Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 109-120
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Redes y seguridad informática
Recibido: 29/05/2022 | Aceptado: 05/07/2022 | Publicado: 30/09/2022

Identificadores persistentes:
ARK: ark:/42411/s9/a62
PURL: 42411/s9/a62

Revisión de los avances y cambios en ciberseguridad en el Perú, para una transformación digital

Review of advances and changes in cybersecurity in Peru, for a digital transformation

Edwin Daniel Leon Gutierrez [1][0000-0002-2519-1785]*, **Cynthia Mayumi Tesillo Gomez** [2][0000-0002-1769-9845], **Yuri Alexander Escobar Arcaya** [3][0000-0001-5739-3050] , **Luis Antonio Godoy Montoya** [4][0000-0001-8860-8843]

[1] Universidad Nacional Jorge Basadre Grohmann, Tacna, Perú. edwin.leon@unjbg.edu.pe
[2] Universidad Nacional Jorge Basadre Grohmann, Tacna, Perú. cynthia.tesillo@unjbg.edu.pe
[3] Universidad Nacional Jorge Basadre Grohmann, Tacna, Perú. yuri.escobar@unjbg.edu.pe
[4] Universidad Nacional Jorge Basadre Grohmann, Tacna, Perú. luis.godoy@unjbg.edu.pe

* Autor para correspondencia: edwin.leon@unjbg.edu.pe

Resumen

El presente trabajo tiene por objetivo explorar publicaciones donde ha sido tratado el tema de ciberseguridad en el Perú. Para ello, se han revisado 12 artículos originales en relación a la temática, publicados en los últimos 5 años. Este artículo cuenta con un claro objetivo descriptivo, exploratorio.

Palabras clave: Ciberseguridad, ciberataques, Estándar, ISO, NTP.

Abstract

This work aims to explore publications where the topic of cybersecurity in Peru has been treated. For this, 12 original articles have been reviewed about the subject, published in the last five years. This article has a clear, descriptive, exploratory objective.

Keywords: *Cybersecurity, Cyberattack, Standard, ISO, NTP.*

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 109-120
https://revistas.ulasalle.edu.pe/innosoft

Introducción

La irrupción de nuevas tecnologías, la proliferación de modernos dispositivos inteligentes, dio origen a una transformación digital no planificada en muchos casos, incentivada en los dos últimos años por el confinamiento al que la población se ha visto sometida por la pandemia originada por el COVID-19. Si bien la situación representa una oportunidad esto también trae consigo algunos riesgos asociados al uso de tecnologías que hasta hace poco no tenían mucha difusión y junto con las amenazas se hace necesario una adecuada planificación de la gestión de las mismas, sobre todo en un entorno cibernético.

El uso masivo de nuevas tecnologías en el campo de las TI, y la sofisticación continua, está originando que los riesgos se tornen más peligrosos y se diversifiquen.

La gestión de la información ha sido considerada como uno de los más preciados activos en toda organización desde inicios de los sistemas de información por ser base para la toma de decisiones con impacto directo o indirecto en las personas [1].

En la actualidad los medios digitales están vinculados a potenciales vulnerabilidades, las cuales de no ser controladas/minimizadas facilitaran el accionar de agentes externos a los sistemas, con el peligro de alteración, robo, secuestro de información o recursos digitales [2].

Es ante estos riesgos latentes que las estrategias en tema de Ciberseguridad se vuelven en una necesidad que debe asumir una nación a fin de garantizar el bienestar de la población [2].

Para [3] en el Perú no existe por parte del estado una real toma de conciencia respecto a los posibles daños que podrían generar a las empresas los ciberataques.

La importancia que han ido alcanzando los ciberataques queda identificada por [4] que para el año de la publicación asignaba al Perú el quinto lugar en cuanto a ciberataques registrados.

En cuanto a protección de datos personales, se tiende a dar prioridad a aquellos campos en donde el uso masivo de información, ha ido de la mano con el incremento de servicios ofertados online, sin embargo debe de prestarse también atención a aquellas áreas en donde el resguardo de la privacidad de la información resulta crítica aun cuando no se vincule a un uso masivo de la misma tal es el caso de información sensible generada por usuarios en la actividad privada tales como médicos, abogados, médicos cirujanos plásticos, etc. [5].

Si bien el estado peruano ha dado pasos hacia un ordenamiento en temas de seguridad informática (ciberseguridad, seguridad de la información, etc.) por medio de la implementación de normas, también es correcto decir que son pocos los avances en los aspectos de organización y capacitación [6].

Se llama en [7] a reflexionar respecto a dar la debida importancia a invertir tanto en tecnología como en recursos humanos, tal es así que se menciona que uno de los mayores riesgos para las entidades bancarias es el sabotaje efectuado por un insider, empleado de la misma organización.

La necesidad de que el estado implemente estrategias nacionales de ciberseguridad no deben de limitarse a garantizar la seguridad de los ciudadanos y las infraestructuras, debe también incluir la instauración de un ecosistema que permita la cooperación público - privada [8].

Respecto a los rápidos cambios tecnológicos a los que nos vemos enfrentados, una pregunta toma forma en [9] ¿Serán capaces de adaptarse rápidamente tanto las personas como las organizaciones a los cambios tecnológicos de los que somos testigos día tras día?, una respuesta negativa puede darnos una idea de lo vulnerables que serán ante las amenazas informáticas. Hemos pasado en poco tiempo de la euforia por los avances tecnológicos revolucionando la vida moderna a la preocupación por el desarrollo de riesgos potenciales a los que sin embargo no se les da la debida importancia [10].

Las PYMES no están ajenas a los abruptos cambios en temas de tecnología y son estas quienes puede ver en ellas una oportunidad de mejora así como una fuente de potenciales riesgos sobre todo en época de pandemia en donde han sido duramente golpeadas financieramente, por lo que el tema de ciberseguridad se torna relevante para enfrentar vulnerabilidades que se pueden generar en el ciberespacio y afectar la continuidad del negocio [11].

Pero existen sectores altamente vulnerables que conforme van adoptando tecnologías IOT, van convirtiéndose en posibles blancos de ciberataques, tal es el caso de empresas dedicadas a servicios tales como tratamiento/potabilización de agua, en las cuales el alto grado de automatización supone un gran desafío para la implementación de sistemas de ciberseguridad [12].

En [13] el año 2019 se indicaba que únicamente el 9% de las empresas peruanas estaban aptas para detectar un ciberataque a tiempo, esta cifra nos da una idea de lo lejano que está que el estado en su conjunto pueda articular acciones conjuntas (sector público y privado) en temas de ciberseguridad y respuesta ante ciberataques.

En cuanto a la “información”, en [1] se indica que es cambiante y por tanto la protección de la misma adquiere esa característica.

En el presente trabajo se presenta una revisión de publicaciones que abordan el tema de ciberseguridad en el Perú, para lo cual se ha realizado una búsqueda de material bibliográfico que permita tener un primer acercamiento a los avances que se realizaron en ciberseguridad en el Perú.

Este artículo tiene por objetivo explorar los avances que se realizaron en ciberseguridad en el Perú a través de la revisión de papers publicados en los últimos 5 años.

Materiales y métodos

El presente trabajo es descriptivo exploratorio, para la recolección de información, se han utilizado unos criterios de búsqueda y de inclusión para seleccionar los artículos que finalmente han formado parte de la revisión. Ambos criterios se describen a continuación.

1. Búsqueda en bases de datos bibliográficas.

   Para realizar la búsqueda bibliográfica se realizó una búsqueda en diferentes bases de datos (Google académico, Dialnet, etc.).

   Las palabras clave utilizadas fueron: ciberseguridad, Perú, normas ISO.

2. Criterios de inclusión.

   Una vez obtenidos los resultados de las búsquedas a través de las técnicas anteriores, los artículos se pasaron por un filtro y solo se aceptó que formaran parte de la revisión aquellos que cumplian con los siguientes criterios:

   - Tener acceso al texto completo del artículo científico.
   - Excluir los artículos donde el tema de ciberseguridad fuese tratado secundariamente.
   - Los documentos deben tener fecha de publicación mayor o igual al 2017.

Resultados y discusión

Después de una depuración de los 18 artículos, la base de datos quedó constituida por 12 artículos.

A continuación, se muestra la distribución de artículos por año de publicación y tipo de artículo.

Tabla 1. Artículos por año de publicación

Año de publicación	N° de Artículos
2017	1
2018	4
2019	2
2020	2
2021	2

2022	1
Total	12

Fuente Elaboración propia

Tabla 2. Artículos por tipo

Tipo de artículo	N°
Artículo Científico	8
Tesis de grado. Maestro	2
Tesis de grado. Licenciatura	1
Tesis de grado. Bachiller	1
Total	12

Fuente Elaboración propia

A continuación, se presentan los artículos seleccionados.

Título: "GESTIÓN DE LA CIBERSEGURIDAD Y PREVENCIÓN DE LOS ATAQUES CIBERNÉTICOS EN LAS PYMES DEL PERÚ, 2016"
Autor: ANTONIO INOGUCHI ROJAS, ERIKA LIZET MACHA MORENO - 2017

En el trabajo de investigación se aborda la situación de las PYMES del Perú ante los desafíos que supone la ciberseguridad, tema que hasta no hace mucho no representaba un foco de interés, sin embargo la masificación de los servicio online que han ido adoptando las PYMES las obliga a replantearse seriamente los riesgos que suponen estas nuevas tecnologías en el ámbito de protección de datos y la seguridad de los sistemas de información., teniendo en cuenta que al referirse a la data informática, se considera toda la información virtual almacenada y disponible en la red privada, siendo este recurso fundamental y vital para que las pymes funcionen correctamente y alcancen los objetivos propuestos. Los autores logran identificar (en la PYME objeto del trabajo) la falta de visión respecto a seguridad de la

información, sobre todo en el tema de ciberseguridad, ya que la pérdida de información o manipulación por personas ajenas a la empresa conlleva a resultados adversos para la empresa misma, a tal punto de correr el riesgo de quiebra. Con los resultados obtenidos en la investigación, se proponen recomendaciones, indicando una propuesta para gestión y prevención de seguridad informática, la cual podrá ser aplicable para la mayoría de pymes de diferentes rubros o giros de negocio, el único requisito es que la pyme se proponga implementar la propuesta de seguridad informática resultante.

Título: "CIBERSEGURIDAD EN LA INFRAESTRUCTURA CRÍTICA MEDIANTE EL SISTEMA SCADA EN PLANTA DE TRATAMIENTO DE AGUA DE LIMA"
Autor: André FERREIRA ALVES MACHADO, Lizet CACHO DE LA CRUZ. - 2018

En el trabajo se aborda el análisis de vulnerabilidades en un sector muy crítico como es el de prestación de servicios básicos específicamente abastecimiento de agua potable. Sectores claves como el que se trata, se respaldan en una amplia gama de sistemas y recursos informáticos para su funcionamiento continuo, confiable y efectivo. Estos sectores son conocidos como infraestructuras críticas. La protección de este tipo de infraestructura ha tomado más relevancia en los últimos años, por el gran impacto sobre la comunidad que supone los riesgos a los que está sometida, lo cual ha motivado a los Estados a generar acciones para garantizar su seguridad. Por otro lado, los cambios permanentes de las tecnologías hacen necesario no solo un profundo trabajo de articulación entre diversos actores sino la evaluación constante de distintos escenarios de compromiso, así como la adopción de medidas preventivas y correctivas para minimizar cualquier impacto de un ataque cibernético sobre los servicios esenciales. adicionalmente el trabajo define y caracteriza a las infraestructuras críticas, presentando la descripción de un conjunto particular de sistemas denominados SCADA o sistemas de control y adquisición de datos, así también describe casos de estudio de vulnerabilidades de dichos sistemas y alega sobre su implementación en la planta potabilizadora de agua en el Perú (Sedapal).

Título: "Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio".
Autor: Beteta Lazarte, Juan Enrique, Narva De la Cruz, Miluska de Jesús-2018

Trabajo en el que se analiza el sector de seguros privados, como el objetivo de evaluar cómo están preparadas Mapfre Perú Seguros y Kallpa corredora de seguros, dos empresas del mismo rubro pero con distinta capacidad financiera, ante

las amenazas de seguridad de la información que podrían impactar en sus operaciones de negocio, teniendo como finalidad el proponer una guía base de controles para mitigar los riesgos.

Título: "La ciberseguridad y el contexto actual"
Autor: Roberto Vizcardo Benavides - 2018

La guerra mundial en el ciberespacio está teniendo lugar. Ejércitos de hackers, espías informáticos y ciberdelincuentes conforman las fuerzas contrincantes; no hay distinción, los adversarios son naciones desarrolladas o en vías de desarrollo, así como grupos e individuos al margen de la ley. Generalmente no hay víctimas mortales ni heridos; pero los daños económicos son inconmensurables. Naciones Unidas y la OEA en particular, han tomado el reto de enfrentar esta nueva amenaza mediante la defensa cooperativa; sin embargo, en el ámbito regional, es poco lo que se ha hecho.

Título: "Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones".
Autor: Vilcarromero Zubiate, Ladi Lizeth; Vilchez Linares, Evit - 2018

En el trabajo, los autores proponen un modelo de gestión de ciberseguridad a una empresa de telecomunicaciones, sobre la base de una adecuada gestión del riesgo y la medición de controles según un nivel de madurez, dada la importancia del área de desenvolvimiento de la misma que es considerada muy crítica. Sectores como el que se abordan representan para la seguridad nacional y económica de los países, un factor importante del cual depende el funcionamiento confiable de su infraestructura crítica. Las amenazas de ciberseguridad explotan la creciente complejidad de dichos sistemas, colocando la economía, la seguridad pública y la salud en riesgo. Al igual que el riesgo financiero y de reputación, el riesgo de ciberseguridad afecta a los objetivos estratégicos de una empresa. Así mismo, la información se ha convertido en uno de los activos más importantes para cualquier organización, y el aseguramiento de la misma como un punto primordial para lograr ventajas competitivas y generación del valor, basando en el adecuado resguardo de la Confidencialidad, Disponibilidad e Integridad de la Información.

Título: "Problemática en ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo".

Autor: Alexis Enrique Poma Vargas - 2019

La seguridad en las redes sociales y sistemas de información son puntos de interés que se analizan en el trabajo, en el cual el autor se plantea investigar si la Ciberseguridad protege los sistemas informáticos y redes sociales en el Perú y el mundo, puesto que existen lugares tales como empresas y entidades propensas a todo tipo de ataques cibernéticos realizados por hackers, quienes sustraen información valiosa de estas. Dicha investigación es cuantitativa, basada en análisis documentario, buscó información local, nacional e internacional de fuentes confiables, que pudiesen aportar alcances estadísticos y casos de protección a medios informáticos, a fin de proporcionar conocimientos sobre vulnerabilidad de sistemas por no contar con los recursos que permitan salvaguardar datos reservados, así como, las soluciones respectivas al caso. Los resultados fueron favorables, en el sentido que se pudo apreciar que, mediante la adopción de medidas rígidas, los sistemas informáticos; así como las redes sociales, se vuelven potencialmente seguros en un 70%. En tal sentido se concluye que la ciberseguridad como protección de medios informáticos potencializa las buenas prácticas en las empresas y protege la información.

Título: "LATINOAMÉRICA ¿CÓMO ESTÁ AVANZANDO LA CIBERSEGURIDAD EN EL PERÚ? BREVE APROXIMACIÓN AL MARCO NORMATIVO".

Autor:Viviana García - 2019

Este artículo busca ejemplificar el marco normativo que se viene desarrollando en el país con relación a la ciberseguridad y mostrar que, si bien no es aparente, sí existe una preocupación por esta materia, dado que el Perú no puede estar ajeno al gran reto que representa para las organizaciones el proceso de transformación digital y que conlleva una necesaria reflexión respecto de las amenazas latentes por la potencial vulneración a la seguridad de los sistemas de información.

Título: "Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional"

Autor: Juan Fernando Ormachea Monte s - 2020

En el trabajo se establece como objetivo proponer estrategias integradas de ciberseguridad necesarias para fortalecer la seguridad nacional del Perú. Se evalúa las estrategias y políticas actuales utilizadas en el ámbito internacional para contrarrestar las ciberamenazas, así como las estrategias de ciberseguridad implementadas específicamente por los Países Bajos, EE. UU., España y Perú. Como resultado de la investigación se encontró que, en los indicadores referidos

a cooperación regional, bilateral y multilateral, el Perú ha manifestado comportamientos disímiles; además, el Estado y la sociedad peruana aún transitan por los enfoques de la concientización y del desarrollo de las capacidades cibernéticas militares, como indicadores prevalentes en el diseño de las políticas nacionales de ciberseguridad. Por ello, se concluyó que la ciberseguridad constituye un compromiso social que demanda articulación entre el sector público y el sector privado, lo que en el Perú aún no se concreta; en consecuencia, el diseño de la Estrategia Nacional de Ciberseguridad del Perú constituye una necesidad que demanda ser satisfecha.

Título: "La seguridad de la información en la administración pública"
Autor: Kadú Josep Altamirano-de-la-Borda - 2020

En el trabajo se aborda la importancia de la información pública, la cual es producto de la administración y transformación de otra información que tiene un efecto directo en la ciudadanía, por lo cual debe ser protegida asegurando su confidencialidad, integridad y disponibilidad, teniendo siempre presentes los principios del derecho al acceso a la información de los ciudadanos. Si bien en el Perú se han dado los pasos adecuados para implementar los sistemas de gestión de seguridad de la información en el ámbito público, solo el 6 % de los organismos públicos ha cumplido con implementar lo dispuesto por la normativa vigente. Por lo cual se hace necesario que el Estado redoble los esfuerzos para proteger su información a través de la implementación de sus sistemas de gestión de seguridad de la información, ya que los nuevos escenarios referentes a la tecnología, la información y la interacción entre Estado y ciudadanía así lo requieren.

Título: "Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense".
Autor:Mayra A. Arévalo Álvarez, Daniel Andrey Hernández Ladino. -2021

En el trabajo los autores por medio de una investigación en algunos de los países Latinoamérica se sumergen en el sistema financiero bancario con el objetivo de identificar si los bancos se han visto expuestos a algún tipo de amenaza en años recientes asociados con su auge en la nube, que medidas de prevención han tomado o han buscado implementar para contrarrestarlas y cuál es la contribución que ofrece o puede ofrecer la informática forense para ayudar a esclarecer procesos de investigación principalmente relacionados con delitos financieros.

Título: Ciberseguridad y protección de datos personales en el Perú

Autor:José Álvaro Quiroga León - 2021

El trabajo realiza un análisis del marco legal en torno a la política de privacidad, así como el Reglamento de la Ley de Protección de Datos Personales.

Título: Marco de referencia "HOGO" para ciberseguridad en PyMES basado en ISO 27002 y 27032

Autor: Carlos Francisco Cruzado Puente de la Vega, Liset Sulay Rodriguez Baca - 2022

El trabajo resalta la importancia de desarrollar el marco referencial "HOGO" basado en las buenas prácticas del ISO 27002 y los controles de seguridad del ISO 27032 para la ciberseguridad en las PyMES. Los resultados de la investigación muestran los beneficios de la implementación del marco referencial "HOGO" en las PyMES, aplicando buenas prácticas relacionadas a la seguridad en internet, de las infraestructuras críticas para la información, seguridad de las redes y seguridad de la información. A medida que las tecnologías de información y comunicación se van empoderando en las organizaciones, se va generando una necesidad de protección del activo más importante, la información ante la necesidad de lograr protección de ataques en el ciberespacio.

Conclusiones

En el presente trabajo se realizó una revisión exploratoria de varias publicaciones que abordan el tema de ciberseguridad en el Perú, evidenciando que el interés en dicha área ha ido incrementando con el transcurso del tiempo.

En los textos explorados los autores presentan varias perspectivas en cuanto a los avances en el tema de ciberseguridad, pasando por la comparación en el área de inversiones en el contexto de Latinoamérica, la situación del Perú respecto a los ataques cibernéticos, la implementación de normas que buscan establecer un ordenamiento tanto para el ámbito estatal como privado.

Así también se identifica la falta de concientización y organización que son importantes para poder dar soporte a la implementación del marco normativo, y la importancia en invertir no solo en tecnología sino también en recursos humanos a fin de poder asegurar el minimizar todos los riesgos potenciales a los que se exponen las organizaciones públicas y privadas en temas de ciberseguridad producto del auge de las nuevas tecnologías y su masificación.

La contribución del presente trabajo radica en que se presenta una revisión exploratoria de las publicaciones que en tema de ciberseguridad se han realizado en los últimos 5 años lo cual permite establecer una línea basal sobre la cual poder realizar otras investigaciones en los próximos años.
Se sugiere como trabajo futuro el poder realizar una revisión con mayor profundidad en este tema dado que el continuo desarrollo de las TIC.

Referencias

[1] Kadú Josep Altamirano-de-la-Borda. La seguridad de la información en la administración pública
Enlace: https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/13917/Altamirano_La-seguridad-de-la-informaci%C3%B3n-en-la-administraci%C3%B3n-p%C3%BAblica.pdf?sequence=1&isAllowed=y

[2] Freddy Linares. Vulnerabilidad en el sector público y la urgencia de pensar en ciberseguridad.(2022)
Enlace: https://ciup.up.edu.pe/analisis/vulnerabilidad-en-sector-publico-la-urgencia-de-pensar-ciberseguridad/

[3] GARCÍA, V. (2019). ¿ CÓMO ESTÁ AVANZANDO LA CIBERSEGURIDAD EN EL PERÚ? BREVE APROXIMACIÓN AL MARCO NORMATIVO. Actualidad Jurídica (1578-956X), (52).
Enlace: https://www.uria.com/es/publicaciones/6687-como-esta-avanzando-la-ciberseguridad-en-el-peru-breve-aproximacion-al-marco-n

[4] Inoguchi Rojas, A., & Macha Moreno, E. L. (2017). Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016.
Enlace: https://repositorio.usil.edu.pe/items/9449a061-bfd2-4ecc-8cf1-770fba7cee45/full

[5] León, J. Á. Q. (2021). Ciberseguridad y protección de datos personales en el Perú. Advocatus, (039), 15-21.
Enlace: https://revistas.ulima.edu.pe/index.php/Advocatus/article/view/5114

[6] Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones.
Enlace: https://repositorioacademico.upc.edu.pe/handle/10757/624832

[7] Álvarez, M. A. A., & Ladino, D. A. H. (2021). Análisis preliminar de la ciberseguridad asociada al sistema financiero en algunos países de Latinoamérica y la contribución de la informática forense. Cuaderno de investigaciones: semilleros andina, 1(14).
Enlace: https://revia.areandina.edu.co/index.php/vbn/article/download/1950/1873

[8] Ormachea Montes, J. F. Integrated cybersecurity strategies for strengthening national security.
Enlace: https://www.recide.caen.edu.pe/index.php/recide/article/view/36

[9] Beteta Lazarte, J. E., & Narva De la Cruz, M. D. J. Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio.
Enlace:
https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625256/BetetaL_J.pdf?sequence=5&isAllowed=y

[10] Benavides, R. V. (2018). La ciberseguridad y el contexto actual. Pensamiento Conjunto, 6(2), 9-9.
Enlace: http://www.pensamientoconjunto.com.pe/index.php/PC/article/view/82

[11] Cruzado Puente de la Vega, C. F., & Rodriguez Baca, L. S. (2022). Marco de referencia "HOGO" para ciberseguridad en PyMES basado en ISO 27002 y 27032.
Enlace: https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/5200/Carlos_Tesis_Maestro_2022.pdf?sequence=1&isAllowed=y

[12] Machado, F. A. (2018). Ciberseguridad en la infraestructura crítica mediante el sistema SCADA en planta de tratamiento de agua de Lima. Revista Escuela de Guerra del Ejército del Perú, 2(3), 48-55.
http://revistas.esge.edu.pe/RESGE/article/view/30

[13] Poma, A., & Vargas, R. (2019). Problemática en ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el mundo. Sciéndo, 22(4), 275-282.
Enlace: https://revistas.unitru.edu.pe/index.php/SCIENDO/article/view/2692

Roles de Autoría

Edwin Daniel León Gutierrez: Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Cynthia Mayumi Tesillo Gomez:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Yuri Alexander Escobar Arcaya:** Análisis formal, Investigación, Metodología, Redacción - borrador original. **Luis Antonio Godoy Montoya:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original.