INFORME DE VIGILANCIA TECNOLÓGICA

SOFTWARE
Ciberseguridad

Patentes de invención, investigaciones y tendencias

DEPARTAMENTO DE INTELIGENCIA DE MERCADOS

1. INTRODUCCIÓN

La Ciberseguridad se relaciona con la protección de sistemas, datos muchos de los cuales son confidenciales, software y hardware a fin de evitar el hurto de los mismos.

Dado que en los últimos años, la nube o computación en la nube ha tomado fuerza en los últimos años dado que son tecnologías a nivel global que comprende servidores con funciones específicas y que están conectados para funcionar como un gran ecosistema único[1], sirve para el almacenamiento y gestión de datos, la ejecución de programas o aplicaciones a fin de brindar servicios a los usuarios de la red global facilitando el acceso a la información desde cualquier dispositivo conectado alámbrica o inalámbricamente a la red.

La nube se caracteriza por tener características tales como ubicuidad, escalabilidad y elasticidad ya que los recursos de la nube son ilimitados gracias a que su tecnología se adapta a la carga de datos ingresados a ella a través de internet, sin importar donde se encuentre la empresa y el usuario, y su capacidad de computación en sus programas y aplicaciones. Otras características observadas son su rendimiento y mantenimiento toda vez que todos los recursos se encuentran disponibles para optimizar el resultado final y sus sistemas son mantenidos automáticamente con lo cual se optimizan los tiempos.[2]

La nube cobra relevancia en la presente crisis mundial, a que "Según la Encuesta de Computación en la Nube 2020, realizada por IDG, el 59% de los encuestados dijo que sus organizaciones planean usar servicios en la nube dentro de los próximos 18 meses. Entre tanto, un 38% confirma ya estar en la nube[3], lo cual es evidente por la crisis generada por la COVID-19 que implica medidas de aislamiento social, con lo cual las empresas han tenido que enfrentar retos de continuidad en sus operaciones para garantizar el acceso remoto a la información. Existen tres clases de nube: públicas, privadas e híbridas.

En este sentido, la ciberseguridad también es un hecho importante de considerar, ya que esta abarca desde los datos e información digital propias del software hasta la protección de los sistemas interconectados[4] A pesar de que los servidores en la nube cuentan con altos estándares de protección en el mundo de internet, se conoce de ciberataques, principalmente para medianas y pequeñas empresas que no cuentan con una infraestructura sofisticada y resulta importante

conocer la manera como la nube está transformando la manera en la cual los usuarios consumen la tecnología y los desafíos en temas de seguridad.

"Los principales proveedores de servicios en la nube como Amazon Web Services o Google Cloud, sobre los cuales operan gran parte de los servidores en la nube ofrecidos en el mercado, han abordado de manera proactiva sus controles de seguridad realizando verificaciones independientes

[1] https://www.infosecuritymexico.com/es/blog/nube-y-ciberseguridad.html
[2] Idem
[3] https://computerworld.co/migrar-a-la-nube-en-tiempos-de-pandemia/
[4] https://mrhouston.net/blog/ciberseguridad-en-la-nube/

de las políticas de seguridad, privacidad y cumplimiento, poniendo estos informes a disposición del público."[5]

[5] https://www.webdoxclm.com/como-funciona-la-ciberseguridad-en-la-nube

2. RESUMEN

El presente documento proporciona información obtenida del proceso de vigilancia tecnológica en las cuales se muestran las principales investigaciones, tesis peruanas, proyectos financiados, patentes internacionales y aquellas que han sido solicitadas en Perú que solicitaron protección en nuestro país, así como nuevos productos, y noticias de interés que surgieron durante el transcurso del año 2021, relacionados a nuevos productos y productos de valor agregado relacionados con la ciberseguridad para soluciones basadas en la nube.

Se utilizó como fuente las patentes ya que éstas contienen información actualizada sobre todas las tecnologías desarrolladas en el mundo. Si bien, el software no es patentable en países de latinoamérica, como por ejemplo, Perú y Colombia, este tipo de tecnología es susceptible de protección en países como Estados Unidos, China e india entre otros, mediante patente, lo cual permite encontrar documentos de patente en dichos países, principalmente en EE.UU, que es uno de los mercados más apetecibles para temas de Software.

La búsqueda se realizó mediante el motor privado PATBASE que accede a la información de prácticamente todas las oficinas de Propiedad Intelectual en el mundo haciendo que este motor sea uno de los más fiables para la búsqueda de tecnologías en cualquier sector. La selección de los documentos relevantes fue realizada utilizando ecuaciones de búsqueda en función a los resultados de un taller y encuestas realizadas con empresas peruanas exportadoras de productos y/o servicios de software, las mismas que fueron operativizadas con el PatBase[6].

Los principales resultados obtenidos fueron los siguientes:

- Desde el año 2010 a la fecha se encontró un número total de 4.071 familias de patentes relacionadas con el tema de Ciberseguridad para un total de 16.717 solicitudes de patente a nivel mundial.
- Estados Unidos, China, Japón, Canadá, Australia, India y Reino Unido, son los principales países en donde se ha registrado un alto número de patentes relacionadas a la industria de software con énfasis en su aplicación al sector ciberseguridad.
- La industria de software aplicado al sector de ciberseguridad mantiene una tendencia creciente a nivel mundial y con un comportamiento casi exponencial.
- Existen distintas tecnologías relacionadas al software y con aplicación a la ciberseguridad que pueden constituir nichos de desarrollo para empresas peruanas a través de la expansión e internacionalización de sus desarrollos (productos y/o servicios).

[6] PatBase es una de las principales herramientas de búsqueda confiable a nivel mundial. Constituye una sólida base de datos de patentes en la que buscar, revisar, compartir y analizar información sobre patentes y literatura no relacionada con patentes de importancia empresarial.
Ofrece acceso a más de 140 millones de patentes y documentos relacionados de más de 105 países, actualizados semanalmente. Organizado en más de 75 millones de familias de patentes, lo que ahorra tiempo y reduce la duplicación.

3. EL SOFTWARE Y LAS PATENTES

Según el instituto de Ingenieros Eléctrico y Electrónicos (IEEE sus siglas en inglés) el software el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación (extraído del estándar 729 del IEEE). Teniendo en cuenta que el software es un producto del intelecto humano, es claro que debe ser protegido por alguna de las vías de Propiedad Intelectual.

Sin embargo, clasificar el software dentro de una categoría de protección intelectual existente ha resultado un reto desde su aparición, toda vez que se ha considerado protegible mediante Derechos de Autor ya que puede verse como una obra literaria de una idea plasmada a través de un lenguaje entendido por una computadora, pero que es escrito por un ser humano (por ejemplo, un ingeniero electrónico). No obstante, a diferencia de una obra literaria convencional, el software comprende elementos como las líneas del código que tienen una función que no depende de su construcción gramatical y el código fuente del programa, que pueden ser diferentes a los de otro software y sin embargo, realizar la misma función y producir un resultado similar [7] a través de su puesta en práctica mediante la utilización de un computador, una red informática u otro aparato programable en los que la ejecución del programa informático produce un efecto técnico que forma parte de una solución a un problema técnico planteado[8].

Teniendo en cuenta esta última consideración que han tenido muchas oficinas de propiedad intelectual en el mundo, el software tiene entonces la oportunidad de hacer parte de tecnologías que cumplan con la característica de ser implementadas por un ordenador y que brinden una solución a un problema técnico, en donde las funcionalidades proporcionadas por el software pueden considerarse como caractericen intrínsecas de una invención implementada por un ordenador. Por esta razón, las invenciones, en todos los campos de la tecnología que comprendan para su realización la aplicación de un software, pueden optar por la protección vía patente ante oficinas de propiedad intelectual a nivel mundial.

Gracias a estas consideraciones se logra entonces realizar la búsqueda en PatBAse de invenciones basadas en aplicación de software para el sector de Ciberseguridad a través de ecuaciones de búsqueda que comprenden palabras claves como, por ejemplo “software”, “cybersecurity”, “artificial intelligence”, “cloud”; “cyber*” y “security” combinadas con los códigos de clasificación internacional de patentes como, por ejemplo “G06” para computación, cálculo; G11 almacenamiento de información y G16 tecnologías de información y comunicación, entre otras clasificaciones utilizadas en la búsqueda.

Teniendo en cuenta esta información fundamental sobre el software y las patentes, se detalla a continuación las estrategias de búsqueda llevada a cabo para la realización del presente informe

Se diseñaron las ecuaciones de búsqueda siguientes, en donde también se utilizaron los códigos de clasificación de patentes, se encontró información relevante relacionada con la actividad de desarrollo de tecnologías relacionadas con la ciberseguridad:

Ec1	TAC=(software AND cybersecurity) AND FT=(cloud AND vulnerability)

[7] https://www.wipo.int/wipo_magazine/es/2008/06/article_0006.html

[8] https://www.sic.gov.co/ruta-pi/mayo31/por-que-se-patentan-las-invenciones-implementadas-por-computador

Ec2	FT=(software AND cybersecurity) AND FT=(cloud AND vulnerability)
Ec3	FT=(software AND cyber AND security) AND FT=(cloud)
Ec4	FT=(software AND cyber AND security) AND FT=(cloud) NOT IC8=(B60 OR G09 OR H02)

Los códigos utilizados en la Ec4, corresponde a los códigos de los campos de la Clasificación Internacional de Patentes (IPC por sus siglas en inglés)[9]

Desde el año 2010 a la fecha se encontró un número total de 4071 familias de patentes relacionadas con el tema de ciberseguridad en la nube para un total de 16.717 solicitudes de patente a nivel mundial.

En la figura 1 más abajo, se puede apreciar la tendencia de incremento de solicitudes de patente relacionadas con ciberseguridad en la nube, en donde se puede apreciar un aumento exponencial de solicitudes de patentes desde el año 2012 hasta alcanzar un pico importante de aproximadamente 2.250 solicitudes en el año 2018, lo cual concuerda con los avances tecnológicos relacionado con el software para empresas y sus aplicaciones en la nube. Se observa también una caída de solicitudes para el año 2019, lo cual puede ser debido al tiempo de publicación de las mismas que corresponde a 18 meses luego de su presentación y a temas relacionados con la pandemia de la COVID-19.

También se puede apreciar que la velocidad de concesión respecto a la solicitud de patente, en promedio es casi la mitad, lo cual significa que las oficinas de propiedad intelectual en el mundo están brindando importancia a las tecnologías relacionadas con la ciberseguridad.

[9] Para mayor detalles, ingresar a la página de la Organización Mundial de Propiedad Intelectual: https://www.wipo.int/classifications/ipc/ipcpub/

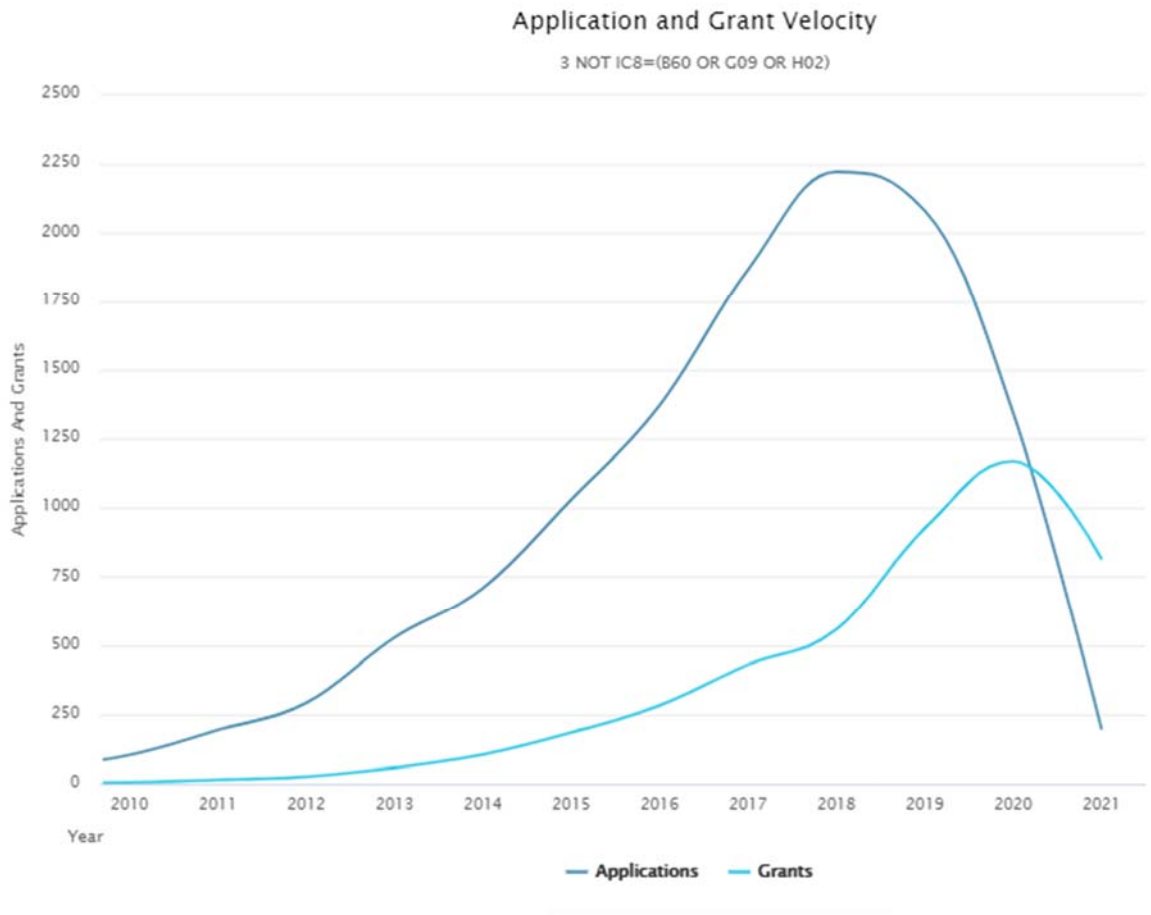

Figura 1
Elaboración y Fuente: Mertz Perú, a través de PatBase

Adicionalmente, en la figura 2 se observa que la concentración de solicitudes de patente a nivel mundial se halla en Estados Unidos, China, Japón, Reino Unido, Canadá, Australia e India.

Figura 2
Elaboración y Fuente: Mertz Perú, a través de PatBase

A continuación, se mencionan los países en donde se presenta la mayor cantidad de solicitudes de patente relacionadas con este tema:

País	Solicitudes de patente	Solicitudes concedidas
Estados Unidos	6.489	3.660
China	530	139
Japón	326	127
Canadá	308	47
Australia	289	103
India	280	6
Reino Unido	142	38

En relación con esta tabla se puede apreciar que el 60% de las solicitudes de patente a nivel mundial se presentan en Estados Unidos y el resto se reparten en los países como China, Japón, Canadá, Australia, India, Reino unido y Europa. Estados Unidos por ser un país generador y consumidor de esta clase de tecnología se ha convertido en una geografía de presentación y protección interesante tanto para solicitantes de ese país como para otros solicitantes que no pertenecen a dicho país.

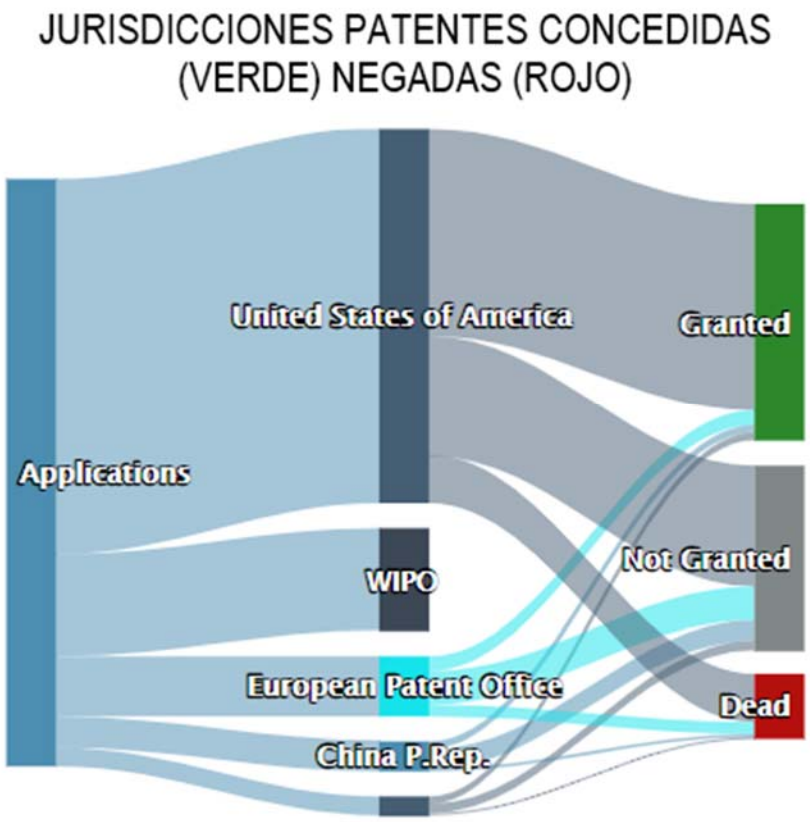

Figura 3
Elaboración y Fuente: Mertz Perú, a través de PatBase

En relación con la proporción de presentación de solicitudes y la concesión de patentes, como se puede observar en la figura 3, Estado Unidos es el principal país donde se presenta la mayor cantidad de solicitudes con un promedio del 56% de concesión de dichas solicitudes.

Respecto a los solicitantes de patentes, se encontró como principal a la empresa Strong Force IOT Portafolio LLc, seguida de IBM y Nokia Technologies OY como se muestra en la siguiente figura 4 :

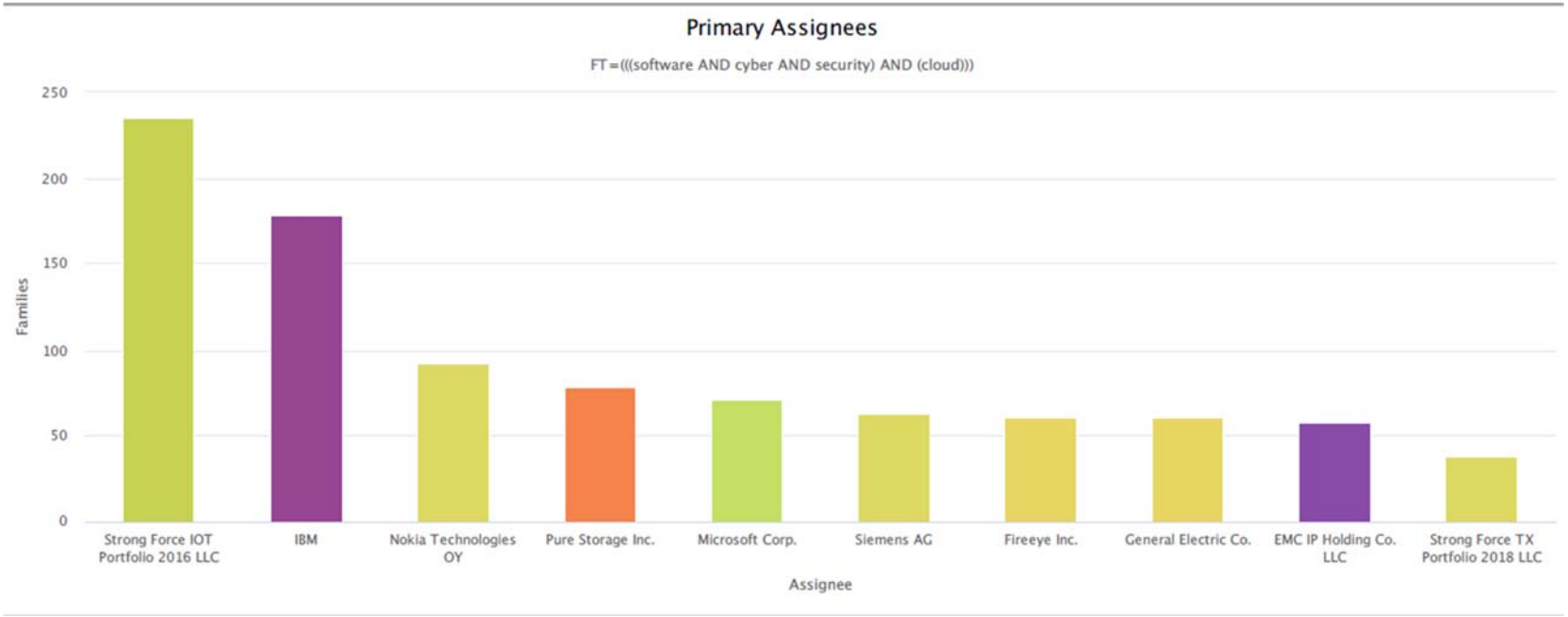

Figura 4
Elaboración y Fuente: Mertz Perú, a través de PatBase

4. PRINCIPALES ARTÍCULOS DE INVESTIGACIÓN

Título: CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments
Autores: Tiago Gasiba et al
Publicado en CyberSecurity Challenges for industrial Software Developers

Descripción: El conocimiento de los temas de ciberseguridad facilita a los desarrolladores de software la producción de código seguro. Esta conciencia es especialmente importante en entornos industriales para los productos y servicios en infraestructuras críticas. En este trabajo, se aborda cómo dar a conocer el software a los desarrolladores sobre el tema de la codificación segura. Se propone la "Desafíos de Ciberseguridad", un juego serio diseñado para ser utilizado en un entorno industrial y abordar las necesidades de los desarrolladores de software. En el estudio se extrae la experiencia adquirida en la realización de estos Desafíos de Ciberseguridad en un entorno industrial. Las principales aportaciones son el diseño de los Desafíos de CyberSecurity de eventos, análisis de los beneficios percibidos y consejos para los profesionales que deseen diseñar o perfeccionar estas prácticas.

Enlace: https://arxiv.org/pdf/2102.05345.pdf

Título: A treat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs
Autores: Max van Haastrecht et al
Publicado en ARES 2021, August 17–20, 2021, Vienna, Austria

Descripción: Los incidentes de ciberseguridad son comunes hoy en día, y las pequeñas empresas medianas (PYMES) son objetivos excepcionalmente vulnerables. La falta de recursos de ciberseguridad a disposición de las pymes implica que son menos capaces de hacer frente a los ciberataques. La motivación para mejorar la ciberseguridad suele ser baja, ya que el conocimiento y la conciencia necesarios para impulsar la motivación son generalmente escasos en las pymes. Una solución que tiene como objetivo ayudar a las pymes a gestionar sus riesgos de ciberseguridad no solo deben ofrecer una evaluación correcta, sino que también deben motivar a los usuarios de las PYME. De la Teoría de autodeterminación (TED), se sabe que al promover la autonomía percibida, competencia y parentesco, las personas pueden estar motivadas para actuar. En este artículo, se explica cómo una ciberseguridad basada en amenazas. El enfoque de evaluación de riesgos puede ayudar a abordar las necesidades descritas en SDT. Proponemos un enfoque de este tipo para las PYME y esbozamos el requisitos de datos que faciliten la automatización. Presentamos una aplicación práctica que cubre varias interfaces de usuario, mostrando cómo nuestro El enfoque de evaluación de riesgos de ciberseguridad basado en amenazas convierte a las PYME datos en recomendaciones priorizadas y procesables.

Enlace: https://dl.acm.org/doi/pdf/10.1145/3465481.3469199

Título: Cybersecurity: Risks, Vulnerabilities and countermeasures to prevent social engineering attacks
Autores: Nabie Y. Conteh et al
Publicado en International Journal of Advanced Computer Research

Descripción: Se evalúan las vulnerabilidades de la tecnología de la información de una organización e infraestructura, que incluye sistemas de hardware y software, medios de transmisión, redes de área local, redes de área amplia, redes empresariales, intranets y su uso de Internet para las intrusiones cibernéticas. Para lograr este objetivo, el artículo intenta explicar la importancia y el papel de la ingeniería social en las intrusiones en la red y el robo cibernético. También analiza con gran detalle las razones de la rápida expansión del ciberdelito.

Enlace: https://www.researchgate.net/profile/Nabie-Conteh-2/publication/294421084_Cybersecurityrisks_vulnerabilities_and_countermeasures_to_prevent_social_engineering_attacks/links/56e2733408aebc9edb19eebc/Cybersecurityrisks-vulnerabilities-and-countermeasures-to-prevent-social-engineering-attacks.pdf

Título: Design of Secure Coding Challenges for Cybersecurity Education in the Industri
Autores: Tiago Gasiba et al
Publicado en eprint arXiv:2101.02108 computer Science/Software Engineering

Descripción: De acuerdo con una encuesta reciente con más de 4000 desarrolladores de software, menos de la mitad de los desarrolladores pueden detectar brechas de seguridad. Como resultado, los productos de software presentan una baja calidad de seguridad expresada por vulnerabilidades que pueden ser explotadas por los ciberdelincuentes. Esta falta de calidad y seguridad es particularmente peligrosa si el software que contiene las vulnerabilidades se implementa en infraestructuras críticas. Los eventos Capture-the-Flag (CTF) han mostrado resultados prometedores en la mejora de la conciencia de codificación segura de los desarrolladores de software en la industria.

Enlace: https://ui.adsabs.harvard.edu/abs/2021arXiv210102108E/abstract

5. PRINCIPALES ARTÍCULOS COMERCIALES

Título: Ciberseguridad para pequeñas empresas 101: consejos sencillos para proteger sus datos

Descripción: CEO de LegalShield e IDShield, protegiendo y empoderando a las personas a través de pLos ciberdelincuentes no solo persiguen a las grandes corporaciones. Por cada Equifax o Colonial Pipeline sobre el que lee en las noticias, hay miles de pequeñas empresas que han visto comprometida la información confidencial de su empresa o de sus clientes.lanes legales y soluciones de gestión de privacidad.

Fuente: https://www.forbes.com/sites/forbestechcouncil/2021/06/14/small-business-cybersecurity-101-simple-tips-to-protect-your-data/?sh=7e3eef744679

Título: La ciberseguridad no es (solo) un problema tecnológico

Descripción: El trabajo remoto durante la pandemia ha significado que las organizaciones tuvieran que acelerar rápidamente sus esfuerzos de ciberseguridad. Pero asegurar el trabajo remoto no es solo el trabajo del equipo de TI: en última instancia, las empresas deben hacer que la seguridad sea parte de la descripción de cada trabajo. Y el ingrediente clave para que eso suceda es la confianza. El autor, el director de seguridad global de Box, identifica cuatro pasos para mejorar la confianza dentro de una organización: 1) Liderar con empatía; 2) Capacitar a los empleados para que tomen decisiones efectivas; 3) Definir lo que más importa; y 4) Honre las distracciones.

Fuente: https://hbr.org/2021/01/cybersecurity-is-not-just-a-tech-problem

Título: ¿Por qué es importante la ciberseguridad en 2021?

Descripción: La ciberseguridad es importante porque protege todas las categorías de datos contra robos y daños. Esto incluye datos confidenciales, información de identificación personal (PII) , información de salud protegida (PHI), información personal, propiedad intelectual, datos y sistemas de información gubernamentales y de la industria. Sin un programa de ciberseguridad, su organización no puede defenderse de las campañas de violación de datos, lo que la convierte en un objetivo irresistible para los ciberdelincuentes.

Fuente: https://www.upguard.com/blog/cybersecurity-important

Título: Informes mejorados de ciberriesgos: abriendo puertas a la ciberseguridad basada en riesgos

Descripción: Los nuevos sistemas de información de gestión de riesgos cibernéticos brindan a los ejecutivos la transparencia de riesgos que necesitan para transformar la ciber resiliencia organizacional.

Fuente: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/enhanced-cyberrisk-reporting-opening-doors-to-risk-based-cybersecurity

Título: La importancia de la ciberseguridad en los negocios

Descripción: Cada año marca otro "peor año" para los ataques cibernéticos en todo el mundo, y las empresas canadienses no han sido inmunes a esos ataques. La buena noticia es que se estima que el 93% de todas las infracciones se pueden evitar si se toman medidas simples. Es por eso que los programas preventivos introducidos por Chubb son tan críticos para evitar problemas masivos en el futuro.

Fuente: http://www.bbc.com/storyworks/chubb-future-proof/the-importance-of-cybersecurity-in-business

Título: Ciberseguridad para pequeñas empresas

Descripción: Internet permite a las empresas de todos los tamaños y desde cualquier ubicación llegar a mercados nuevos y más grandes y brinda oportunidades para trabajar de manera más eficiente mediante el uso de herramientas informáticas. Ya sea que una empresa esté pensando en adoptar la computación en la nube o simplemente usar el correo electrónico y mantener un sitio

web, la ciberseguridad debe ser parte del plan.

Fuente: https://www.fcc.gov/general/cybersecurity-small-business

Título: Transformando la ciberseguridad. Nuevos enfoques para un panorama de amenazas en evolución

Descripción: Durante los últimos tres años, el crecimiento de los delitos cibernéticos ha continuado, si no se ha acelerado, en la industria de servicios financieros.

Fuente: https://www2.deloitte.com/cl/es/pages/financial-services/articles/transforming-cybersecurity.html

6. PRINCIPALES PATENTES INTERNACIONALES

NÚMERO Y FECHA PUBLICACIÓN: US2020/000758 2 de enero de 2020

Título: MÉTODO Y SISTEMA PARA INCIDENTE DE CIBERSEGURIDAD AUTOMATIZADO Y VISUALIZACIÓN Y CORRELACIÓN DE ARTEFACTO PARA CENTROS DE OPERACIÓN DE SEGURIDAD Y EQUIPOS DE RESPUESTA DE EMERGENCIA POR COMPUTADORA

Solicitante: DFLABS S.P.A.

Aspectos importantes de la invención: Se proporciona un método y un sistema para visualizar y navegar por la información de ciberseguridad. Un hiperárbol se muestra en un dispositivo de visualización de un sistema computarizado. El hiperárbol incluye una pluralidad de nodos vinculados por bordes, uno o más de los nodos que representan incidentes de ciberseguridad y uno o más de los nodos que representan elementos o artefactos de incidentes de ciberseguridad, los bordes representan una relación específica entre los nodos vinculados por los bordes. El sistema computarizado muestra una ayuda de navegación interactiva para permitir que un usuario navegue por el árbol elevado y recibe un comando de navegación del usuario a través de la ayuda de navegación interactiva. El sistema computarizado modifica el árbol hídrico mostrado en respuesta al comando de navegación. El comando de navegación comprende la eliminación selectiva o la restauración de bordes o nodos en el hiperárbol para permitir al usuario visualizar fácilmente las interrelaciones entre los nodos mostrados que son importantes para una investigación o respuesta de ciberseguridad.

Fuente:
https://pdfstore.patentorder.com/getminesoft/630850016/us/20200102/a1/020200/00/75/88/us-20200007588-a1-20200102/us2020007588.pdf

NÚMERO Y FECHA PUBLICACIÓN: WO2018/136944 26 de julio de 2018

Título: MÉTODO Y DISPOSITIVO PARA GESTIONAR LA SEGURIDAD EN UNA RED DE COMPUTADORAS

Solicitante: HASAN Syed

Aspectos importantes de la invención: El método y el dispositivo para gestionar la seguridad en una red informática incluyen algoritmos de crecimiento de inteligencia iterativa, evolución iterativa y vías de evolución; subalgoritmos de identificación de tipo de información, detección de conspiración, escáner de medios, análisis de aislamiento de privilegios, gestión de riesgos de usuarios y gestión de entidades extranjeras; y módulos de comportamiento de seguridad, creatividad, amenaza artificial, guía de crecimiento automatizado, analizador genérico / de respuesta, módulo de revisión de seguridad y sistema de interacción de monitoreo. Las aplicaciones incluyen seguimiento predictivo de malware, retribución de inteligencia de máquinas clandestinas a través de operaciones encubiertas en el ciberespacio, defensa en tiempo real de base de datos cero deducida lógicamente, protección de infraestructura crítica y retribución a través de la nube y seguridad de la información por niveles, y memoria y percepción del pensamiento crítico.

Fuente: https://pdfstore.patentorder.com/pdf/wo/944/wo18136944.pdf

NÚMERO Y FECHA PUBLICACIÓN: US2021/0029029 28 de junio de 2021

Título: ARQUITECTURA DE RED DEFINIDA POR SOFTWARE INDUSTRIAL PARA EL DESPLIEGUE EN UN SISTEMA DE AUTOMATIZACIÓN DEFINIDO POR SOFTWARE

Solicitante: Schneider Electric Industries S.A.S

Aspectos importantes de la invención: Se describe una arquitectura, un sistema y métodos de red definida por software industrial (SDN) para la gestión centralizada y simplificada de una red industrial. La arquitectura SDN industrial se compone de un plano de infraestructura que incluye dispositivos físicos y virtuales, un plano de control que comprende controladores para controlar y administrar los dispositivos físicos y virtuales en el plano de infraestructura, los controladores lógicamente centralizados que incluyen un controlador de red, un controlador de gestión de virtualización y una ciberseguridad, un plano de aplicación que comprende una o más aplicaciones industriales de usuario final, y un plano de plataforma que comprende un conjunto de servicios de software e interfaces de programación de aplicaciones (API) para definir una interfaz de comunicación al plano de aplicación al norte y al plano de control al sur para proporcionar una aplicación industrial en el plano de aplicación, acceso programático a uno o más de la pluralidad de controladores en el plano de control para una gestión simplificada y centralizada de la red industrial.

Fuente: https://pdfstore.patentorder.com/pdf/us/029/us2021029029.pdf

NÚMERO Y FECHA PUBLICACIÓN: US11,075,930 27 de julio de 2021

Título: SISTEMA Y MÉTODO DE DETECCIÓN DE ATAQUES REPETITIVOS DE CIBERSEGURIDAD CONSTITUYENDO UNA CAMPAÑA DE CORREO ELECTRÓNICO

Solicitante: FIREEYE, INC

Aspectos importantes de la invención: Se proporciona un sistema para detectar una campaña de correo electrónico, incluye lógica de extracción de características, lógica de preprocesamiento, lógica de análisis de campaña y un motor de informes. La lógica de extracción de características obtiene características de cada uno de una pluralidad de mensajes de correo electrónico maliciosos recibidos para su análisis, mientras que la lógica de preprocesamiento genera una pluralidad de representaciones de correo electrónico que están dispuestas en una secuencia ordenada y corresponden a la pluralidad de mensajes de correo electrónico maliciosos. La lógica de análisis de campaña determina la presencia de una campaña de correo electrónico en respuesta a un número prescrito de representaciones de correo electrónico sucesivas que se correlacionan entre sí, donde los resultados de la detección de la campaña de correo electrónico se proporcionan a un administrador de seguridad a través del motor de informes.

Fuente: https://pdfstore.patentorder.com/pdf/us/930/us11075930.pdf

NÚMERO Y FECHA PUBLICACIÓN: US2021/0224388 22 de julio de 2021

Título: APARATO Y APLICACIÓN DE PROTECCIÓN DE DATOS E INFORMACIÓN

Solicitante: MAN SCIENCES INC

Aspectos importantes de la invención: Se proporciona un sintetizador de autoprogramación con comportamiento neuroplástico que usa enlace variable y sustitución que, al ingresar un dato **n**, produce un nuevo algoritmo f(n) y también afecta un algoritmo existente f(n). El sintetizador comprende al menos un metal desnudo y una plétora de coprocesadores, un cálculo de inferencia implementado en lógica reprogramable. El sintetizador también puede incluir un microvisor, conversión de analógico a digital y salidas de digital a analógico para algunas aplicaciones. Además, el sintetizador puede incluir un generador de frecuencia de reloj interno o externo separado. La porción de plasticidad proporcionada por el cálculo de inferencia agrega una inteligencia artificial reconfigurable. La invención combina la detección dinámica de amenazas con el control directo de los recursos del sistema para detectar y mitigar las amenazas y proteger el sistema de un ciberataque**.**

Fuente: https://pdfstore.patentorder.com/pdf/us/388/us2021224388.pdf

NÚMERO Y FECHA PUBLICACIÓN: US2021/0092097 25 de marzo de 2021

Título: LISTA BLANCA PARA COMUNICACIONES HART EN UN SISTEMA DE CONTROL DE PROCESOS

Solicitante: FISHER ROSEMOUNT SYSTEMS INC

Aspectos importantes de la invención: Un sistema de ciberseguridad para su uso en una planta de proceso que proporciona una lista blanca de comandos de lectura HART de práctica común y específicos del dispositivo en los controladores de proceso y los controladores de seguridad para realizar comunicaciones muy seguras en una planta de proceso, pero que aún permiten la implementación de la funcionalidad avanzada proporcionada en dispositivos HART. Una aplicación de implementación de lista blanca que aplica una o más listas blancas en un dispositivo de puerta de enlace de seguridad para determinar si los mensajes, como los mensajes HART, deben permitirse o procesarse. Una aplicación de aprendizaje de lista blanca crea y configura automáticamente listas blancas mediante el uso de un modo de bloqueo/aprendizaje, y una aplicación de configuración de lista blanca que descubre los comandos HART de práctica común y específicos del dispositivo emitiendo solicitudes de descripción de dispositivos a dispositivos específicos, analizando la respuesta y comunicando la configuración de la lista blanca información con los tipos de comando analizados a los controladores de proceso relevantes y controladores de seguridad para su uso en las listas blancas. Una interfaz de usuario permite a los usuarios interactuar y guiar el proceso de configuración para proporcionar un sistema altamente seguro que aún permite el diagnóstico y otras funciones de alto nivel de los dispositivos de campo en una planta de proceso.

Fuente: https://pdfstore.patentorder.com/pdf/us/097/us2021092097.pdf

NÚMERO Y FECHA PUBLICACIÓN: US2021/0216642 25 de julio de 2021

Título: ANÁLISIS DE SENTIMIENTOS PARA ASEGURAR EL CÓDIGO DE COMPUTADORA

Solicitante: BANK OF AMERICA

Aspectos importantes de la invención: Se proporcionan sistemas y métodos para implementar el análisis de sentimientos de código de computadora. Los desarrolladores que escriben código fuente pueden incluir comentarios u otros artefactos del lenguaje natural en el código fuente. Estos artefactos pueden ser ilustrativos de amenazas de ciberseguridad actuales o heredadas. Los sistemas y métodos pueden extraer comentarios y/u otros artefactos de código, con el doble propósito de detección y mitigación de amenazas de ciberseguridad. Se puede aprovechar el análisis de código avanzado para una comprensión más profunda de los sentimientos expresados por los artefactos. Tal sentimiento puede incluir sentimientos negativos expresados en la selección de códigos de error y/o descripciones. Toda la información recuperada es preferiblemente independiente de la identidad humana de acuerdo con el cumplimiento de la regulación de datos personales.

Fuente: https://pdfstore.patentorder.com/pdf/us/642/us2021216642.pdf

NÚMERO Y FECHA PUBLICACIÓN: WO2021/138591 8 de julio de 2021

Título: MARCO DE MITIGACIÓN DE VULNERABILIDADES DE SEGURIDAD

Solicitante: BATTELLE MEMORIAL INSTITUTE

Aspectos importantes de la invención: Se proporcionan sistemas, métodos y medios informáticos para mitigar las vulnerabilidades de seguridad cibernética de los sistemas. La madurez actual de la seguridad cibernética de un sistema se puede determinar en función de los criterios de madurez. Los criterios de madurez se pueden clasificar según la importancia. Los candidatos a soluciones para aumentar la madurez de la seguridad cibernética del sistema se pueden determinar en función de la clasificación. Los candidatos a la solución especifican niveles de ciberseguridad para los criterios de madurez. Se puede calcular un valor de estado actual que refleje la madurez actual de la ciberseguridad del sistema. Para los candidatos a la solución, se puede determinar un valor de estado de implementación y un valor de estado de transición. El valor del estado de implementación representa la implementación de los niveles de madurez del candidato de solución, y el valor del estado de transición representa una transición del valor del estado actual al valor del estado de implementación. Según los valores del estado de transición, se puede seleccionar una solución candidata para el sistema y el sistema se puede modificar en consecuencia.

Fuente: https://pdfstore.patentorder.com/pdf/wo/591/wo21138591.pdf

---

NÚMERO Y FECHA PUBLICACIÓN: US2021/0211452 8 de julio de 2021

Título: GESTIÓN DE RIESGOS DE CIBERSEGURIDAD DE UN DISPOSITIVO

Solicitante: BATTELLE MEMORIAL INSTITUTE

Aspectos importantes de la invención: Se describe un método para implementar la gestión de riesgos de ciberseguridad para dispositivos conectables a la red. El método implica la evaluación de riesgos y la vulnerabilidad del dispositivo, la corrección de riesgos, la detección de riesgos y la respuesta a incidentes. La evaluación de la vulnerabilidad y el riesgo considera tanto factores técnicos como humanos. El método también incluye el uso de métodos de crowdsourcing, como juegos y gamificación, de forma independiente o en combinación con otras tecnologías para el desarrollo de inventarios, la evaluación de riesgos y la detección de riesgos. La remediación / mitigación de riesgos y la respuesta a incidentes incluyen roles priorizados y ejecución basada en habilidades de controles de seguridad y respuestas a incidentes, donde los controles de seguridad y las respuestas a incidentes se pueden seleccionar entre múltiples opciones según la efectividad y el costo. El método implica además la gobernanza del proceso de gestión de riesgos en una entidad.

Fuente: https://pdfstore.patentorder.com/pdf/us/452/us2021211452.pdf

7. PRINCIPALES PATENTES SOLICITADAS EN PERÚ

No se registraron patentes internacionales solicitadas en Perú en el último semestre. Sin embargo, se encontraron las siguientes solicitudes:

Numero	Título	Solicitante	Estado
PE00982016(2014)	SISTEMA DE INTERACCIÓN Y TRANSMISIÓN DE DATOS DE CONTENIDO SIMULTÁNEO	GIGA ENTERTAINMENT MEDIA INC	
PE12422015 (2013)	DEFENSA DE RED EMERGENTE	GEORGE WASHINGTON UNIV	

NÚMERO Y FECHA PUBLICACIÓN: PE00982016 17 de julio de 2014

Título: SISTEMA DE INTERACCIÓN Y TRANSMISIÓN DE DATOS DE CONTENIDO SIMULTÁNEO.

Solicitante: GIGA ENTERTAINMENT MEDIA INC

Aspectos importantes de la invención: Un método y sistema implementado por computadora distribuye simultáneamente flujos de datos de contenido (CDS) de múltiples formatos de contenido, por ejemplo, contenido de televisión por cable en vivo, contenido de juegos, contenido de redes sociales, contenido generado por el usuario, etc., a uno o más dispositivos informáticos. Una plataforma de distribución de contenido interactivo (ICDP) recibe selecciones de usuario de los CDS y los formatos de contenido a través de una interfaz gráfica de usuario (GUI) y recibe uno o más CDS en uno o más formatos de contenido de múltiples fuentes de contenido según las selecciones del usuario. El ICDP sincroniza los CDS codificando los CDS en un formato de datos común y ajustando la velocidad de transmisión de los CDS. El ICDP transmite y muestra simultáneamente los CDS sincronizados en una o más ventanas configurables en una pantalla de visualización de cada dispositivo informático en instancias de tiempo configurables a través de la GUI. El ICDP facilita las interacciones e inicia transacciones entre dispositivos informáticos durante la visualización simultánea de los CDS sincronizados.

Enlace:
https://pdfstore.patentorder.com/getminesoft/697637529/wo/20150820/a8/002014/11/01/92/wo2014110192a8/wo14110192a8.pdf

NÚMERO Y FECHA PUBLICACIÓN: PE12422015 18 de septiembre de 2013

Título: DEFENSA DE RED EMERGENTE

Solicitante: GEORGE WASHINGTON UNIV

Aspectos importantes de la invención: Se proporciona un sistema y un método de un nodo para su uso en una red que tiene una pluralidad de nodos. El nodo está configurado para identificar el (los) nodo (s) vecino (s) dentro de una proximidad predeterminada de dicho nodo, medida por cualquiera de los saltos de red físicos, lógicos, enlace de red o cercanía de análisis de vértices. El nodo determina un nivel de nerviosismo de sí mismo y envía y/o recibe comunicación en cuanto al nivel de nerviosismo a los nodos vecinos.

Enlace:
https://pdfstore.patentorder.com/getminesoft/697653394/wo/20150924/a3/002014/18/23/26/wo20141822326a3/wo14182326a3.pdf

8. PRINCIPALES SERVICIOS DE SOFTWARE SOLICITADOS INTERNACIONALMENTE

sencinet

Descripción: Empresa que conecta personas, empresas y negocios a través de soluciones de comunicación integradas y seguras a través de redes corporativas rápidas, seguras y confiables.

Enlace: ***https://conteudos.sencinet.com***

ManageEngine
Log360

Descripción:: Una solución SIEM integral para Amenazas de combate; Mitigar ataques; Auditar eventos de seguridad y Aseguramiento de datos confidenciales.

Enlace: https://www.manageengine.com/log-management/siem-solution-log360.html?utm_source=Capterra&utm_medium=dest_url&utm_campaign=product_listing_cybersec&capterra_ADAP_ERP_Log360=capterra

Descripción: Empresa que protege los negocios de ciberamenazas y las filtraciones de datos relacionadas con contraseñas.

Enlace: https://www.keepersecurity.com/es_ES/password-manager-free-trial-sign-up.html?utm_source=capterra&utm_medium=referral&utm_campaign=capterra_spanish

Descripción Equipos de seguridad cibernética, estrategia, riesgo, cumplimiento y resiliencia.
Compañía: EY
Enlace: https://www.ey.com/es_co/consulting/cybersecurity-strategy-risk-compliance-resilience

Descripción Plataformas para protección contra el phishing, perfiles falsos en redes sociales, filtraciones de datos**.**
Compañía: AXUR
Enlace: https://axur.com/es/

9. NUEVOS LANZAMIENTOS

A continuación se muestra la información relacionada a los nuevos lanzamientos, que consisten principalmente en start-up que brindan servicios relacionados a ciberseguridad, basado en el desarrollo de software, con distintos enfoques en su modelo de negocio:

Descripción Nueva herramienta que soporta el Sistema de Gestión de Aseguramiento (SGA); consiste en una metodología que permite mediante una serie de procesos, procedimientos y lineamientos elevar el nivel de seguridad de los activos tecnológicos involucrados de las compañías en cuanto a cumplimiento, procesos y gestión del aseguramiento de sus activos tecnológicos.

Compañía: GIOTTO
Enlace: https://2secure.co/productos/giotto/

Descripción Plataforma de ciberseguridad que se encarga de la protección inteligente contra

infracciones. Se encargan de proteger los datos, dispositivos y servicios en la nube de ataques de sus clientes. Además de proteger las credenciales de empleados y clientes resultantes de violaciones de datos de terceros e intentos de adquisición de cuentas (ATO)
Usan una solución poderosa y unificada que combina big data, IA y blockchain asegura su información.
Compañía: HEROIC
Enlace: https://heroic.com/

Descripción: Tecnología que permite implementar múltiples módulos a través de una sola plataforma y un solo agente, ya sea empaquetado o modular con otras herramientas en el tejido de seguridad. Para la seguridad en la red ofrece detección y respuesta de red autónoma, capaz de aprendizaje continuo para predecir, detectar y mitigar los actores de amenazas en la red. Es la diferencia entre recopilar inteligencia frente a actuar automáticamente sobre la base de información procesable en tiempo real, lo que ahorra un tiempo valioso en la respuesta a incidencias. El sistema de protección utiliza inteligencia artificial en los terminales, proporcionando el mismo nivel de protección y comodidad, ya sea que esté trabajando fuera de la oficina o desde casa (seguridad multimodal).
Compañía: AUTHBASE
Enlace: https://sites.google.com/view/authbase/

Descripción Plataforma que cuenta con defensa contra amenazas en tiempo real, visibilidad procesable, cumplimiento continuo en tiempo de ejecución. Detienen el malware, el ransomware, el cryptojacking y las amenazas “comando y control”.
Obtenga visibilidad procesable en las cargas de trabajo, la red y el almacenamiento en la nube. Encuentre configuraciones incorrectas, incumplimiento y actividad no autorizada
Compañía: BLUE HEXAGON
Enlace: https://bluehexagon.ai/

Descripción: Utiliza todo el potencial de las primeras empresas en aprovechar el poder de las capacidades de las Unidad de Procesamiento Gráfico o GPU (graphics processing unit) para combinar la detección de anomalías de inteligencia artificial, la transmisión de video en vivo y el análisis de transmisión para proporcionar los campos de internet de las cosas (IOT) y automoción de seguridad y ciberseguridad definitivos.
Compañía: ATII
Enlace: http://at-instr.com/

Descripción: Comercializa productos basados en Big Data e Inteligencia Artificial, enmarcados en dos gamas diferenciadas: safety y security. Es en esta segunda rama donde Ironchip trabaja para proteger entornos industriales y financieros mediante el uso de “domes” (sitios secretos) capaces de evitar cualquier ataque. También ofrece la posibilidad de acceder a soluciones que se adaptan a las necesidades específicas de cada uno de sus clientes
Compañía: IRONCHIP
Enlace: https://www.ironchip.com/

10. PRINCIPALES TENDENCIAS TECNOLÓGICAS

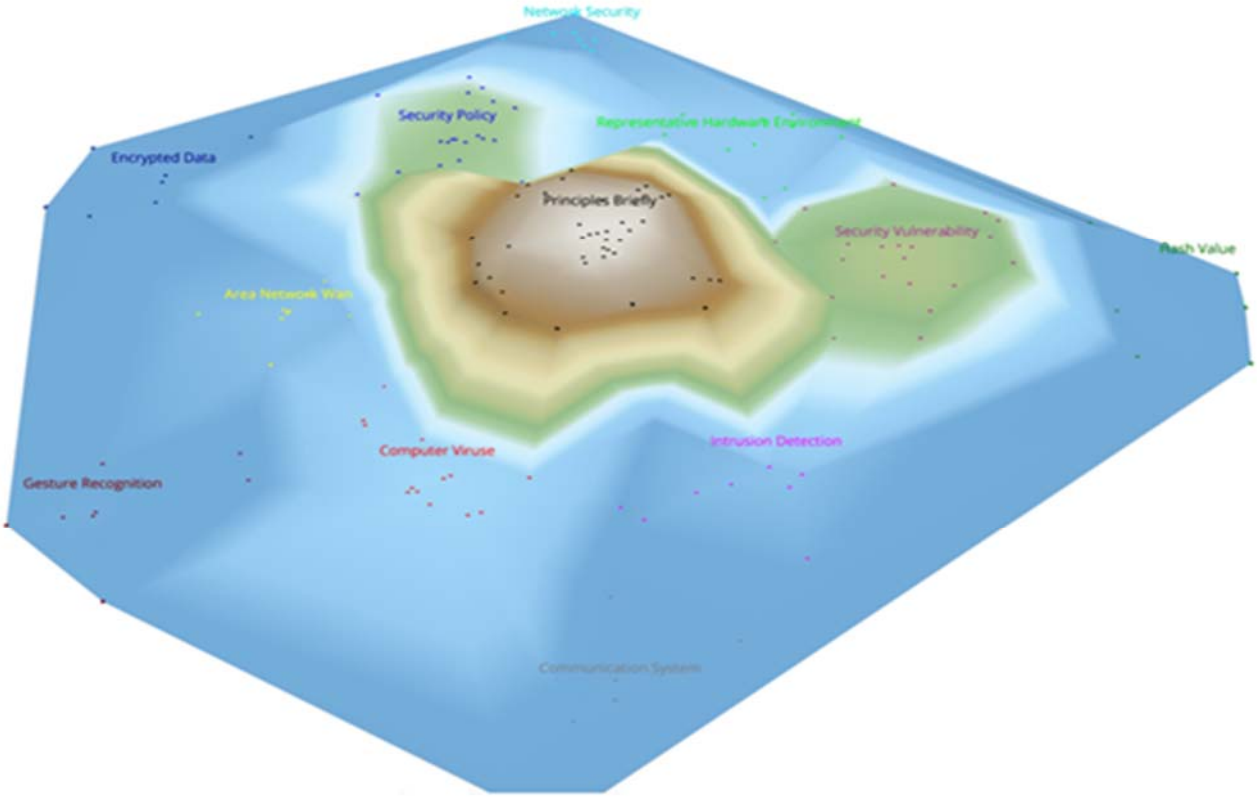

FIGURA 5. Mapa 3D tecnologías relacionadas con Ciberseguridad

En la figura se observa que las tecnologías relacionadas con principios básicos de seguridad son las más agrupadas y utilizadas para este sector, rodeadas de tecnologías para detección de virus de computadora, detección de intrusos, detección de vulnerabilidades de la seguridad, encriptación de datos, políticas de seguridad, valores “flash”, seguridad en la red y reconocimiento gestual.

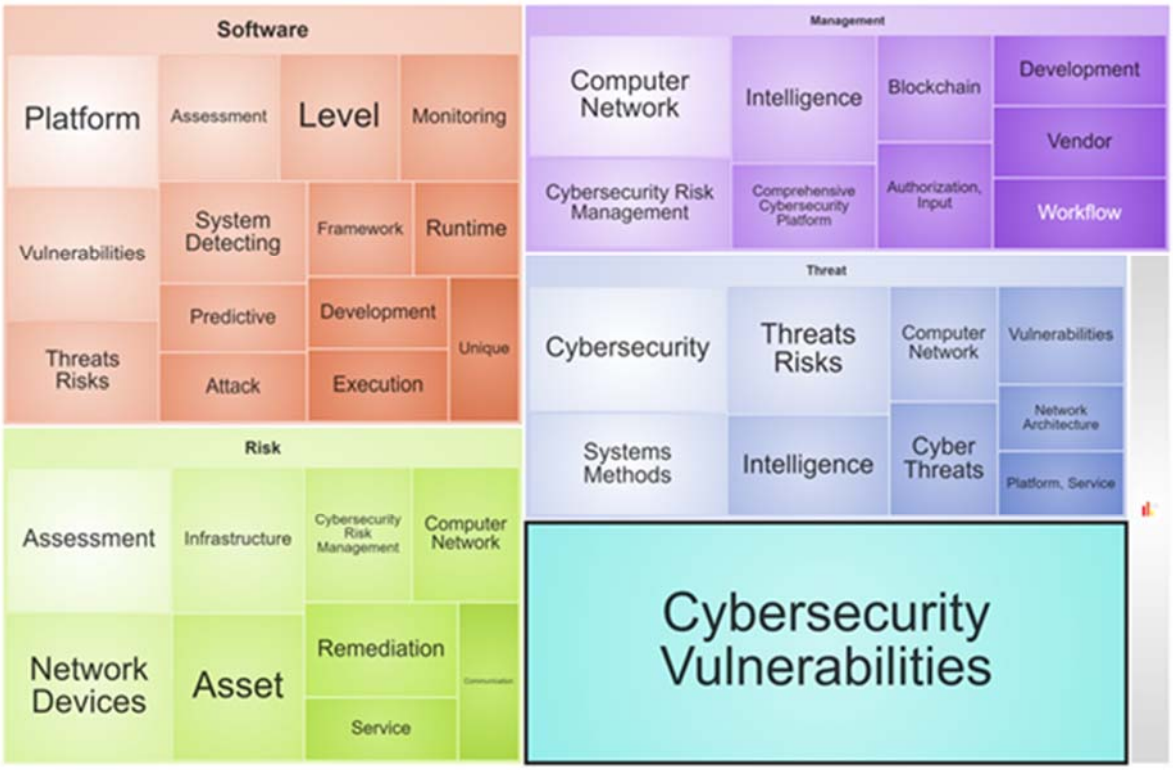

FIGURA 6. Palabras claves relacionadas con Ciberseguridad

De acuerdo con la figura 6, los principales conceptos relacionados con la ciberseguridad se agrupan en Software, administración, administración de riesgos de amenazas, evaluación de riesgos y ataques, seguridad de dispositivos en la red, sistemas de detección de ataques a plataformas y sistemas de seguridad para almacenar información tal como Blockchain, códigos de autorización temporales de acceso tipo Token y plataformas integrales de ciberseguridad.

11. TENDENCIAS TECNOLÓGICAS EN REDES SOCIALES

Para el análisis de redes sociales, se utilizaron las búsquedas en Google Analytic y la plataforma BuzzSumo, con el cual se analizan las tendencias por palabras clave en las búsquedas de Google y distintas interacciones en las redes sociales; esto último, se analizó a través de : Facebook Engagement, Twitter Shares, Pinterest Shares, Reddit Engagements, Número de Links y Evergreen Score.

Para el caso de las búsquedas en Google, se compararon las palabras clave software, cloud y cybersecurity, tal como se muestran en las siguientes figuras

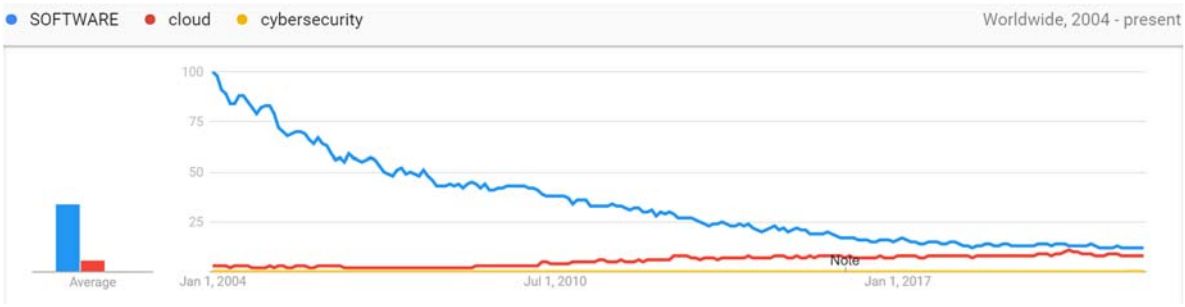

Figura 7 Búsquedas a nivel mundial, en Google, desde el 2014 al presente (20 septiembre)
Fuente: Búsqueda en trends.google.com realizado el 20.09.2021

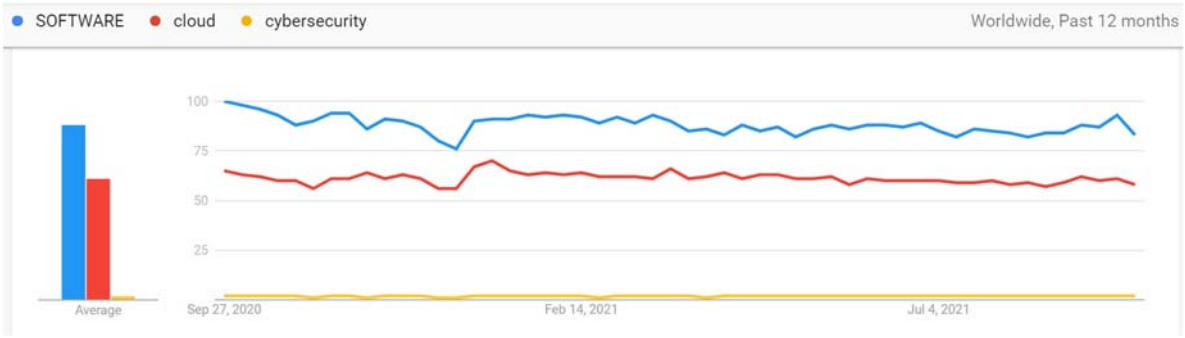

Figura 8 Búsquedas a nivel mundial, en Google, desde septiembre 2020 a la fecha (20 septiembre)
Fuente: Búsqueda en trends.google.com realizado el 20.09.2021

Los números representan el interés de búsqueda en relación con el punto más alto del gráfico para la región y el tiempo dados. Un valor de 100 es el pico de popularidad del término. Un valor de 50 significa que el término es la mitad de popular. Una puntuación de 0 significa que no había suficientes datos para las palabras clave.

Si bien las búsquedas han disminuido en los últimos seis años, es importante prestar atención a los países donde más búsquedas se han realizado, para el cual mostramos los primeros diez (10) países donde más interés se muestran a través de Google:

Figura 9 Países con mayor interés según las búsquedas realizadas
Fuente: Búsqueda en trends.google.com realizado el 20.09.2021

En atención a las redes sociales, se muestran las figuras siguientes:

Figura 10 Contenido web y vinculación con redes sociales (Software, cloud, cybersecurity)
Fuente: Resultados de la búsqueda en https://app.buzzsumo.com/ el día 20.09.2021

Figura 12 Fuente de información tecnológica con mayor tendencia (engagement) a través redes sociales (cloud, cybersecurity)
Fuente: Resultados de la búsqueda en https://app.buzzsumo.com/ el día 20.09.2021

Como se puede observar en las figuras precedentes, la página TheHackersNews, tiene el mayor número de vinculación con las redes sociales, puesto que The Hacker News (THN) es una plataforma de noticias de ciberseguridad líder, confiable y ampliamente reconocida que atrae a más de 8 millones de lectores mensualmente, incluidos profesionales de TI, investigadores, piratas informáticos y tecnólogos.

12. CONCLUSIONES

- Estados Unidos, China, Japón, Canadá, Australia, India y Reino Unido, son los principales países en donde se ha registrado un alto número de patentes relacionadas a la industria de software con énfasis en su aplicación al sector ciberseguridad, los cuales pueden constituirse en los principales países donde empresas del Perú pueden explorar su ingreso, alianzas o representaciones con aliados estratégicos en dichos países.
- La industria de software aplicado al sector de ciberseguridad mantiene una tendencia creciente a nivel mundial y con un comportamiento casi exponencial que posiblemente se mantenga por los siguientes años.
- Existen distintas tecnologías relacionadas al software y con aplicación a la ciberseguridad que pueden constituir nichos de desarrollo para empresas peruanas a través de la expansión e internacionalización de sus desarrollos (productos y/o servicios).
- Las redes sociales tienen un componente global para encontrar tendencias de información relacionada a la ciberseguridad, con énfasis en aplicaciones en la nube; sin embargo, no brindan necesariamente una profundidad técnica o tecnológica, pero si el interés de mercados hacia donde se pueden dirigir los esfuerzos comerciales y herramientas de marketing, que acompañen el desarrollo tecnológico de las empresas que exportan o desean exportar servicios.

13. OTROS DOCUMENTOS DE INTERÉS

- ★ Boletín Tecnológico de Software: Sector Bancario y Financiero
- ★ Boletín Tecnológico de Software: Desarrollo y Arquitectura
- ★ Boletín Tecnológico de Software: Manufactura, Planeamiento y Control
- ★ Boletín Tecnológico de Software: Minería de Datos y Almacenamiento