo actualmente, miembro colaborador de grupos de investigación nacionales e internacionales. https://orcid.org/0000-0002-4417-6740