Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

Universidad Pedagógica Experimental Libertador
Vicerrectorado de Investigación y Postgrado
Instituto Pedagógico "Rafael Alberto Escobar Lara"
Subdirección de Investigación y Postgrado

DESAFÍOS Y ESTRATEGIAS DE SEGURIDAD DIGITAL PARA COMBATIR LA CIBERCRIMINALIDAD EN EL PERÚ

Autor: Eber Geisel Trujillo Vega
etrujillove13@ucvvirtual.edu.pe
https://orcid.org/0000-0001-5995-5774
Universidad César Vallejo
Lima - Perú

PP. 130-147

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

DESAFÍOS Y ESTRATEGIAS DE SEGURIDAD DIGITAL PARA COMBATIR LA CIBERCRIMINALIDAD EN PERÚ

Autor: Eber Geisel Trujillo Vega
etrujillove13@ucvvirtual.edu.pe
https://orcid.org/0000-0001-5995-5774
Universidad César Vallejo
Lima - Perú

Recibido: Julio 2024 **Aceptado:** Noviembre 2024

Resumen

En la actualidad, la cibercriminalidad se ha convertido en un problema apremiante en Perú, afectando a ciudadanos, empresas y gobiernos por igual. Las diversas formas en las que se pueden cometer delitos informáticos requieren una revisión de los desafíos que estos representan para pensar en las estrategias de seguridad que se pueden implementar. Esta investigación consistió en revisar sistemáticamente documentos en la web, siguiendo dos criterios de selección: primero, documentos centrados en la temática de la seguridad digital; y segundo, información sobre la cibercriminalidad en Perú. Posteriormente, los documentos fueron procesados por medio de una hermenéusis que cubrió tres dimensiones: lectura, explicación y traducción. Las conclusiones iniciales indican que existen tres elementos desafiantes: la brecha digital, la insuficiente alfabetización digital y la actualización desacelerada en Perú de la legislación que protege contra estos delitos, en comparación con la velocidad en la que evolucionan las amenazas.
Palabras clave: Legislación cibernética, brecha digital, alfabetización digital, cibercriminalidad.

DIGITAL SECURITY CHALLENGES AND STRATEGIES TO FIGHT CYBERCRIMINALITY IN PERU

Abstract

Today, cybercrime has become a pressing problem in Peru, affecting citizens, companies and governments alike. The various ways in which cybercrimes can be committed require a review of the challenges they represent to think about the security strategies that can

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

be implemented. This research consisted of systematically reviewing documents on the web, following two selection criteria: first, documents focused on the topic of digital security; and second, information about cybercrime in Peru. Subsequently, the documents were processed through a hermeneusis that covered three dimensions: reading, explanation and translation. The initial conclusions indicate that there are three challenging elements: the digital divide, insufficient digital literacy and the slowed updating in Peru of the legislation that protects against these crimes, compared to the speed at which the threats evolve.
Key words: Cyber legislation, digital gap, digital literacy, cybercrime.

Introducción

La globalización y los acelerados avances tecnológicos que se viven en el presente siglo XXI, han venido acompañados de grandes progresos, pero también de enormes desafíos. Uno de ellos está enmarcado en las acciones ilícitas que pueden cometerse por medio de cualquier dispositivo tecnológico que esté conectado a la Web. El borrador de la convención contra la ciberdelincuencia, establecido por la Asamblea General de las Naciones Unidas en este año 2024, indica que la tecnología "ha creado oportunidades para que los delitos adquieran mayor escala, velocidad y alcance, desde el terrorismo hasta el tráfico de drogas, la trata de personas, el tráfico ilícito de migrantes, el tráfico de armas de fuego, entre otros" (Naciones Unidas, 2024; s/p).

Pensar en los desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en el Perú, lleva, en primer lugar, a establecer algunas definiciones, para esclarecer la intencionalidad del presente artículo. En principio, se puede develar qué significa criminalidad. La Real Academia de la Lengua Española (RAE, 2024), define la criminalidad como aquella "cualidad o circunstancia que hace que una acción sea criminal" (s/p), entendiendo que esta última es, una acción indebida o censurable. Luego, se puede especificar a qué se hace referencia cuando se habla de cibercriminalidad; Kaspersky (2024), una empresa privada internacional de ciberseguridad, la define como "una actividad delictiva que se dirige a una computadora, una red informática o un dispositivo en red, o bien que utiliza uno de estos elementos" (s/p), ya sea para ganar dinero, para dañar computadoras o redes y/o por razones distintas en las que no se ataca

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

para la obtención de dinero de forma ilegal, sino por motivos políticos, personales o de cualquier otra índole.

Aclarados los términos anteriores, es fundamental destacar el elemento generador de interés de estudio del presente artículo. Partiendo de que, América Latina y el Caribe es una de las regiones más atacadas del mundo debido al estado actual de su ciberseguridad, causado por variados factores como la falta de estándares y regulaciones sumado a la ausencia de una cultura o educación sobre seguridad cibernética en los usuarios, en un contexto caracterizado por la escasez de profesionales cualificados y de recursos que se inviertan en tecnologías de seguridad, han convertido esta región en una zona especialmente vulnerable a las ciberamenazas y ha motivado a realizar una revisión específica en el Perú para que, en virtud de reconocer los desafíos que enfrenta esta región latinoamericana, se puedan vislumbrar algunas estrategias de seguridad digital y acciones educativas que permitan combatir la cibercriminalidad.

Marco Teórico

Delincuencia y Seguridad Ciudadana en Perú

La Encuesta Nacional de Programas Presupuestales, ejecutada por el Instituto Nacional de Estadística e Informática (INEI, 2024) en coordinación con el Ministerio de Economía y Finanzas, que tiene como tema principal la *Seguridad Ciudadana* y como propósito conocer si la población de 15 y más años de edad, ha sido víctima de algún hecho delictivo o tiene la percepción de inseguridad, publicado en el boletín de julio de 2024, deja ver que el "86,1% de la población del área urbana a nivel nacional percibe que en los próximos doce meses puede ser víctima de algún hecho delictivo que atente contra su seguridad" (p. 69); siendo importante destacar que "comparando con los similares semestre móviles enero - junio 2022 y enero - junio 2023, la percepción de inseguridad por estafa aumentó en 9,5 y 7,6 puntos porcentuales respectivamente" (p. 77). Significando, que un alto porcentaje de los ciudadanos peruanos, se sienten susceptibles de ser estafados o afectados por la criminalidad en su país.

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

Además, este mismo documento expresa que la población urbana a nivel nacional, víctima de algún hecho delictivo que realizó la denuncia fue de apenas «16,7% y explica que la población que no denuncia es por considerar que "Es una pérdida de tiempo" (48,1%), seguido de la razón "Desconoce al delincuente" (18,0%) y, también, porque "Desconfía de la policía" (13,8%)» (INEI, 2024, p. 47); a sabiendas que factores como la falta de recursos en las fuerzas del orden, la corrupción y la desigualdad económica contribuyen al aumento del crimen.

Según las estadísticas, más del 70% de los peruanos encuestados desconfían de la PNP (77.5%), del Poder Judicial (79.3%) y del Ministerio Público (74.8%) (Trinidad, 2024). Es así como, la criminalidad en la seguridad ciudadana es un desafío significativo que afecta a países latinoamericanos como el Perú, siendo un problema que incluye crimen organizado, narcotráfico, violencia callejera y diversos delitos amenazantes de la estabilidad social y económica. En este contexto, según números oficiales, provenientes del Instituto Nacional de Estadística e informática (INEI), elaborado en el 2021, un aproximado de 35 distritos fiscales del país acumuló más de 4.700 denuncias por extorsión, una cifra 64,6% más alta que las del 2020; demostrando el franco aumento, año tras año de los delitos cometidos en el país.

Ciberdelitos en Perú

De la amplia gama de delitos que son susceptibles de estudio en la región peruana, este artículo se limita a exponer aquellos que son producidos a través de los medios tecnológicos. Así, los tipos de ciberdelitos más comunes que se realizan en Perú, expuestos en el portal Gob.pe (2024) del Estado Peruano, y a los que se hacen referencia en este estudio, son: el *Phishing* (envío de correos electrónicos con mensajes fraudulentos que se hacen pasar por instituciones o empresas confiables con el objetivo de obtener información personal y financiera de las víctimas, como contraseñas y datos bancarios); *Vishing* (combina información obtenida previamente por internet con una llamada telefónica fraudulenta); *Smishing* (ocurre por mensaje de texto o por WhatsApp, cuando el delincuente se hace pasar por un banco, alerta sobre una compra sospechosa con la

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

tarjeta de crédito y solicita los datos bancarios); *Carding* (estafa a través de la obtención de los datos de la tarjeta de crédito para realizar compras *online*); *Pharming* (utilización de malware o software malicioso para redireccionar a los usuarios hacia versiones falsas de sitios web y obtener así sus datos personales); *Keylogging* (spyware o software malicioso oculto que se introduce en el ordenador o en el smartphone y registra en secreto lo que se escribe, obteniendo información de cuentas y otros datos personales); *Sniffing* (conexión a través de una red Wi-Fi que no está protegida ni cifrada, por medio de la cual los *hackers* roban los datos al rastrear el tráfico de internet con herramientas especiales.

También, es necesario mencionar otra terminología usada para hacer referencia a los delitos de ciberdelincuencia como son: *Ransomware* (secuestro de datos de un sistema informático, a través de la encriptación, a cambio de un rescate económico); *Fraudes electrónicos* (engloba, desde compras fraudulentas en línea hasta la clonación de tarjetas de crédito); *Suplantación de identidad* (ciberdelincuentes que se hacen pasar por otra persona para cometer fraudes o delitos); *Difusión de contenido ilícito* (contenido pornográfico infantil, amenazas, calumnias y difamación a través de las redes sociales); y, *Ataques a sistemas informáticos* (para robar información confidencial, sabotear operaciones o causar daños a la infraestructura digital). Siendo, a nivel latinoamericano, Brasil, Colombia, México y Perú, los países que sufren más ciberacoso, a través de Ransomware, Malware, Troyanos bancarios, Phishing, Malware móvil, y Spyware (Obando, 2024).

En este sentido, Forbes (2024) publicó que, según Fortinet, el Perú sufrió 5.000 millones de intentos de ciberataques en el año 2023, cifra menor al año anterior pero significativa, sobre todo porque es un indicativo de que han disminuido los ataques masivos pero, ha aumentado el "volumen de explotaciones únicas y variantes nuevas de malware y ransomware que son mucho más dirigidos" (s/p), queriendo decir, que los ataques realizados son para objetivos específicos, siendo más sofisticados y con mayor posibilidad de éxito, sobre todo si las empresas u organizaciones atacadas no cuentan con defensas de ciberseguridad integradas, automatizadas y actualizadas. Al respecto, Obando (2024) afirma que "los malware siguen siendo los principales ciberataques, sobre todo

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

mediante archivos de Office como lo son Excel, Word y PowerPoint. Este tipo de ataques de ciberseguridad representan cerca del 50%" (s/p). De ahí la importancia de pensar y actuar en la búsqueda de las estrategias de seguridad digital para combatir la cibercriminalidad en el Perú siendo sumamente imprescindible.

Desafíos Clave para Combatir la Cibercriminalidad

La *brecha digital*, entendida como "la desigualdad en acceso y uso del servicio de internet o, a mayor escala, del uso de las Tecnologías de la Información y las Comunicaciones" (Escobar Del Solar y Chigne Hernández, 2023) es un desafío clave que debe enfrentarse para combatir la cibercriminalidad en Perú. Por su parte, "la Organización para la Cooperación y el Desarrollo Económicos (OCDE) define a la brecha digital como la diferencia en términos de acceso y uso de TIC a nivel individual [entre personas], organizacional [entre empresas] o global [entre países]" (Libaque-Saenz, 2023, p. 186). Estos mismos autores señalan que,

> …la Unión Internacional de Telecomunicaciones (UIT) sugiere que esta brecha está compuesta por tres dimensiones: acceso, que se refiere a la infraestructura; uso, que se refiere a la generación de valor; y habilidades, que se refiere a la capacidad para hacer uso de las TIC" (citado en Libaque-Saenz, 2023, p. 186).

En este sentido, limitaciones en el acceso, causados por la falta de inversión en estructura tecnológica; el uso gubernamental, económico y educativo poco productivo que se hace con las tecnologías de la información y la comunicación; y, las escasas habilidades que se tienen para el manejo de las mismas, se convierten en desafíos clave a superar para poder combatir la cibercriminalidad.

Al respecto, Meza Lovón (2023) expone que "solo el 5,9% de los hogares de áreas rurales tuvieron acceso a Internet al término del primer trimestre del 2020 y cerca de 300.000 alumnos desertaron de la educación básica en el 2020" (s/p); lo que trajo como consecuencia una escasa formación en el uso y aprovechamiento de estos recursos, y la

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

exposición a los riesgos que genera manipular herramientas tecnológicas desde el desconocimiento. Es decir, existe una *insuficiente alfabetización digital* o habilidades en las personas, para utilizar las tecnologías de la información y comunicación de manera segura, crítica y efectiva.

En consecuencia, la limitada alfabetización digital en Perú, dificulta la prevención y detección de delitos cibernéticos, representando un obstáculo significativo en la lucha contra la cibercriminalidad. De tal manera que, existe mayor susceptibilidad al phishing, por ejemplo, siendo la población más propensa a caer en engaños por medio de correos electrónicos fraudulentos o sitios web falsos que roban la información personal o financiera. Además, la población peruana que carece de formación en los medios digitales tiene mayor dificultad para identificar las amenazas y reconocer las señales de un ataque cibernético, como enlaces sospechosos o solicitudes de información inusuales. A esto se suma las dificultades que se le presenta por desconocimiento, al momento de denunciar los delitos cibernéticos, pues no saben cómo reportar un incidente o a quien acudir en busca de ayuda.

En este sentido, si bien existe el Código Penal peruano que contiene disposiciones penales aplicables a conductas delictivas que se cometen utilizando medios informáticos, y la Ley de Protección de Datos Personales que establece los principios y derechos en esta materia y sanciona las infracciones a los mismos, no estando enfocada exclusivamente en la ciberdelincuencia, pero teniendo una estrecha relación con ella, ya que muchos delitos cibernéticos involucran el tratamiento ilícito de datos personales, como sucede en los casos mencionados en párrafos anteriores; de este contexto se deriva otro desafío clave para combatir la cibercriminalidad en Perú, y es la *falta de legislación y regulación*; sobre todo por la existencia de algunas lagunas e inconsistencias del marco legal peruano en materia de ciberseguridad que favorecen el accionar de los cibercriminales.

Por ejemplo, existen leyes como la N° 30096 (promulgada en el 2013) de delitos informáticos, que constituye el marco legal fundamental para la prevención y sanción de los delitos cometidos a través de sistemas informáticos, estableciendo los tipos penales

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

como el acceso no autorizado a sistemas informáticos, la intercepción de datos, la suplantación de identidad, entre otros. Esta ley es modificada constantemente, siendo la Ley N° 30171 (Obando, 2024) una modificación de la misma, que busca proteger la infraestructura de la información, adecuar la legislación peruana a los estándares internacionales en materia de cibercriminalidad, incorpora nuevos tipos y refuerza las sanciones para ciertos delitos relacionados con conductas ilícitas y el uso indebido de tecnologías de la información y la comunicación.

Sin embargo, aunque la ley N° 30171 abarca una amplia gama de delitos informáticos, existen delitos que podrían no estar explícitamente tipificados o que podrían requerir una interpretación más amplia, como: los delitos relacionados con inteligencia artificial, dados por el avance de la IA, de donde podrían surgir nuevos tipos de delitos, como el uso malicioso de algoritmos para manipular información o tomar decisiones discriminatorias; delitos en la deep web y darknet, que son redes anónimas utilizadas para actividades ilícitas como la venta de drogas, armas o la explotación infantil; delitos relacionados con criptomonedas, como el lavado de dinero, la financiación del terrorismo y los fraudes relacionados con las ICO (Initial Coin Offerings); delitos relacionados con la Internet de las Cosas (IoT), debido a que los dispositivos conectados a internet pueden ser vulnerables a ataques cibernéticos; los delitos que involucran la manipulación de la opinión pública, entre los que está la difusión de fake news, la manipulación de elecciones y la creación de cuentas falsas en redes sociales, entre los muchos ejemplos de delitos que podrían no estar claramente definidos en la ley.

Así, vemos que, gracias a la evolución constante de la tecnología, la cibercriminalidad a la par evoluciona, dificultando que la legislación se adapte a tiempo a las nuevas amenazas. A esto se suma la falta de especialización de los operadores de justicia, ya que muchos jueces, fiscales y policías, carecen de la capacitación especializada necesaria para investigar y juzgar delitos cibernéticos; sobre todo, cuando existe la dificultad de obtener pruebas digitales, ya que la evidencia digital es volátil, difícil de preservar y puede ser fácilmente manipulada, dificultando su recolección y valoración en los procesos judiciales. Todas estas faltas de legislación adecuada pueden generar la

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

sensación de impunidad entre los ciberdelincuentes, incentivándolos a cometer más delitos.

Metodología

El presente artículo fue elaborado haciendo una revisión sistemática de documentos en la web, estableciendo previamente dos criterios de selección de las fuentes: Primero, documentos centrados en la temática de la seguridad digital; y, segundo, información sobre la cibercriminalidad en el Perú; por lo que se revisaron repositorios digitales, noticias, revistas científicas y portales del gobierno del Perú, para obtener información actualizada que permitiera realizar un proceso hermenéutico, siendo este el que permite "una alternativa propia para la interpretación" (Quintana y Hermida, 2019 p. 75).

Este proceso hermenéutico cubrió las tres dimensiones de la hermenéutica: *lectura* (proceso dialéctico que ocurre entre la lectura interpretativa y el entendimiento; *explicación* (aspecto discursivo de la comprensión); y, *traducción* (énfasis en lo histórico-contextual). Estas dimensiones son partes del *círculo hermenéutico* en el que se establece la relación entre el todo y las partes, de esta forma, el significado de las partes o componentes siempre estuvo determinado por el conocimiento previo del todo y el conocimiento del todo fue y será "corregido continuamente y profundizado por el crecimiento en nuestro conocimiento de los componentes" (Martínez, 1996, p. 138).

Resultados, Análisis e Interpretación: Estrategias de Seguridad Digital para Combatir la Cibercriminalidad en el Perú

A continuación se presentan algunas estrategias de seguridad digital para combatir la cibercriminalidad en Perú, considerando los desafíos expuestos en el apartado correspondiente. Como toda producción intelectual seria, es necesario aclarar que con este estudio no se pretende agotar todas las posibilidades para afrontar el problema, pero sí se quiere dejar expuestos algunos puntos esenciales que deben tomarse en cuenta al

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

plantear soluciones que aspiren transformar drásticamente la situación planteada en la búsqueda de mejorar las condiciones de vida de la población peruana.

Estrategias de Seguridad Digital para reducir la brecha digital

En cuanto a las tres dimensiones que establece la *brecha digital, se plantean algunas estrategias en cuanto* al acceso, uso y habilidades que permitan coadyuvar a la reducción de la misma en especial en las partes más vulnerables de la población:

Acceso: referida a la infraestructura o disponibilidad física de las tecnologías que incluye factores como la existencia de redes de internet, la cobertura de telefonía móvil, el acceso a dispositivos como computadoras y smartphones, y la asequibilidad a estos servicios, como suele suceder en zonas rurales o de bajos recursos, limitando el acceso a internet y dejando a la población desconectada del mundo digital.

La estrategia para combatir la cibercriminalidad en Perú sería el Desarrollo de infraestructura tecnológica invirtiendo en aquella necesaria para garantizar la seguridad de los sistemas informáticos del Estado y para expandir la cobertura de internet de alta velocidad en zonas rurales y urbanas marginadas para reducir la brecha digital; para lo cual se requeriría la Cooperación público-privada a través de la creación de alianzas entre el sector público y el sector privado para modernizar los sistemas gubernamentales, robusteciendo los sistemas de seguridad en las instituciones públicas para proteger la información ciudadana.

Además, se requeriría de la fomentación de la investigación y desarrollo de iniciativas que promuevan la investigación en ciberseguridad y el desarrollo de soluciones locales. Una opción que fortalecería la infraestructura tecnológica y el acceso a internet sería la instalación de puntos de acceso público a internet en lugares estratégicos como bibliotecas, centros comunitarios y escuelas.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

Uso: en la generación de valor, refiriéndose a la forma en que las personas utilizan las TIC para mejorar su vida, incluyendo actividades como buscar empleo, realizar trámites en línea, acceder a la educación a distancia, comunicarse, realizar transacciones comerciales, entre otras.

Pueden crearse alianzas estratégicas que permitan desarrollar soluciones conjuntas y promover la ciberseguridad en el uso de las herramientas tecnológicas, para lo cual es necesario informar a los usuarios sobre sus derechos y el cómo proteger sus datos personales en línea; además, se debe fomentar el uso de tecnologías seguras, a través del uso de herramientas y aplicaciones que protejan la privacidad y la seguridad de los usuarios.

Como incentivos para la adopción de buenas prácticas a nivel empresarial o de organismos públicos y privados, se pueden otorgar reconocimientos a empresas y organizaciones que implementen medidas de seguridad robustas y que promuevan una cultura de ciberseguridad. Además, se pueden ofrecer incentivos fiscales a las empresas que inviertan en la capacitación de sus empleados en el tema de la ciberseguridad.

Habilidades: Competencias y conocimientos que son necesarios para utilizar las tecnologías de manera efectiva, incluyendo habilidades para navegar en internet, utilizar programas de computadora, gestionar el correo electrónico, evaluar la información, proteger la privacidad en línea, por mencionar algunos. De tal manera, que el ciudadano tenga la capacidad de distinguir entre fuentes de información confiables y falsas, siendo una habilidad fundamental para dejar de ser víctimas de desinformación o de estafas en línea. Este desafío requiere de la implementación de programas escolares, en los que se incorpore la educación digital en los currículos desde niveles básicos, para fomentar no solo una cultura de seguridad en línea desde temprana edad, sino también, el desarrollo de habilidades y competencias que permitan el acceso a internet de manera eficiente y efectiva. Parte importante de esta formación, sería la capacitación de adultos mayores a través del diseño de programas específicos, ya que son parte de la población vulnerable a los ciberataques.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

En síntesis, si la principal barrera para superar la brecha digital, la cual incide directamente en el aumento de la cibercriminalidad, es la falta de acceso a internet en una región, se pueden implementar políticas para expandir la infraestructura de telecomunicaciones. Si el problema es la falta de habilidades, se pueden desarrollar programas de capacitación para enseñar a las personas a utilizar las TIC. Si el obstáculo es la falta de dispositivos se pueden implementar programas de donación o venta de equipos a bajo costo.

Estrategias para abordar el desafío de la limitada alfabetización digital

Entre las estrategias necesarias para abordar el desafío de la limitada alfabetización digital se encuentra la promoción de la cultura de la ciberseguridad, que consistiría en promover la educación en ciberseguridad desde edades tempranas, tanto en el ámbito escolar como en el ámbito laboral. Esto involucraría la concientización sobre la importancia de la protección de datos personales y sensibles, a través de campañas para informar sobre los riesgos de la cibercriminalidad y las medidas de prevención que se pueden adoptar. Esto puede hacerse a través de diversos canales de comunicación como televisión, radio, redes sociales, eventos comunitarios, entre otros, para llegar a un público amplio y diverso.

Otra forma de alcanzar una educación digital masificada y personalizada sería a través de la organización de talleres y cursos gratuitos o a bajo costo para diferentes grupos poblacionales (niños, jóvenes, adultos mayores) enfocados en temas específicos como la protección de datos personales, el reconocimiento de phishing y el uso seguro de redes sociales

También podrían desarrollarse materiales educativos accesibles, es decir, la creación de materiales fáciles de entender y adaptados a diferentes niveles de conocimiento, para lo cual sería necesaria la cooperación entre el sector público y privado, de tal manera que el trabajo en conjunto desarrolle soluciones y recursos educativos variados que permitan implementar una metodología de aprendizaje adecuada para la temática de la

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

ciberseguridad. Y, aprovechando la misma tecnología, pueden desarrollarse plataformas en línea o aplicaciones móviles que ofrezcan cursos personalizados y adaptados a las necesidades individuales de los usuarios. En síntesis, es necesario invertir en educación, concientización y el desarrollo de herramientas y recursos que permitan a la población utilizar las tecnologías de manera segura y responsable.

Estrategias para abordar el desafío de la falta de legislación y regulación

Entre las estrategias que pueden proponerse para enfrentar el desafío de la falta de legislación y regulación en materia de la cibercriminalidad, está buscar el fortalecimiento del marco legal a través de la actualización de las leyes para que abarquen las nuevas formas de cibercrimen y las tecnologías emergentes.

En cuanto a los datos personales y su protección, se puede fortalecer el marco legal en este sentido y establecer mecanismos de supervisión y control efectivos, de tal manera que se puedan sancionar de manera ejemplar a las empresas que infrinjan la normativa y pongan en riesgo los datos de los usuarios. También, es necesaria la creación de nuevas leyes específicas para abordar delitos como el hackeo, el phishing, el ransomware y la difusión de contenido ilícito.

Como la cibercriminalidad trasciende fronteras, el establecimiento de mecanismos de cooperación internacional es fundamental para investigar y perseguir a los delincuentes. Es por ello que es necesaria la recomendación de participar activamente en redes internacionales de intercambio de información sobre amenazas cibernéticas y buenas prácticas en ciberseguridad y el fortalecer la cooperación con otros países en la investigación y persecución de cibercriminales.

También, la capacitación de las fuerzas del orden en la investigación de delitos cibernéticos, la recolección de pruebas digitales y el uso de herramientas forenses, puesto que, los ciberdelitos involucran conceptos técnicos complejos y técnicas actualizadas, que requieren un conocimiento especializado tanto de la parte investigadora como de la

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

judicial. En tal sentido, las leyes deben ser redactadas de manera clara y precisa para garantizar que los operadores jurídicos puedan aplicarlas correctamente.

Conclusiones

Hemos podido observar con este estudio que, la ciberdelincuencia es un flagelo que acecha en las sombras de la era digital, al ser conscientes de esto, es necesario afirmar que se deben buscar respuestas contundentes y proactivas. En este contexto, la alfabetización digital se constituye como una estrategia indispensable para fortalecer las defensas contra los ataques cada vez más sofisticados. Esto requiere ir más allá del simple conocimiento de las tecnologías, que también es necesario, implica desarrollar un pensamiento crítico que permita navegar de manera consciente y segura por el ciberespacio.

Al empoderar a la ciudadanía con las habilidades necesarias para, por ejemplo, identificar amenazas, proteger sus datos y tomar decisiones informadas en línea, se estará construyendo una sociedad más acorde con las exigencias del siglo XXI, caracterizada por los acelerados avances tecnológicos. En un mundo donde la tecnología avanza a un ritmo vertiginoso, la alfabetización digital es una habilidad esencial que debemos adquirir todos. Solo así podremos disfrutar de los beneficios del mundo digital sin poner en riesgo nuestra seguridad y privacidad.

Al invertir en educación y concienciación, podemos reducir significativamente el impacto de los ciberataques y construir un ciberespacio más seguro para todos. Es fundamental que gobiernos, empresas y organizaciones de la sociedad civil trabajen de forma conjunta para promover la alfabetización digital y garantizar que todas las personas tengan acceso a los conocimientos y herramientas necesarias para protegerse en línea.

El desarrollo de habilidades y competencias específicas para afrontar la cibercriminalidad en Perú se vuelve cada vez más fundamental. Estas capacidades no solo permiten a las personas protegerse a sí mismas, sino que también contribuyen a

Publicación en Línea (Semestral) UPEL-Maracay (Venezuela)
DL: PPL201102AR3941
ISSN: 2244-7962
Julio-Diciembre 2024. Vol. 21, Nº 2
Revista Multidisciplinaria Dialógica

fortalecer la resiliencia de las organizaciones y del país en su conjunto. Al conocer los mecanismos de los ciberataques, las personas pueden identificar y evitar caer en las trampas de los delincuentes cibernéticos, pueden reconocer las señales de alerta y los comportamientos sospechosos que le permitirán actuar rápidamente ante una amenaza.

También, podrá poner en práctica, si es necesario, los protocolos de seguridad y las herramientas que estén disponibles para el resolver el incidente. Todo lo anterior incidiría de forma retroactiva en el desarrollo económico, ya que, empresas y organizaciones con capital humano formado con una sólida cultura en seguridad cibernética generarán confianza y atraerán nuevas y más inversiones.

En cuanto a la falta de legislación y regulación como desafío en la lucha contra la cibercriminalidad en Perú, es posible afirmar que la misma se comporta como tal porque la legislación peruana existente es insuficiente para abordar la rápida evolución de los delitos cibernéticos, puesto que, las leyes actuales no están diseñadas para enfrentar nuevas modalidades de cibercrimen y/o contienen lagunas legales que los delincuentes pueden explotar.

No obstante, para enfrentar este desafío, es necesario fortalecer el marco legal, capacitar a las fuerzas del orden, invertir en tecnología, promover la cooperación público-privada e internacional y fomentar una cultura de la ciberseguridad. Así vemos que, la creación de nuevas leyes específicas para abordar los delitos cibernéticos en Perú es una necesidad imperante, ya que un marco legal sólido y actualizado permitirá una lucha más efectiva contra estos delitos, protegiendo a las personas, las empresas y el Estado.

Finalmente, la ciberdelincuencia es un desafío complejo que requiere una respuesta multifacética. La inversión en la formación de habilidades y competencias en ciberseguridad es una inversión en el futuro. Al empoderar a las personas con los conocimientos necesarios, podemos construir una sociedad más segura y resiliente en el mundo digital.

Es fundamental que el Estado, el sector privado y la academia trabajen en conjunto para promover la alfabetización digital y desarrollar programas de capacitación que abarquen a todos los sectores de la población. Solo así podremos enfrentar los desafíos de la ciberdelincuencia y aprovechar al máximo las oportunidades que ofrece el mundo digital.

Referencias

Escobar Del Solar, H. A. y Chigne Hernández, G. (2023, septiembre 7). *Brecha digital en el Perú ¿cuál es su estado y qué mecanismos existen o son necesarios para reducirla?* [Post]. LinkedIn. https://www.linkedin.com/pulse/brecha-digital-en-el-per%C3%BA-cu%C3%A1l-es-su-estado-y-qu%C3%A9-mecanismos/

Gob.pe. (14 de enero de 2024). *Delitos de ciberdelincuencia*. https://www.gob.pe/23409-delitos-de-ciberdelincuencia

Forbes. (25 de marzo de 2024). *El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet*. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet

Instituto Nacional de Estadística e Informática. (2024). *Estadísticas de seguridad ciudadana enero-junio 2024*. https://m.inei.gob.pe/media/MenuRecursivo/boletines/estadisticas-de-seguridad-ciudadana-enero-junio-2024.pdf

Meza Lovón, G. L. (2023). *La brecha digital del Perú: Remedios que no la cierran*. Universidad Católica San Pablo. https://acortar.link/WCBKMV.

Libaque-Saenz, C. F. (2023). Estrategias para reducir la brecha digital en el Perú: Lecciones de la República de Corea. *Política Internacional*, (133), 184–197. https://doi.org/10.61249/pi.vi133.71

Martínez Miguélez, M. (1996). *Comportamiento humano: Nuevos métodos de investigación* (2a. ed.). México: Trillas.

Obando, J. (15 de julio de 2024). *Seguridad digital en Perú: cuál es su estado*. https://linktic.com/blog/seguridad-digital-en-peru-cual-es-su-estado/

Oficina de las Naciones Unidas contra la Droga y el Delito. (09 de agosto de 2024). *Estados Miembro de las Naciones Unidas aprueban borrador para una convención contra la ciberdelincuencia*. https://acortar.link/cnQvig

Quintana, L. y Hermida, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Perspectivas en Psicología. 16*(2), 73-80.

Real Academia Española: Diccionario de la lengua española, 23.ª ed., [versión 23.7 en línea]. https://dle.rae.es/

Trinidad, S. (26 de septiembre de 2024). Ola de extorsiones: "La ciudadanía ya no denuncia pues ha perdido la confianza en las instituciones". *PuntoEdu.* https://puntoedu.pucp.edu.pe/coyuntura/ola-de-extorsiones-la-ciudadania-ya-no-denuncia-pues-ha-perdido-la-confianza-en-las-instituciones/

Síntesis Curricular

Eber Geisel Trujillo Vega

Abogado con Maestría en Derecho Penal y especialización en Derecho Penal y Procesal Penal, lo que ha permitido desarrollar un profundo conocimiento y dominio en la aplicación de estas disciplinas. A lo largo de la carrera profesional, ha adquirido una sólida experiencia, destacándose en su rol como Fiscal Adjunto Provincial del Distrito Fiscal de Cañete en Perú.

Trujillo Vega, E.G. (2024). Desafíos y estrategias de seguridad digital para combatir la cibercriminalidad en Perú. *Dialógica, Revista Multidisciplinaria.* 21(2), 130-147.