

ENSAYO

"LA IDENTIDAD VIRTUAL, FRENTE A LOS RIESGOS DE LA SOCIEDAD CIVIL"

MSc. Anneth Yerania Mora Jiménez*

**Bachillerato en Ciencias de La Educación con Énfasis en la Enseñanza de la Informática, Bachillerato en Ciencias de la Educación con Énfasis En I Y II Ciclos, Licenciatura en Ciencias de la Educación con Énfasis en I Y II Ciclos, Licenciatura en Ciencias de la Educación con Énfasis en Administración Educativa, Maestría Profesional en Administración Educativa, anmoraj@gmail.com*

Universidad San Isidro Labrador, sede Pérez Zeledón.

Resumen

El impacto de los avances tecnológicos y la globalización en la identidad virtual, destaca cómo las tecnologías de la información han transformado la forma en que nos percibimos y nos relacionamos. Esta nueva realidad plantea desafíos en términos de inclusión y riesgo social, ya que la brecha digital puede excluir a ciertos grupos y aumentar la desigualdad. A medida que la sociedad se globaliza, la identidad virtual se convierte en un elemento trascendental en la interacción humana, pero también aumenta la vulnerabilidad de la información de las personas.

Es fundamental abordar los riesgos que sufre la identidad de las personas, mediante políticas que promuevan la inclusión digital y protejan la privacidad en un mundo cada vez más interconectado, por último, se subraya la necesidad de equilibrar los beneficios de la identidad virtual con los riesgos que plantea en una sociedad globalizada, buscando así obtener el mayor aprovechamiento de las tecnologías de la comunicación y la información.

Palabras Claves: avances tecnológicos, globalización, Identidad virtual, inclusión, riesgo social, sociedad globalizada, tecnologías de la información.

Abstract

The impact of technological advances and globalization on virtual identity highlights how information technologies have transformed the way we perceive and relate to each other. This new reality poses challenges in terms of inclusion and social risk, as the digital divide can exclude certain groups and increase inequality. As society globalizes, virtual identity becomes a crucial element in human interaction, but it also increases the vulnerability of people's information.

It is essential to address the risks facing individuals' identity through policies that promote digital inclusion and protect privacy in an increasingly interconnected world. Finally, there is an emphasis on the need to balance the benefits of virtual identity with the risks it poses in a globalized society, thus seeking to maximize the use of communication and information technologies.

Keywords: technological advances, globalization, virtual identity, inclusion, social risk, globalized society, information technologies.

"La identidad virtual, frente a los riesgos de la sociedad civil"

En la era digital en la que vivimos, la identidad social se entrelaza cada vez más con el mundo virtual. Desde perfiles en redes sociales hasta transacciones financieras en línea, nuestra presencia en la web se ha convertido en una extensión integral de la sociedad. Sin embargo, esta creciente interconexión no está exenta de riesgos, especialmente en un contexto donde la sociedad civil enfrenta desafíos constantes.

(Quirós, 2018) menciona en el capítulo 9 "La identidad virtual frente a los riesgos de la sociedad digital" del Informe Hacia la Sociedad de la Información y el Conocimiento 2018, una repentina realidad de lo que vive la sociedad con los avances y el desarrollo globalizado de las Tics detallando que,

En los últimos diez años, el acelerado desarrollo de las tecnologías y de la Internet como fenómeno de la globalización, así como el acceso y uso a diversas redes sociales ha conducido a nuevas formas de comunicación y a esquemas de comportamiento interactivo diarios en donde predomina la instantaneidad; (pág. 309)

La noción de identidad virtual abarca mucho más que simplemente tener un alias en la red, se trata de cómo nos presentamos, interactuamos y nos relacionamos en el paisaje digital, a medida que abrazamos esta nueva forma de

expresión y comunicación, también nos enfrentamos a una serie de amenazas y desafíos que pueden comprometer nuestra seguridad, privacidad y bienestar, por otra parte, las plataformas de redes sociales nos han permitido estar conectados de formas antes inimaginables, rompiendo las barreras geográficas y culturales en nuestra interacción diaria, además, la sobreexposición en línea ha erosionado la privacidad personal y ha generado preocupaciones sobre la autenticidad en nuestras interacciones.

Por ende, en este ensayo argumentativo, apoyado de diferentes actores se explorará la compleja relación entre la identidad virtual y los riesgos que acechan en la sociedad civil., desde la pérdida de privacidad hasta la manipulación de datos, pasando por la difusión de la desinformación y el acoso cibernético, donde se examinará cómo estos desafíos impactan en nuestra vida cotidiana y en la estructura misma de nuestra sociedad.

A través del análisis crítico y la reflexión profunda, buscamos no solo comprender los riesgos inherentes a nuestra identidad virtual, sino también explorar soluciones y estrategias para mitigarlos. Desde la educación digital hasta la implementación de políticas de protección de datos, nuestro objetivo es fomentar un entorno en línea más seguro e inclusivo para todos los miembros de la sociedad civil.

En el paisaje digital moderno y la noción de identidad ya no se limita a nuestras interacciones cara a cara, sino que se extiende a través de la extensión del ciberespacio en el que se afronta la realidad social. La presencia en línea e identidad virtual, ha venido a cambiar la vivencia de las personas, con un camino evolucionado para convertirse en una parte integral de quiénes somos, cómo nos relacionamos y cómo nos perciben los demás, sin embargo, este cambio hacia lo virtual no está exento de riesgos, especialmente en un mundo donde la sociedad civil enfrenta desafíos cada vez más complejos.

Existen muchas teorías y muchas situaciones que generan una serie de cambios en el ámbito social, político y económico de la sociedad, donde las Tecnologías de la información y comunicación “Tics” han venido a cambiar el diario vivir de las personas en la sociedad, involucrándose en su desarrollo social y profesional, dándole un giro a las actividades cotidianas de las personas.

A lo largo del tiempo, especialmente en las últimas décadas, se ha generado una importante revolución tecnológica que ha tenido, como consecuencia, el surgimiento de la denominada sociedad informacional, la cual consiste en la generación, en la gestión y en el uso de datos. (Martínez V., Rincón E., 2021).

En las últimas décadas, ha surgido una significativa revolución tecnológica que ha transformado radicalmente la manera en que interactuamos con el mundo que nos rodea, este cambio fundamental ha dado lugar a lo que ahora se conoce como la sociedad informacional. Desde la rápida expansión de internet, hasta el desarrollo de la inteligencia artificial, donde hemos presenciado un vertiginoso avance en la capacidad de recopilar, almacenar, procesar y analizar datos a una escala nunca antes imaginada. La revolución tecnológica ha dado lugar a la digitalización de casi todos los aspectos de nuestras vidas, desde la manera en que nos comunicamos y compartimos información, hasta cómo consumimos bienes y servicios, la tecnología ha permeado cada faceta de nuestra existencia.

Como lo detallan Martínez y Rincón en el artículo “Problemas y desarrollo de la identidad en el mundo digital”, en esta nueva era, los datos se han convertido en el activo más valioso, impulsando el crecimiento económico, la innovación y el desarrollo social, siendo un revulsivo social, en el que las personas se adaptan al medio, sin ver las repercusiones a futuro.

Por ende, se debe considerar para iniciar un análisis exhaustivo del tema como se da a conocer la identidad digital, su conceptualización y su aporte a la vida

cotidiana, desde un enfoque crítico sobre su interferencia en el ámbito, social, político y económico de los países y las personas.

(Lecuit, 2020) menciona que, “La identidad digital permite el reconocimiento y actuación de los individuos, las corporaciones o los poderes públicos en Internet.”

Ante esto, se debe dimensionar que, la identidad digital abre un mundo de posibilidades, permitiéndonos conectarnos con personas de todo el mundo, acceder a información instantánea y participar en comunidades diversas. Sin embargo, este mismo mundo virtual también presenta una serie de riesgos que pueden socavar nuestra seguridad y bienestar.

Basado en diferentes conceptos y publicaciones realizadas por diferentes organizaciones, se puede determinar que el concepto de identidad digital según Forbes México, en el artículo publicado por Javier López “Identidad Digital, ¿qué es y por qué es tan importante?”, el concepto más allegado a la realidad de la identidad digital lo determina desde visualizar a que “es la versión en internet de la identidad física de una persona.” (López, 2022), además en la publicación ¿Qué es la identidad digital?, del Banco Santander detalla que, “La identidad digital es el conjunto de información que sumado proyecta una imagen o reputación acerca de nosotros en Internet”, (Santander, 2023), por ende, desde los dos criterios presentados se puede determinar que la identidad digital es la imagen que refleja una persona en los equipos tecnológicos a nivel universal, desde una foto en una red social, sus correos y su forma de utilizar las aplicaciones digitales, “la identidad digital va un paso más allá de esta fase relacionada a nuestro comportamiento en la red, debe también validar que realmente somos quienes decimos ser” (Santander, 2023), ante ello la identidad digital o virtual también saca a relucir la presencia que tienen las tecnologías de la información y la comunicación en el diario vivir de las personas, impactando ya sea de forma positiva o negativa en su desarrollo social y emocional.

El uso de las Tecnologías de la Información y de la Comunicación (TIC) ha permitido que en muchas ocasiones los datos personales sean utilizados para fines distintos a los que originalmente fueron recabados, es decir, son transmitidos a otras instancias distintas de las que la persona dueña de los datos confió información, violentando su privacidad, por lo que, bajo el concepto de protección de datos personales, el titular tiene el derecho y la libertad de elegir qué desea comunicar, cuándo y quién, manteniendo el control sobre su información personal. (Rivera, 2019)

En un mundo donde la identidad virtual y los riesgos de la sociedad civil están intrínsecamente entrelazados, es fundamental abordar estos desafíos de manera proactiva y colaborativa, esto implica no solo adoptar medidas para proteger nuestra privacidad y seguridad en línea, sino también promover una cultura digital que fomente el respeto, la inclusión y la responsabilidad.

La sociedad nos ha llevado a redefinir nuestra relación con la tecnología, a cuestionar los límites de la privacidad y la seguridad de los datos, a aprender a explorar el potencial transformador de la información en la construcción de un futuro más conectado e innovador. En este contexto, la capacidad de adaptación y la alfabetización digital se han vuelto esenciales para participar de manera activa y significativa en esta nueva era de la información.

Hoy en día se ve marcado una realidad hacia el interés de la población estudiantil hacia el uso y estudio de especialidades acorde a las Tics, muchos estudios han salido a la luz donde se marca esta iniciativa de la población, pero sacan a relucir diferencias importantes hacia el interés de estas Rivera V., menciona en su artículo “Realidad sobre la Privacidad de los Datos Personales en Costa Rica”, que,

Frente al constante avance de cambios tanto sociales como tecnológicos, más personas jóvenes desean estudiar Computación e Informática; no obstante, en su mayoría son hombres quienes se inclinaban

por este tipo de carreras tal y como lo señaló Teletica el 1 de marzo del 2019 bajo el tema: "Costa Rica retrocede en inclusión de mujeres a trabajos con tecnología, afirma estudio", indicando que en el año 2000, 3 de cada 10 nuevos profesionales fueron mujeres y que para el año 2016 esa cifra bajó a 2 de cada 10;...(2019).

Aunque históricamente las especialidades como la informática en todos sus ámbitos han sido dominadas por hombres, la creciente demanda y relevancia de la tecnología ha abierto puertas a una mayor diversidad de estudiantes, incluidas más mujeres, el artículo de Teletica titulado "Costa Rica retrocede en inclusión de mujeres a trabajos con tecnología, afirma estudio", pone de relieve una disminución en la inclusión de mujeres en el campo tecnológico en el país, con una mayor inclusión de mujeres en el campo tecnológico, se busca abordar las barreras y promover un entorno que fomente la diversidad y la igualdad de oportunidades tanto para hombres y mujeres en el ámbito de formación profesional.

Con lo mencionado anteriormente, la sociedad hoy en día ha ido formalizando un desarrollo hacia la identidad digital, lo cual busca es generar ese interés hacia la misma, pero no se puede dejar de lado la problemática social y legal que ha venido a generar en muchas situaciones por los mismos errores que cometen las personas a la hora incursionar en las redes cibernéticas de hoy en día.

La sociedad globalizada en muchos momentos pierde el interés hacia el conocimiento de la protección de la identidad digital, la protección de datos y de información que se puede llamar como información clasificada en ocasiones no es protegida de la mejor manera y el error de este lo cometen las mismas personas a la hora de crear e implementar diferentes herramientas de protección de datos.

Desde la pérdida de privacidad y la exposición a la desinformación hasta el acoso cibernético y la manipulación de datos, los riesgos asociados con la

identidad digital son numerosos y variados, la velocidad y la escala en la que se propagan estas amenazas pueden ser abrumadoras, dejando a las personas vulnerables a ataques y abusos en línea.

La protección de la información y la privacidad no puede ser violentada, (Medrano, 2022) menciona “Los derechos digitales son aquellos sustentados en la protección de la dignidad, la libertad y las oportunidades de las personas frente a la tecnología, en relación con sus actividades en entornos digitales o el mundo físico” (pág. 316). En Costa Rica, la garantía de los derechos digitales se presenta como un desafío crucial en un contexto donde la tecnología avanza a pasos agigantados. Si bien es cierto que la protección de la dignidad, la libertad y las oportunidades de las personas en entornos digitales o físicos es fundamental, la realidad del país evidencia una brecha significativa entre los discursos y las acciones concretas para asegurar estos derechos. A pesar de los esfuerzos por promover la inclusión digital y la protección de datos, persisten preocupaciones en torno a la vigilancia digital, la censura en línea y la desigualdad de acceso a las tecnologías, sin dejar de lado la falta de regulaciones adecuadas y la limitada conciencia sobre los derechos digitales entre la población que contribuyen a una vulnerabilidad generalizada frente a posibles abusos por parte de diferentes actores.

Por otro lado, el reconocimiento y la defensa de los derechos digitales en Costa Rica también ofrecen oportunidades para fortalecer la democracia y la participación ciudadana en la era digital, la sociedad civil y los organismos de derechos humanos tienen un papel crucial en la promoción de políticas inclusivas y en la capacitación de la ciudadanía en el ejercicio responsable de sus derechos en línea.

El impulso de iniciativas que fomenten la transparencia, la rendición de cuentas y la protección de la privacidad se convierte en una necesidad apremiante para garantizar que el avance tecnológico no se traduzca en una merma de los derechos fundamentales de los ciudadanos costarricenses, es por ello que con la

aparición de la Agencia de Protección de Datos de los Habitantes (PRODHAB), el país ha ido logrando avanzar en estos temas a pasos cortos pero se han cumplido objetivo necesarios para evitar situaciones que compliquen el desarrollo de la globalización tecnológica en el país.

En Costa Rica existe la Agencia de Protección de Datos de los Habitantes (PRODHAB), una institución de desconcentración máxima adscrita al Ministerio de Justicia y Paz encargada de fiscalizar y regular las bases de datos de nuestro país, pudiéndose acudir a ella en caso de anomalías. relacionado con datos personales, quién actuará de oficio o a petición del interesado; (Rivera, 2019).

La existencia de la Agencia de Protección de Datos de los Habitantes (PRODHAB) en Costa Rica representa un avance significativo en la protección de la privacidad y los derechos digitales de los ciudadanos. El conocer y saber que la protección de datos es de interés universal para la población, es importante y más cuando existen entidades que brindan ese apoyo en pro de cuidar la integridad digital de las personas, en Costa Rica desde el 7 de abril del 2011, bajo la Ley N.º8968 la cual tiene por objetivo garantizar la protección de la información que poseen las personas ante organizaciones y entidades que tratan datos sobre las personas, logrando así una protección efectiva en sus derechos. Si bien es cierto, existen leyes que respaldan si alguien utiliza incorrectamente nuestros datos, se debe cuidar la información que comparte, ya a quién se le suministra debe de garantizar que no almacene ni trate datos de carácter persona, evitar que se expongan fotos en redes sociales y que no se proporcione a desconocidos la dirección de correo, con el fin de evitar suplantación de imagen, afectación de la misma y duplicidad de información en diferentes ámbitos sociales.

A menudo, los ciudadanos desconocen sus derechos en materia de privacidad digital o no saben cómo aplicarlos en pro de su protección ante la sociedad. Esta falta de educación y conciencia puede dificultar el proceso de

denuncia y desincentivar la participación activa de los ciudadanos en la defensa de sus derechos ante posibles abusos por parte de las entidades públicas o privadas que utilicen dicha información sin consentimiento, sabiendo que Código Penal, en la Sección VIII. sobre delitos informáticos y conexiones, artículos 230 y 231 menciona:

Artículo 230.- Suplantación de identidad: Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información.

Artículo 231.- Espionaje informático: Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. (Legislativa, 2012).

Hoy en día es fundamental que la PRODHAB no solo se enfoque en la aplicación de la ley y el código penal como tiene que ser, sino también en la sensibilización y la educación pública sobre la importancia de la protección de datos personales en la sociedad actual, ya que es fundamental para salvaguardar la privacidad y la seguridad en el entorno digital, a sabiendas que la efectividad de estas disposiciones puede verse comprometida por diversos factores, políticos, económicos y sociales.

Hoy en día es crucial fortalecer la capacidad técnica y de investigación de la PRODHAB, así como promover la cooperación internacional en la lucha contra los delitos informáticos, se necesita una mayor sensibilización y educación pública sobre los riesgos asociados con el uso de la tecnología y las mejores prácticas para proteger la privacidad y la seguridad en línea con el fin de abordar eficazmente la problemática del cibercrimen que se pueda dar en Costa Rica y así proteger los derechos digitales de sus ciudadanos.

Durante los últimos años las empresas y el estado se han visto afectados por

los ciberataques, los cuales se han visto en tener que reformar la forma de trabajar la protección de la identidad digital de las empresas, “Un 35 por ciento de pequeñas y medianas empresas (pymes) costarricenses que encuestadas en un estudio han experimentado problemas de ciberseguridad.” (Murillo, 2023), una de las principales dificultades que enfrentan las empresas y el estado en la protección contra ciberataques radica en la falta de recursos humanos y financieros dedicados a este fin. Muchas pymes carecen de personal capacitado en protección de datos y no cuentan con los presupuestos necesarios para implementar medidas robustas de protección de datos, el gobierno no se queda atrás la protección de datos administrados por el gobierno de gran población costarricense se vio sustraída por hackers donde “Desde el mes de abril de 2022, varias entidades gubernamentales costarricenses fueron víctimas de un ataque con ransomware por el grupo Conti, que sustrajo al menos un terabyte de datos del gobierno” (PwC, 2024). Ante esto y con la creciente incidencia de ciberataques en empresas y entidades gubernamentales en Costa Rica durante los últimos años ha generado una urgente necesidad de reformar las estrategias de protección de la identidad digital y los datos sensibles. Si bien es cierto que los avances tecnológicos han brindado numerosas oportunidades para el desarrollo económico y la eficiencia operativa, también han abierto la puerta a nuevas formas de amenazas cibernéticas que pueden tener repercusiones devastadoras para las organizaciones y la sociedad en su conjunto, considerando temas de inversión y de capacitación a corto y mediano plazo para las mejoras y protección de lo mencionado.

...0,06% del plan de gastos del gobierno central de \$12 billones es lo que recibirá el Ministerio de Ciencia y Tecnología (Micitt) para defender al país de los cibercriminales, a la vez que ya se registran un total de 674 intentos al mes de vulneración de los sistemas públicos. (Siles, 2022).

Como lo he mencionado: ¿puede mejorar el país? En determinadas ocasiones en diferentes conferencias de prensa se habla que el gobierno invierte en seguridad y protección de los datos digitales de las personas, pero si comenzamos a

investigar, es todo lo contrario “Para el 2023, el presupuesto para el Micitt y la atención de ciberseguridad será de unos ₡7.106 millones, es decir, uno de los más bajos del Estado.” (Siles, 2022). Si bien es cierto que las alianzas estratégicas pueden brindar beneficios significativos en términos de recursos técnicos y financiamiento, también plantean serias interrogantes sobre la dependencia del país de actores externos para resolver problemas internos de seguridad digital.

El panorama es aún más desalentador si se tiene en cuenta que la mayor esperanza del país sería únicamente apoyarse en la ‘buena voluntad’ de empresas privadas y diversos Gobiernos que deseen ayudar al país en el marco de eventuales alianzas estratégicas. (Siles, 2022).

El hecho de que el panorama para abordar los desafíos de Costa Rica en materia de ciberseguridad y protección de datos digitales de la población dependa en gran medida de la “buena voluntad” de empresas privadas y otros gobiernos refleja una preocupante falta de recursos y capacidad institucional para hacer frente a estas amenazas de manera efectiva. Esto puede dejar al país en una posición vulnerable, sujeta a las problemáticas de pérdida de información y datos sensibles, por ende, el país necesita desarrollar una estrategia integral y sostenible que combine la cooperación internacional con el fortalecimiento de las capacidades internas y la inversión en infraestructuras y sistemas de seguridad digital robustos. Solo de esta manera podrá garantizar la protección efectiva de sus datos, infraestructuras críticas y soberanía en el entorno digital.

Costa Rica se encuentra en una encrucijada donde la responsabilidad y la celeridad son imperiosas. Es fundamental que el Gobierno y los diversos sectores tomen medidas significativas y concretas para fortalecer la protección de datos y la implementación de la ciberseguridad en el país de una forma muy integral, abordando aspectos legales, inversiones relevantes y promoviendo la colaboración pública y privada. Aunque los desafíos persisten, se observan esfuerzos en aumento para elevar la conciencia, mejorar la capacidad de respuesta ante incidentes,

adoptar soluciones costo efectivas y fomentar la educación en ciberseguridad desde edades tempranas.

En conclusión, la compleja intersección entre la identidad virtual y los riesgos de la sociedad civil, es evidente que estamos inmersos en un paisaje digital en constante evolución, donde la seguridad y la privacidad son preocupaciones omnipresentes. La identidad virtual, en todas sus facetas, se ha convertido en un componente esencial de nuestras vidas, y los riesgos asociados con ella requieren una atención cuidadosa y continua.

Se conoce los desafíos que enfrentan las personas, las empresas y el gobierno, desde la exposición a la desinformación y la manipulación en línea hasta el acoso cibernético y la violación de la privacidad. Sin embargo, también hemos examinado las posibles soluciones y estrategias para abordar estos problemas, desde la educación digital hasta la implementación de medidas de seguridad más sólidas.

Por otra parte, es fundamental reconocer que la protección de nuestra identidad virtual y la mitigación de los riesgos sociales asociados no son responsabilidades exclusivas de los individuos, sino que también requieren la colaboración y el compromiso de gobiernos, empresas, organizaciones y la sociedad en su conjunto. Es a través de un enfoque holístico y colaborativo que podemos crear un entorno en línea más seguro, donde la diversidad, la inclusión y el respeto sean los pilares fundamentales.

“El panorama de ciberseguridad en Costa Rica refleja los desafíos y avances en la protección de la infraestructura tecnológica y la información sensible en el país.” (Lizano, 2023), La población debe aprender a llevar un debate sobre los derechos digitales en Costa Rica, no solo requiere con un enfoque crítico sobre las políticas y prácticas actuales, sino también con un compromiso activo de todos los actores sociales puedan construir un entorno digital más justo, inclusivo y

respetuoso de los derechos humanos, En este contexto, se hace evidente la necesidad de una estrategia integral y sostenible que combine la cooperación internacional con el fortalecimiento de las capacidades internas y la inversión en infraestructuras y sistemas de seguridad digital robusto.

Como navegantes en este mundo digital, es imperativo que sigamos siendo conscientes y proactivos en la protección de nuestra identidad virtual y en la promoción de una cultura digital responsable al educarnos, fortalecer nuestras habilidades digitales y abogar por políticas y prácticas que promuevan la seguridad y la privacidad en línea, podemos construir un futuro digital más resiliente y empoderado para todos.

En última instancia, al enfrentar los riesgos de la sociedad civil en el contexto de la identidad virtual, estamos llamados a actuar con determinación y solidaridad. Juntos, podemos navegar hacia un futuro digital donde nuestras identidades estén protegidas, nuestros derechos sean respetados y nuestra sociedad sea más fuerte y más justa que nunca.

Referencias bibliográficas

- a. Lecuit, J. (17 de marzo de 2020). REAL INSTITUTO ELCANO. Obtenido de Identidad digital y seguridad online:
<https://www.realinstitutoelcano.org/analisis/identidad-digital-y-seguridad-online/>
- b. Legislativa, A. (10 de julio de 2012). Sistema Costarricense de Información Jurídica. Recuperado el 27 de febrero de 2024, de Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048:
https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=73583
- c. López, J. (23 de diciembre de 2022). Identidad Digital, ¿qué es y por qué es tan importante? Obtenido de Forbes México: <https://www.forbes.com.mx/identidad-digital-que-es-y-por-que-es-tan-importante/>
- d. Martínez V., Rincón E. (diciembre de 2021). Revista chilena de derecho y tecnología. Obtenido de Problemas y desarrollo de la identidad en el mundo digital: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842021000200251
- e. Medrano, J. (2022). Hacia el reconocimiento de los derechos digitales en Costa Rica. En PROSIC, Hacia la sociedad de la información y el conocimiento (págs. 314- 384). San José: UCR.
- f. Murillo, E. (5 de abril de 2023). Costa Rica | 35% de pymes nacionales ha experimentado problemas de ciberseguridad. Obtenido de DPL News:
<https://dplnews.com/costa-rica-35-de-pymes-nacionales-ha-experimentado-problemas-de-ciberseguridad/>
- g. Pc. (1 de marzo de 2024). Ciberataque paraliza numerosos sistemas de TI en Costa Rica y otros países de América Latina. Obtenido de PwC Interaméricas:
<https://www.pwc.com/ia/es/prensa/Ciberataque-que-paraliza-numerosos-sistemas-de-TI-en-Costa-Rica.html>
- h. Quirós, A. (2018). La Identidad Virtual Frente a los Riesgos de la Sociedad Digital. En PROSIC, Informe Hacia la Sociedad de la Información y el Conocimiento 2018 (págs. 309-341). San José: UCR.
- i. Rivera, V. (7 de mayo de 2019). Realidad sobre la Privacidad de los Datos Personales en Costa Rica. doi:<http://dx.doi.org/10.15517/eci.v9i2.37503>

- j. Santander, B. (14 de febrero de 2023). ¿Qué es la identidad digital? Obtenido de Banco Santander: <https://www.santander.com/es/stories/que-es-la-identidad-digital#:~:text=La%20identidad%20digital%20es%20el,acerca%20de%20nosotros%20en%20Internet> .
- k. Siles, A. (28 de noviembre de 2022). Debilidad de Costa Rica en ciberseguridad hará de instituciones públicas un blanco de ataque para hackers en 2023. Obtenido de La República: <https://www.larepublica.net/noticia/debilidad-de-costa-rica-en-ciberseguridad-hara-de-instituciones-publicas-un-blanco-de-ataque-para-hackers-en-2023>.