

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

[DOI 10.35381/cm.v12i1.2098](https://doi.org/10.35381/cm.v12i1.2098)

Ciberseguridad frente al derecho y la protección a los ataques digitales

Cybersecurity versus the law and protection against digital attacks

Jadira Jessenia Cesen-Vimos
jadiracv74@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador

<https://orcid.org/0009-0007-2934-9598>

Eliana Marisol Chuquimarca-Paguay
elianacp23@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador

<https://orcid.org/0009-0008-2855-5178>

Valeria Estefanía Vicuña-Pozo
ur.valeriavp84@uniandes.edu.ec
Universidad Regional Autónoma de Los Andes; Riobamba; Chimborazo
Ecuador

<https://orcid.org/0000-0002-1883-8384>

Recepción: 15 de diciembre 2025
Revisado: 26 de febrero 2026
Aprobación: 15 de marzo 2026
Publicado: 01 de abril 2026

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

RESUMEN

El objetivo de la presente investigación fue prevenir a la sociedad frente a los ataques cibernéticos y dar a conocer sus debidos derechos frente a la seguridad digital. Metodológicamente, se utilizó el método descriptivo ya que se no busca manipular las variables, pero si proporciona dediciones claras y concretas en aquel tema a investigar. En los resultados, se logró evidenciar que la ciberseguridad es un problema global que requiere la colaboración de diferentes entidades como los gobiernos, corporaciones y personas. La ausencia del trabajo en conjunto puede provocar vulnerabilidades y ciberataques. Es esencial que se desarrollen normas de seguridad uniformes y se intercambien datos y herramientas. En conclusión, global la ciberseguridad frente al derecho aboga por una protección integral que complemente medidas técnicas como un marco jurídico que garantice la protección de los derechos y la integridad frente a los ataques digitales.

Descriptores: Cibernética; delito informático; protección de datos; digitalización; norma jurídica. (Tesauro UNESCO).

ABSTRACT

The objective of this research was to warn society about cyberattacks and raise awareness of their rights regarding digital security. Methodologically, the descriptive method was used, as it does not seek to manipulate variables but provides clear and concrete decisions on the topic under investigation. The results showed that cybersecurity is a global problem that requires the collaboration of different entities such as governments, corporations, and individuals. The absence of joint efforts can lead to vulnerabilities and cyberattacks. It is essential to develop uniform security standards and exchange data and tools. In conclusion, global cybersecurity in relation to law advocates comprehensive protection that complements technical measures, such as a legal framework that guarantees the protection of rights and integrity against digital attacks.

Descriptors: Cybernetics; computer crime; data protection; digitization; legal norm. (UNESCO Thesaurus).

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

INTRODUCCIÓN

La ciberseguridad se convirtió en una de las áreas más relevantes en la época actual, donde la digitalización de todos los aspectos de la vida cotidiana que dio lugar a una mayor exposición a riesgos y ataques cibernéticos. En el proceso, el derecho juega un papel crucial para garantizar la protección de la sociedad y las organizaciones frente a las amenazas digitales. La integración de la ciberseguridad con el marco legal era esencial para proteger la privacidad, la integridad de los datos y la seguridad de las infraestructuras críticas.

El enfoque no solo nos permite ver los impactos de los ataques cibernéticos, sino también establecer mecanismos de respuesta concretas, alineados con los principios éticos y los derechos fundamentales, como la protección de los datos personales el incremento de los delitos digitales exige una cooperación eficaz entre las autoridades jurídicas y los expertos en tecnología ofrecieron una protección efectiva en el entorno digital, de tal manera que se brindó más seguridad a la sociedad.

La ciberseguridad ha adquirido una importancia crucial en la actualidad debido al incremento de los ataques digitales, el robo de datos y los cibercrímenes. La protección en el entorno digital se ha convertido en un derecho fundamental para la seguridad de individuos, empresas y gobiernos, haciendo necesario un marco legal sólido que regule y proteja frente a estos ataques (Tapia Hernandez, Canizales Ruiz y Vega Paez, 2021).

El RGPD. Es la fuerza legislativa establecida para proteger los derechos de cuya información personal y sensible se almacena en las organizaciones, pueden solicitar acceso a su información personal, así como solicitar que una organización destruya su información personal. Este reglamento afecta a casi todos los sectores (Utimaco, s.f.). La importancia de este artículo es ver la relación entre la ciberseguridad y el derecho, en el marco legal es un pilar fundamental para los ataques digitales, ya que las leyes deben ser actualizadas constantemente para enfrentar nuevas amenazas dado el incremento de ciberataques a nivel global.

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

En ese sentido, es necesario que las personas conozcan las amenazas a las que se exponen en el entorno virtual, así como la vulneración a los derechos en específico que ocasionan cada una de éstas, con la finalidad de que su uso sea responsable y tomen acciones preventivas, en aras de proteger y salvaguardar sus derechos humanos y en consecuencia la seguridad en entornos digitales (Tapia Hernández, Canizales Ruiz y Vega Paez, 2021).

Existe diferentes tipos de ataques cibernéticos maliciosos. Esos pueden afectar tanto a computadoras como a dispositivos móviles sin que los usuarios se den cuenta. En primer lugar, se encuentran los malware. Este es un software que se instala sin autorización y puede causar daño al sistema. Otro ataque muy común es el phishing. Es una forma de ingeniería social en la que los hackers intentan engañar a los usuarios y Así obtienen sus contraseñas y otros datos personales (Ramírez, 2023).

Por esta razón se le anticipa a la sociedad cambiar las claves de sus cuentas regularmente y actualizar constantemente las alertas de seguridad de los sistemas de software. Ingresar a paginas seguras y verificar que no contenga ningún tipo de virus, de esta manera evitaremos todo tipo de hackeos y amenazas dirigidas hacia las personas y puedan tener la tranquilidad al momento de navegar en redes. En función de antes expresado, surge la siguiente investigación que tiene como objetivo general analizar la evolución histórica y el reconocimiento normativo de la ciberseguridad en diferentes ámbitos y aspectos, identificando las principales leyes y macos jurídicos implementados para proteger los ataques digitales y cuan efectivo son las leyes actuales para proteger la privacidad y los datos personales de la sociedad.

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

MÉTODO

En la presente investigación se aplicó la metodología descriptiva e histórica ya que se enfocó en proporcionar definiciones claras y concretas pues se utilizaron elementos de carácter doctrinal como los elementos teóricos, revisión bibliográfica, leyes, estudios académicos y casos relevantes sobre ciberseguridad desde la perspectiva del derecho y la protección frente a ataques digitales así comprenderemos a fondo este artículo y cuál es la importancia en la actualidad; no busca manipular las variables pero si se basa en observar y registrar detalladamente. La técnica de análisis de contenido en este artículo se basa en revisar de manera sistemáticas y detallada los documentos legales , informes técnicos, artículos académicos y cuestiones prácticas relacionadas con la ciberseguridad y la protección legal gracias a esta técnica podremos determinar los modelos, tendencias permitiendo extraer conclusiones sobre la efectividad de las medidas implementadas además permite detectar que aspectos de la seguridad digital necesita mejora y como las regulaciones pueden adaptarse a garantizar una mejor protección a la privacidad de las personas.

RESULTADOS

Se define la ciberseguridad como un conjunto de procesos y tecnologías diseñadas con el objetivo de proteger programas, ordenadores, redes de comunicación y también datos ante ataques, y/o accesos no autorizados, asegurando de esta manera la confidencialidad, integridad y disponibilidad de los sistemas. A pesar de que no es posible garantizar una seguridad total, la ciber-seguridad tiene como objetivo evitar los ataques maliciosos, reducir la vulnerabilidad de la información consecuencia de errores propios y paliar los daños ocasionados como consecuencia de estos según (Estevan, 2021).

La ciberseguridad o también conocida como la seguridad digital, son herramientas que ayudan a proteger la información digital contra ataques cibernéticos esto incluye datos personales, cuentas, archivos y fotos estos tienen tres pilares fundamentales

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

los cuales son: Confidencialidad eso abarca que los datos del usuario solo deben obtener personas autorizadas. Integridad eso se trata de que la información no debe ser manipulada ni cambiada sin su autorización. Acceso puede ser en casos concretos cuando en verdad sea necesario ese tipo de información.

En la era digital que vivimos la seguridad informática se ha convertido en un tema de vital importancia tanto para las organizaciones como para los individuos esto influye, pero no se limita la implementación de medida técnicas, procesos y políticas que garantizan la seguridad digital con esto podemos acceder al internet de forma segura. Importancia de la seguridad digital prevenir los ataques maliciosos como el phishing, ransomware, malware ya que afectan negativamente el cumplimiento legal esto nos ayuda a regular la información para evitar sanciones legales y proteger la privacidad de los usuarios.

La protección de la reputación es esencial ya que es clave mantener una buena imagen pública. Esto no solo es responsabilidad de las empresas sino también de las personas que tiene un papel fundamental en la protección de sus datos por ello hay diversos consejos prácticos como las claves complejas, mantener tus dispositivos y softwares actualizados, ser precavidos con los enlaces y correos sospechosos, evitar las redes de wifi publicas sin protección. Con estas indicaciones podrás reconocer, analizar de manera más cercana los riesgos asociados de la ciberseguridad.

La evolución de la ciberseguridad ha ido de la mano de los avances en las tecnologías de la comunicación. A medida que pasamos de los telégrafos a los teléfonos inteligentes, también lo han hecho los tipos de ciberataques, desde el gusano Morris hasta el avanzado Stuxnet y, más recientemente, el ransomware Snake. Hemos recorrido un largo camino desde cifrados simples hasta algoritmos sofisticados, todo para proteger los datos y la comunicación. Si bien es casi imposible describir todos los incidentes que dieron forma al desarrollo de la ciberseguridad tal como la conocemos hoy, los siguientes son algunos de los momentos cruciales que no deben pasarse por alto (ManageEngine Log 360, 2025).

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

Gracias a los algoritmos de capacitación automáticos efectivos y excelentes, la inteligencia artificial en aplicaciones de ciberseguridad, las amenazas prácticas se pueden encontrar en tiempo real y reaccionar automáticamente a los incidentes y la mejora continua. Los motores que correlacionan las amenazas efectivas que encuentran sus primeras etapas se volverán más sofisticados, como la primera defensa de la organización. Al observar estas etapas de seguridad cibernética, está claro que la imagen panorámica de la amenaza se está desarrollando constantemente.

Los ciberdelincuentes aumentan en la complejidad y la escala. La protección de datos y la seguridad de la infraestructura tecnológica requieren un enfoque más positivo mediante el uso de tecnologías avanzadas como la IA ya que esta permite un acceso rápido a dicha información requerida, junto con estrategias de defensa confiables. Cuando las amenazas de la organización de desarrollo, debe adaptarse rápidamente a sí mismas contra nuevas formas de ataques, mientras que todavía están invirtiendo en nuevos talentos y tecnologías.

La ciberseguridad y su reconocimiento normativo

La ciberseguridad se define como el conjunto de estrategias, tecnologías, procesos y normativas destinadas a proteger sistemas, redes y datos contra ataques cibernéticos. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información en entornos digitales. La seguridad de la red ha cambiado del concepto técnico al problema principal en el campo de la gestión empresarial y la protección de datos globales, contribuyendo al desarrollo de reglas y marcos legales para el reconocimiento y el control. Debido a que se volvió más complicado, los gobiernos y las organizaciones internacionales han implementado reglas y estándares para garantizar una protección de la información.

El reconocimiento de los recursos normativos en el campo de la ciberseguridad se refiere a las normas y regulaciones de acuerdo con la ley y las regulaciones sobre la gestión de las prácticas avanzadas, identificando los requisitos de seguridad y la

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

determinación de las obligaciones legales. Estas reglas no solo se centran en prevenir los ataques, sino también en las respuestas a los incidentes y proteger los derechos del usuario. El diagnóstico de seguridad cibernética es la clave para establecer una base coherente y efectiva, lo que permite a las organizaciones proteger contra la ciberseguridad y observar las expectativas legales y éticas. (Szabo, 2024).

Aunque las normas del Código Orgánico Integral Penal (COIP) y la Ley Orgánica de Protección de datos personales actuales son de importancia básica para aumentar la seguridad digital, es necesario actualizar y adaptarse constantemente al rápido desarrollo de amenazas y tecnología (Asamblea Nacional de Ecuador, 2014; Asamblea Nacional de Ecuador, 2021). El reconocimiento normativo de la ciberseguridad implica la incorporación de regulaciones y marcos legales que establecen medidas de prevención, detección y respuesta ante amenazas digitales. A nivel internacional, organismos como la Unión Europea, la Organización de las Naciones Unidas (ONU) y la Organización de Estados Americanos (OEA) han promovido normativas para fortalecer la protección digital.

Derecho a la protección de datos personales y privacidad

El derecho a proteger los datos y la seguridad personales es el principio básico en el campo de los derechos humanos y la seguridad de la red, que ha sido apoyado durante décadas del desarrollo de tecnologías digitales y la recolección de bienes. Esta ley tiene como objetivo proteger sus datos personales contra el uso ilegal, el mal uso o el acceso ilegal, asegurando que los datos estén controlados por seguridad y a la voluntad de todos. Esta ley se refiere a las capacidades de las personas para controlar cómo se recopilan, archivan, procesan y difunden por sus datos personales.

Que, el artículo 66 numeral 19 de la Constitución de la República reconoce garantiza a las personas: 19. El derecho a la protección de datos carácter personal, como su correspondiente protección. La recolección, archivo, procesamiento, distribución o

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

difusión de estos datos personales requerirán la autorización del titular o el mandato de ley (Asamblea Nacional Constituyente, 2008; Asamblea Nacional del Ecuador, 2021).

El marco legal en el Ecuador ha tomado medidas importantes para ayudar a proteger la privacidad y los datos personales. Los datos personales incluyen toda la información que puede identificar a una persona como nombre, dirección, datos bancarios, historial de enfermedades, información laboral. Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021): Esta ley, en proceso de implementación, establece las bases para la regulación del tratamiento de datos personales, tanto en el sector público como privado.

Por su parte, en el Código Orgánico Integral Penal (COIP), se tipifican los delitos informáticos, como el robo de datos personales o el acceso no autorizado a sistemas de información. Este marco penal refuerza la protección contra los ataques digitales (Asamblea nacional del Ecuador, 2021). Conformación de la Agencia de Protección de Datos Personales: En Ecuador, se ha creado una Agencia Nacional de Protección de Datos Personales que será responsable de velar por el cumplimiento de la ley, así como de garantizar que las entidades que manejan datos personales respetan los derechos de los ciudadanos.

Los marcos, como GDPR es una normativa europea que proporcionan a las personas más control de su información, pero el logro tecnológico aún representa nuevos problemas que requieren un enfoque dinámico y actualizado para garantizar la seguridad de los datos. Establece principios claves como el consentimiento informado, la transparencia, la seguridad de los datos y el derecho de acceso, rectificación y cancelación de estos por parte de los titulares de los datos.

DISCUSIÓN

La ciberseguridad es un problema global que requiere la colaboración de diferentes entidades como los gobiernos, corporaciones y personas. La ausencia del trabajo en conjunto puede provocar vulnerabilidades y ciberataques. Es esencial que se

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

desarrollen normas de seguridad uniformes y se intercambien datos y herramientas. El trabajo conjunto también puede ser útil para evitar ataques y minimizar las repercusiones financieras. Así mismo, la colaboración entre naciones es vital para luchar contra la delincuencia digital. La formulación de normativas y regulaciones comunes puede ayudar a salvaguardar los derechos en el entorno digital.

La falta de legislación y regulación de la ciberseguridad en Latinoamérica es sumamente importante para la protección de los derechos de los ciudadanos, según un estudio de la Organización de Estados Americanos (OEA), solo el 40% de los países tienen leyes y regulaciones específicas para combatir los delitos cibernéticos. Es esencial desarrollar marcos legales robustos y eficaces para salvaguardar la información personal y la privacidad de los individuos, aunque esto se enfrenta a numerosos retos, tanto en el ámbito técnico como legal.

A pesar de que Ecuador ha hecho progresos mediante la creación de la Ley Orgánica de Protección de Datos Personales y la inclusión de delitos cibernéticos en el Código Orgánico Integral Penal, la rapidez con que surgen nuevas amenazas digitales pone en cuestión la habilidad de estas legislaciones para adaptarse y seguir siendo eficaces. Las entidades encargadas de hacer cumplir estas leyes necesitan tener acceso a las herramientas adecuadas y a la formación necesaria para actuar rápidamente ante incidentes de seguridad y ajustarse a las nuevas estrategias de ataque.

Así mismo, hay una desconexión entre la legislación y su aplicación real. Las organizaciones tanto públicas como privadas todavía se enfrentan a obstáculos para cumplir con los requerimientos de seguridad y protección de datos, debido a la carencia de infraestructura tecnológica, financiamiento y personal especializado. La falta de una cultura de seguridad digital agrava este asunto, ya que muchos usuarios y trabajadores ignoran las medidas básicas para defenderse de ataques, como crear contraseñas seguras o detectar intentos de phishing.

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

Los ciberataques no conocen límites geográficos, La implementación creciente de tecnologías innovadoras, como la inteligencia artificial y el Internet de las Cosas, introduce nuevos retos para la ciberseguridad en el ámbito legal, por lo que es crucial que los países y organismos globales colaboren para identificar y detener a quienes cometen estos delitos. Sin embargo, la diversidad en las regulaciones y la ausencia de acuerdos internacionales complican esta coordinación.

Otro asunto importante es encontrar un balance entre la seguridad y la privacidad. Las estrategias de ciberseguridad, como la supervisión y la recopilación de datos, pueden chocar con los derechos de privacidad y la protección de datos personales. El objetivo se centra en cómo lograr una seguridad efectiva sin infringir los derechos básicos de las personas, lo que demanda un marco legal claro y la vigilancia de entidades independientes, para recolectar y manejar grandes cantidades de información incrementa el riesgo de ataques y brechas lo que exige una constante revisión de las leyes y protocolos de seguridad.

Además, la seguridad en el ciberespacio en relación con la legislación y la defensa contra agresiones digitales necesita una mezcla de leyes firmes, una tecnología altamente desarrollada, una cultura de protección sólida y una colaboración eficaz tanto a nivel nacional como global. La adaptación constante a las amenazas emergentes y la salvaguarda de los derechos esenciales serán elementos claves para asegurar un ámbito digital seguro y confiable al momento de navegar en internet, o descargar las diversas aplicaciones existentes.

Una de las principales sugerencias es la necesidad de actualizar y adaptarse constantemente las leyes para abordar las nuevas amenazas tecnológicas, ya que los ciberdelincuentes emplean nuevas técnicas cada vez más sofisticadas, también se sugiere a la sociedad cambiar con frecuencia sus contraseñas. Además, se recomienda promover la cooperación internacional, dado que los ataques cibernéticos a menudo cruzan fronteras, lo que requiere una respuesta coordinada entre gobiernos y organizaciones.

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

CONCLUSIONES

En un entorno cada vez más digital, la ciberseguridad se ha convertido en una prioridad tanto a nivel técnico como legal. Los ataques digitales no solo amenazan la integridad de los sistemas y los datos, sino que también encuentran problemas importantes en el campo de los derechos básicos, como la seguridad y los datos personales. En el ámbito de inversión de la ciberseguridad en América Latina es notablemente baja en comparación de otras partes del mundo, un informe del programa ciberseguryty ventures indico que el año 2020 la inversión en este sector alcanzo solo \$1.400 millones, lo que esto equivale apenas el 2% de inversión global en ciberseguridad. Es extremadamente importante que las regulaciones y los políticos en el campo de la ciberseguridad se adapten a la velocidad que realizan las tecnologías, garantizan una protección efectiva sin violar los derechos del usuario.

Gracias al enfoque interdisciplinario, que combina innovaciones tecnológicas con las regulaciones apropiadas, realmente puede proteger contra ataques digitales, tanto la protección de infraestructura importante como los derechos básicos de las personas para el ciberespacio. Es por eso que lo extremadamente importante es desarrollar mecanismos de cooperación entre organizaciones que le permitan enviar información y recursos entre las organizaciones participantes. Del mismo modo, no hay suficiente capacitación profesional de empleados de la corte en el campo de la seguridad cibernética, enfatizando la necesidad de realizar capacitación y actualizaciones profesionales.

Finalmente, un enfoque holístico que combine la ciberseguridad con el respeto a los derechos humanos es indispensable para preservar la confianza pública en el ciberespacio. El derecho a la privacidad y a la protección de datos debe ser un principio rector, incluso en la implementación de medidas de seguridad más estrictas. La ciberseguridad no solo es una cuestión de defensa técnica, sino también de equilibrio entre la protección de la infraestructura digital y el respeto a las libertades individuales. En este sentido, un marco legal bien estructurado, que se

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

base en la transparencia, la justicia y la equidad, es fundamental para construir un entorno digital más seguro y respetuoso con los derechos humanos.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A la Universidad Regional Autónoma de los Andes, en el desarrollo de esta investigación.

REFERENCIAS CONSULTADAS

Arollo et al. (2020). Ciberseguridad. Madrid: CSIC. <https://n9.cl/2c204>

Asamblea Nacional Constituyente del Ecuador (2008). Constitución De La Republica Del Ecuador 2008. *Registro Oficial 449 de 20-oct-2008*, Quito, Ecuador. <https://n9.cl/hd0g>

Asamblea Nacional de Ecuador. (2014). Código Orgánico Integral Penal, Quito: Lexis. <https://n9.cl/s1o44>

Asamblea Nacional de Ecuador.(2021). Ley Organica de Proteccion de Datos Personales .Quito: Registro Oficial Suplemento 459. <https://n9.cl/mv7ow>

Estevan, J. L. (2021). Avances recientes en la aplicacion de la ciencia de datos a la ciberseguridad industrial . *Tecnologia de las comunicaciones*, 1. <https://n9.cl/0g4oh>

ManageEngine Log 360. (2025). Blogs de ciberseguridad . Obtenido de Evolucion e historia de la ciberseguridad :Una breve cronologia. <https://n9.cl/10c4fu>

Ramirez, k. (2023). Ciberseguridad: protege tus datos personales en la era digital. *coneccion PUCE*. <https://n9.cl/b24zy>

Szabo, M. (2024). *welivessecurity*. Obtenido de cumplimiento de las normativas en ciberseguridad. <https://n9.cl/vfmic>

Jadira Jessenia Cesen-Vimos; Eliana Marisol Chuquimarca-Paguay; Valeria Estefanía Vicuña-Pozo

Tapia Hernandez,E. ; Canizales Ruiz.R. y Vega Paez,A. (2021). Importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Mision juridica*, 4. <https://n9.cl/2cd1o>

Universidad Europea . (2025). Tipos de ataques Ciberneticos y como prevenirlos *Universidad Europea*. <https://n9.cl/o995hb>

Utimaco. (s.f.). ¿Qué es el Reglamento General de Protección de Datos (RGPD)?.utimaco. <https://n9.cl/ow9kk>

ZPEDIA. (2025). ¿Qué es la protección contra amenazas cibernéticas? *zsca/er*. <https://n9.cl/lkzqt>