Volumen 1. Número 3. Serie A
ISBN: 978-99939-0-055-9
ISSN: 2708-1141

CyberSecurity

Información & Privacidad

Resumen de Conferencias

INCIBE Guatemala

OWASP A03:2021-Injection

como Referente para el Desarrollo Seguro de Aplicaciones Web

Aplicabilidad de dominios y controles de Ciberseguridad

en ciudades inteligentes

Ciberseguridad en Centros Educativos Públicos de Guatemala,

un mecanismo para la protección de niños, niñas y adolescentes en el ciberespacio

© Copyright 2020-2022 AUCI

CyberSecurity
Información & Privacidad

CyberSecurity

Información & Privacidad

Proyecto de:

Con financiamiento de:

INCIBE GT
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ISBN: 978-99939-0-055-9

CyberSecurity
Información & Privacidad

Dirección General INCIBE Guatemala
Junta Directiva 2019-2021
Cybersecurity Magazine - Información y Seguridad

Universidad Mariano Gálvez de Guatemala

Ing. Daniela de Villatoro

Ing. Criss Velásquez

Universidad Galileo Guatemala

Lic. Maria Escobar

Universidad San Carlos de Guatemala

Lic. Daniel Villatoro

Universidad Da Vinci

Lic. Ana Escobar

Diseño:

INCIBE Guatemala

Los artículos que aparecen en esta edición no reflejan necesariamente el pensamiento de la **CsecMagazine**. Se publican bajo la responsabilidad de los autores.

Enero – Abril 2022

La presente publicación pertenece al Instituto Nacional de Ciberseguridad de Guatemala (INCIBEGT) y está bajo una licencia Reconocimiento-No comercial-Compartir Igual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

• **Reconocimiento**. El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE Guatemala y la Revista Digital Cybersecurity Información y Privacidad y sus sitios web: https://www.incibe.gt y https://www.csecmagazine.com. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE Guatemala presta apoyo a dicho tercero o apoya el uso que hace de su obra.

• **Uso No Comercial**. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

• **Compartir Igual**. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Algunas de estas condiciones pueden no aplicarse si se obtiene el permiso de INCIBE Guatemala como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES

Nota del editor

La afectación de vulnerabilidades sobresale de acuerdo con la cantidad de sistemas tecnológicos que estemos utilizando, con esto nuestra preocupación aumenta por mitigarlos a la brevedad posible y evitar que estos afecten a nuestra empresa u organización, razón por la cual se recomienda el uso de software licenciado para contar con estas protecciones y evitar ser victimas de un ataque de día cero o el robo y secuestro de la información privada o sensible. La desventaja que se tiene al utilizar el ciber espacio como herramienta de trabajo es que, los ciber delincuentes cuentan con herramientas especializadas para cometer ciber delitos, en la actualidad y a futuro estos serán más selectivos y certeros en sus ataques por tal razón es importante aumentar el grado de madurez en los aspectos de seguridad de la información y ciberseguridad para estar preparados para una respuesta o recuperación tras un ataque masivo a nuestras plataformas.

Con estos temas también sobresalen otros aspectos como los procesos, tecnologías, los datos y las personas que están implícitos dentro de la ciberseguridad y nacen otros conceptos prioritarios para nosotros como la inclusión en la ciberseguridad donde nos debemos de basar en marcos eficaces que promuevan este proceso inclusivo, algunos otros como las capacidades en el liderazgo para contrarrestar administrativamente brechas de seguridad, la sostenibilidad y responsabilidad que se tiene desde la alta gerencia, los responsables de la seguridad dentro de la organización hasta los usuarios finales.

Para concluir, seguimos trabajando de la mano de la sociedad civil, organizaciones internacionales en pro de una cultura de ciberseguridad que empieza a ser vital, por esto presentamos nuevamente nuestros artículos y resumen de conferencias realizadas durante el ultimo cuatrimestre del 2021, esperando una participación de ustedes con artículos o compartiendo información en nuestros canales digitales.

Daniela

CyberSecurity
Información & Privacidad

Resumen de conferencias

INCIBE Guatemala

Resumen de Conferencias INCIBE Guatemala

Independientemente segurxs

Por motivo de la celebración de los 200 años de independencia de Guatemala se llevó a cabo la Conferencia "**Independientemente Segurxs**" el 17 de septiembre del año 2021, este contó con la participación de 3 invitados especiales quienes realizaron exposiciones magistrales para exponer temas relevantes sobre el estado de la ciberseguridad en Guatemala. La conferencia inicio con la participación del Lic. Byron Cartagena quien abordó el tema de "La Firma electrónica avanzada" es Director Ejecutivo del Ministerio de Economía (MINECO) en Guatemala, durante la charla el Lic. Cartagena explicó que Guatemala adoptó la firma electrónica avanzada y por tal razón se crea el Decreto Ley 47-2008 que regula las comunicaciones y las firmas electrónicas y así crear el marco jurídico en Guatemala, además se crea el Registro de Prestadores de Servicios de Certificación quien es una dependencia del MINECO en Guatemala quien regular, registra, supervisa a los prestadores de servicios de certificación en el país. Aborda la creación de la Identidad Digital por la Comisión de las Naciones Unidas desde el año 1996 y específicamente en el año 2001 como elemento necesario para las comunicaciones y comercio electrónico. Explica los tipos de firmas electrónicas (siempre y avanzada) y los Prestadores de Servicios de Certificación que actualmente están habilitados en Guatemala para la generación de las firmas electrónicas quienes son: La Cámara de Comercio, Transacciones y Transferencias (5B) y Prisma. Dentro de la misma da 2 aspectos importantes para la generación de las firmas electrónicas y es que deben de generarse en un dispositivo seguro y un tercero de confianza para la acreditación de la firma electrónica avanzada. Por último recalca la confidencialidad, integridad y no repudio que debe de brinda la firma electrónica avanzada. La segunda conferencia se brindó por parte del Ingeniero Angel Salazar de la reconocida empresa de ciberseguridad a nivel latinoamericano Soluciones Seguras con el tema "Ciber pandemia ¿Cómo proteger los negocios en épocas encientas?". El Ing. Salazar inicia la charla con un resumen de los casos registrados a nivel mundial de Covid-19 y su relación con los ciber ataques que se generaron en el año 2003. Resalta la cantidad de riesgos del ciber crimen en Guatemala comparado a nivel mundial de Cryptominer, ransomware, mobile, infostealer, banking y botnet. Además en la conferencia hace hincapié en la creación de dominios falsos por parte de los ciberdelincuentes para engañar a las personas y con ello poder robar información sensible o personal. El Ing. Salazar aborda técnicamente los riegos como criptojacking, mobile, infostealer, banking, botnet y ransomware y con ello tener más conocimiento y las técnicas que utilizan los ciberdelincuentes para explotar vulnerabilidades en equipos y también a personas. Para finalizar la presentación hace conciencia en la gestión de riesgos para

minimizar el impacto de ataques tanto a nivel empresarial como personal, hace referencia al tema tratado previamente por el Lic. Cartagena del Ministerio de Economía de Guatemala. Para finalizar la actividad la Lic. Elizabeth Martinez de ESET Guatemala brinda su charla "La brecha de ciberseguridad en Guatemala frente al contexto global de ciber amenazas" donde indica el valor de la ciberseguridad y como esta se convierte en algo crítico para nuestra seguridad y prosperidad, así mismo los riesgos que la ciberseguridad puede generar en temas de democracia, valores, derechos humanos entre otros. Martinez hizo hincapié en la capacidad de mitigar y responder ante riesgos informáticos que se dan en el ciber espacio. Por último también recalco sobre aspectos de privacidad y el estado actual de Guatemala en el Reporte de Ciberseguridad 2020 de riesgos, avances y el camino a seguir en América Latina y el Caribe.

+Fuertes y Seguras

El congreso **+Fuertes y Seguras** se llevó a cabo el 29 de octubre del año 2021 con la participación de Nancy Perez de Guatemala, Vanesa Garcia Carbone de Argentina, Soledad Fuster de Argentina y Soledad Magnone de Ecuador. El objetivo de la actividad era presentar a las niñas y mujeres conferencias con expertas en las áreas de Violencia en las redes y el uso inadecuado de internet y minimizar el Ciberbulling, Violencia de Género, Grooming, Sexting y Ciberacoso entre otros durante su navegación en internet y fuera de él. En Guatemala este fenómeno va en aumento y las autoridades aún no realizan los esfuerzos necesarios para minimizar estos riesgos latentes que afectan a nuestras niñas y mujeres en el ciber espacio con programas que lleguen a toda la población. Con todo esto el proyecto de **Women In Security** busca que las participantes puedan conocer los riegos tecnológicos que afectan a niñas y mujeres en el ciber espacio, proponer ideas para minimizar su impacto, realizar las recomendaciones para evitar ser víctima y dar a conocer la ruta de Denuncia que desde **INCIBE Guatemala** está proponiendo en su página web, la cual pueden utilizar para denunciar y con ello apoyarles en todo aspecto. Nancy Perez - directora y fundadora de la Asociación Jóvenes por el Cambio en Guatemala expuso sobre el tema **"La prevención de la violencia de Genero"** en este contexto explico como la mujer guatemalteca se ve afectada por violencia en los ambientes públicos como privados donde se involucra uno o varios agresores y una o varias víctimas dentro de estos fenómenos. prosiguió explicando teóricamente los machismos y micromachismos ya que son pequeños gestos sexistas o machistas, algunos de ellos muy sutiles, que ayudan a perpetuar roles de género, machismo y violencia suavizada contra las mujeres. Algunos otros temas relacionados con este tipo de violencia se encuentra la emigración, inmigración hacia la mujer indígena, comunidad LGTB+ y No binarios. Seguidamente Vanesa Garcia Carbone, Perfiladora Criminal.

Directora y creadora de la División de Criminología, Criminalística y Análisis de la Conducta Criminal de la Sociedad Argentina de Trastornos de la Personalidad y Psicopatías, Investigadora Forense del OCEDIC con su charla **El Perfil Criminal del PEDERASTA DIGITAL El nuevo Delincuente Sexual del Siglo XXI.** La charla inicio abordando los riesgos tecnológicos para niñas y adolescentes, dentro de estos el delito de grooming ya que ahora es considerado el nuevo método de captación de abuso sexual hacia niñas, niños y adolescentes de los pederastas digitales o groomers pasando de lo físico a lo digital, dentro de su charla se explicó la fenomenología de este fenómeno ya que cuenta con una Fase Digital y Física, además de ello indicó lo complejo de este delito sexual, prosiguió indicando los efectos de este fenómeno como las amenazas, sextorsión, trata de personas, M.A.S.I. (Material de Abuso Sexual contra las Infancias), Abuso sexual, lesiones, femicidio y/o homicidios. Detallando el MASI formula que es "toda representación de un NNA de menos de 18 años dedicado a actividades sexuales explicitas o toda representación de sus partes genitales con fines predominantemente sexuales" Hace la aclaración que la pornografía infantil es utilizado por los pederasta y pedófilos y tratar estos riesgos de esta forma es incorrecta, ya que, es esta se toma como evidencia digital del abuso sexual a que fue sometida una víctima. Relata las modalidades del grooming de acuerdo con la clasificación del tipo de agresión sexual de acuerdo al numero de autores desde individuales, manada digital (2 o más), asimismo detalla la clasificación del tipo de agresión sexual de acuerdo al numero de víctimas, escenario e intervalo, dentro de estas individual (dos o mas victimas en diferentes lugares y momentos) manada digital (varios agresores digitales abusando de una sola victima), y el pederasta digital múltiple (dos o más victimas en un mismo tiempo y lugar, un solo escenario), menciona la diferencia entre el abuso sexual entre la pedofilia y la pederastia. Comenta también la categorización de la pirámide situacional de grooming, desde el pederasta digital como base, Groomer pederasta, el Groomer cazador, el Groomer sugar daddy / Groomer sugar mommas, productores de M.A.S.I, hasta llegar al Groomer depredador. Por último expone la teoría de la oportunidad con 3 aspectos que aumentan el riesgo de grooming, desde un autor motivado, una victima expuesta y la falta de vigilancia recomiendo también la metodología de la ruta de protección de NNA con los anillos de contención y seguridad, primer anillo de contención: núcleo familia (padre, madre, tutor) y el segundo anillo: profesores, maestros, psicólogos y pediatras. Seguidamente Soledad Fuster, Licenciada y profesora en psicología, Diplomado en Informe Pericial de Imputados y Niños víctimas de abuso sexual con el tema **El grooming como abuso sexual contra niños, niñas y adolescentes**. La licenciada Fuster inicia su charla indicando que aunque en Guatemala aun no es tipificado el grooming como un crimen en otros 80 países aproximadamente ya son castigados por la ley, habla de la relación entre la realidad y

virtualidad y su relación con los groomers. Además recalca sobre la configuración del Grooming y que han sido organizadas en 4 componentes (Victimas, Medio tecnológico, contenido sexual y el Groomer). Realiza una explicación de lo que es el grooming catalogándolo como: "El abuso sexual contra un niño, niña o adolescente ocurre cuando un niño es utilizado para la estimulación sexual de su agresor o la gratificación de un observador". De igual forma explica el proyecto de Ley en Guatemala que propone añadir el articulo 190bis al decreto 17-73 del Código Penal de Guatemala el cual tipificara el delito de seducción por medios digitales a niños, niñas y adolescentes con penas de 6 a 8 años a quienes utilizando cualquier ardid, engaño, argucia, presión o amenaza, contactara a un menos, con la finalidad que le envíe o de terceras personas o tener relaciones sexuales con el hostigador, instigador o seductor, independientemente que logre su propósito. Para finalizar su charla detalla las consecuencias del grooming, entre estas: Físicas (sueño, alimentación, esfínteres), Conductuales (autolesiones, consumo, bajo rendimiento escolar), Emocionales (culpa, vergüenza, depresión, miedo a ser reconocido), Sociales (retraimiento, desconfianza, dificulta en vínculos), Sexuales (rechazo propio cuerpo y/o contacto físico, sobreexposición) y recomienda que antes cosas de grooming se pueda: resguardar la evidencia digital, preservar la configuración del delito, reducir los riesgos, denuncias y contener a la víctima, hasta llegar a la generación de competencias digitales para la prevención del grooming. proyectos para información de las familias, formación profesional y uso de ESI como perspectiva digital. Por último para finalizar la actividad, Soledad Magnone socióloga uruguaya enfocada en las intersecciones entre educación, tecnologías digitales y derechos humanos, directora de Jaaklac con el tema "**Violencia digital y educación sexual integral (ESI) digital para adolescentes**" aborda el contexto social en américa latina particularmente desde el año 2015 donde organizaciones feministas y movimientos independientes realizan diferentes acciones en pro de la justicia social y equidad de género, además la igual de oportunidades para mujeres, legislaciones y condiciones para trabajadores sexuales, la interrupción voluntaria del embarazo y comunidad LGBTQ+ entre otras. También de la brecha digital de género, ya que las mismas son causa y consecuencia de las brecas sociales y en América latina es la región más desigual del mundo, indica también que de acuerdo a Web Foundation los hombres tienen el 21% mas de probabilidades de usar el internet que las mujeres, con esto las brechas digitales deben e cubrir costos, niveles de educación digital bajos y mayores probabilidades de ser víctimas de violencia digital. Por otra parte también expone que la Violencia de genero se está convirtiendo en un problema global con las graves implicaciones para la sociedad y economías, ya que se observan estadísticas que suponen un riesgo para la paz y prosperidad para todas las personas por no cumplirse con los objetivos de desarrollo inclusivo y sostenible que sitúe la igual de género y el empoderamiento clave

de las mujeres para lograrlo. Recomienda el uso de la educación digital para el desarrollo y exploración de adolescentes pero también que la educación digital no acompaña suficientemente estrategias que para adolescentes aprendan sobre los diferentes riesgos tecnológicos y como prevenirlos y minimizar sus daños, según la UNESCO solamente 5 países en América latina disponen de marcos educativos enfocados al mercado laboral, excluyendo habilidades para una ciudadanía digitalmente activa. Aporta de igual forma el proceso de creación del proyecto ESI Digital con talleres mixtos (virtuales/presenciales) favoreciendo el intercambio y desarrollar competencias digitales entre personas adultas y adolescentes. Con esto la creación de guías dinámicas a partir de las conversaciones entre adolescentes y adultes, consignas de trabajo planteadas en taller, información recogida con base a la revisión de literatura e investigaciones. Por último detalla los sitios para descargar el proyecto y pueda ser utilizado por investigadores en América latina para aumentar su grado de madurez en estos aspectos.

Búsqueda activa de NNA y mujeres a través de las tecnologías abiertas

Nuestro último proyecto en colaboración con Women In Security fue la búsqueda activa de mujeres, niñas, niños y adolescentes con alertas activas Alba-Keneth e Isabel-Claudina en Guatemala, este contó con la participación de profesionales en ciber seguridad en un bootcamp con la guía de 2 profesionales: **Aimery Parekh** de Brigada Osint España, OSINT Analist and investigator, Digital Forensic Investigator, Ninja Information, Citizen Detective, Researcher and Cyberpunk y **Jose Martin Vila** Co-Fundador de la Comunidad Argentina de Ingeniería Social, Coordinador del CTF de niñ@s desaparecid@s en Colaboración con Missing Children Argentina y No Encontrados ONG que se desarrolla en Ekoparty, Co-organizador del Social Engineering Space de Ekoparty y OSINT Analyst y R Data Scientist, dicha dinámica reunió a empresas e investigadores en la búsqueda de personas con alertas activas de desaparición en Guatemala, durante la actividad se contó con la exposición de un robot capaz de realizar trazabilidad sobre redes sociales siguiendo “hashtags” para la recolección de información, en la parte practica se dividieron en 2 grupos para la búsqueda activa de niñ@s y mujeres, para finalizar la actividad se dieron a conocer los resultados obtenidos de cada uno de los equipos y su documentación para presentar a las autoridades guatemaltecas.

Artículos

CyberSecurity
Información & Privacidad

OWASP A03:2021-Injection como Referente para el Desarrollo Seguro de Aplicaciones Web

OWASP A03: 2021-Injection as a Reference for the Secure Development of Web Applications

Dulce Lucía Alvizures Osorio, Josué Itamar Morataya Arizandieta, Jhoan Sebastian Samayoa Mayen y Kevin Rolando Guerra Pérez
email: josueitmar@gmail.com

Recibido: 10/noviembre/2021. Revisado: 12/noviembre/2021. Aprobado: 15/diciembre/2021.
Disponible en internet el 1 de enero de 2022

Resumen: La implementación de prácticas de desarrollo seguro en servicios y aplicaciones web, debe realizarse de manera eficiente en cada una de las organizaciones que cuente con áreas de desarrollo de software o al ser contratista de este tipo de servicios. La importancia del desarrollo seguro de aplicativos web, se intensifica con el hecho de que los servicios web están disponibles a nivel mundial y los atacantes de este tipo de servicios se encuentran al acecho para aprovecharse de vulnerabilidades causadas por controles de seguridad deficientes. En el ciclo de desarrollo de software, es necesario considerar una metodología de desarrollo seguro desde la fase de planificación, y no posteriormente, ya que puede representar graves riesgos para la información procesada, lo cual se traduce en costos elevados para la organización. Existe variedad de metodologías y marcos de referencia para el desarrollo seguro, no obstante en presente estudio se enfoca en el desarrollo de aplicaciones web, por lo que se hará uso del marco de referencia propuesto por OWASP (Open Web Application Security Project), el cual propone un enfoque basado en diez de las vulnerabilidades más comunes que afectan a aplicaciones web, y son mejor conocidas como OWASP TOP 10, esta lista de vulnerabilidades es administrada por una comunidad de profesionales en seguridad y desarrollo web, por lo que es un marco de referencia sólido y actualizado constantemente. Pese a que las vulnerabilidades listadas en OWASP TOP 10 son relevantes, el análisis del presente documento se enfocará en el riesgo más frecuente y de mayor impacto en aplicaciones web: Inyección SQL. El estudio de la vulnerabilidad por inyección SQL, refleja la necesidad de aplicar un modelo de desarrollo seguro, por parte de los equipos de desarrollo de aplicaciones web y la importancia de la inversión en soluciones y personal apto para desempeñar actividades desde una perspectiva de seguridad integral en el ámbito informático.

Palabras Claves: Desarrollo Seguro, OWASP, Inyección SQL, SQL Injection, Desarrollo Web, Aplicaciones Web.

Abstract: The implementation of secure development practices in web services and applications must be carried out efficiently in each of the organizations that have software development areas or by being a contractor for this type of services. The importance of secure web application development is intensified by the fact that web services are available

worldwide and attackers of this type of service are on the prowl to take advantage of vulnerabilities caused by poor security controls. In the software development cycle, it is necessary to consider a secure development methodology from the planning phase, and not later, since it can represent serious risks for the processed information, which translates into high costs for the organization. There is a variety of methodologies and frameworks for secure development, however this study focuses on the development of web applications, so the framework proposed by OWASP (Open Web Application Security Project) will be used, which proposes an approach based on ten of the most common vulnerabilities that affect web applications, and they are better known as OWASP TOP 10, this list of vulnerabilities is managed by a community of professionals in web security and development, so it is a framework of solid reference and constantly updated. Although the vulnerabilities listed in OWASP TOP 10 are relevant, the analysis of this document will focus on the most frequent and most impactful risk in web applications: SQL injection. The study of SQL injection vulnerability reflects the need to apply a secure development model by web application development teams and the importance of investing in solutions and personnel capable of carrying out activities from a comprehensive security perspective in the computer field.

Introducción

El presente estudio permitirá al lector, la comprensión del modelo de desarrollo seguro en aplicaciones web, basado en el dominio A03:2021 del modelo OWASP TOP 10, el cual hace referencia a las vulnerabilidades de tipo SQL Injection.
Desde esta perspectiva, los objetivos de investigación se detallan a continuación:

- Expresar la importancia de adoptar un modelo de desarrollo seguro en servicios y aplicaciones web.
- Describir el dominio A03 de OWASP TOP 10 en su versión 2021.
- Analizar las posturas y opiniones de profesionales del ámbito informático guatemalteco, respecto al desarrollo web seguro y su relación con la vulnerabilidad de inyección SQL.

El análisis del presente documento, gira en torno al estudio de las vulnerabilidades de tipo SQL Injection y su relación con el modelo de desarrollo seguro basado en OWASP TOP 10, utilizando en esta ocasión, información obtenida de conocimientos y experiencias vividas por profesionales informáticos en el ámbito de desarrollo y seguridad de aplicaciones en diversas organizaciones (públicas y privadas) del país de Guatemala.
La selección y enfoque en el modelo de seguridad OWASP TOP 10, es debido a sus características seguras y bien definidas para aplicaciones web, que este modelo ofrece. Dicho

modelo es considerado como un estándar en seguridad de aplicaciones web, pues ha sido desarrollado y madurado por la comunidad OWASP desde el año 2001.
A nivel mundial, las aplicaciones web cumplen funciones esenciales para la sociedad en general. Guatemala es un país representativo en el ámbito tecnológico centroamericano y latinoamericano, por ello, se vuelve necesario comprender las principales vulnerabilidades a las cuales se encuentran expuestas las aplicaciones web, así como, las acciones a tomar en cuenta para minimizar el riesgo ante posibles amenazas.
Según múltiples estudios realizados a la fecha, se tiene la certeza de que la vulnerabilidad web más aprovechadas por los ciberdelincuentes, es la inyección SQL, el cual puede definirse como: un ataque a una aplicación web, que compromete su base de datos mediante instrucciones SQL maliciosas.

Basados en las vulnerabilidades por inyección SQL, el presente estudio, ofrecerá resultados fundamentados en entrevistas, encuestas y recopilación de información documental, el cual expondrá la criticidad a la cual están afectas las aplicaciones web, y principalmente cuales son las medidas de seguridad a tomar en cuenta para el desarrollo seguro y la mitigación de esta clase de vulnerabilidad y sus variantes.

Materiales y Métodos

La investigación se llevó a cabo en cuatro instituciones en la Ciudad de Guatemala tomando como base la experiencia, recursos y disponibilidades tecnológicas de estas organizaciones, cuyo enfoque es la implementación de soluciones de seguridad como parte de las buenas prácticas establecidas por el modelo OWASP TOP 10 A03, orientadas al desarrollo de sistemas de información.

Para esto fue necesario hacer uso de recursos como:

- Físicos: Equipo de Computo
- Personales: Profesionales Informáticos
- De recolección: Encuestas, entrevistas y documentos informativos

Definiendo que el tema central de esta investigación fue refinado para el establecimiento de un enfoque sólido, que permitiera alinear las incógnitas en los recursos de recolección de datos anteriormente mencionados, iniciando con la investigación profunda y almacenamiento de información , se efectuó la segmentación para obtener el personal objetivo que aportó sus conocimientos a la investigación, aplicando técnicas proyectivas e ingeniería social para la apertura en la confiabilidad y desenlace de los temas específicos, realizando de esta manera

las encuestas por correo electrónico y las entrevistas a través de reuniones virtuales de una manera semi formal respetando las restricciones y medidas de seguridad establecidas actualmente por la pandemia (COVID-19).

El tipo de investigación realizada es de carácter cualitativo y cuantitativo. Debido a la gran variedad de información que fue recolectada a través de la subjetividad del personal en cada una de las instituciones que adicionalmente permitieron la obtención de resultados significativos que apoyan al desarrollo seguro de aplicaciones web.

Resultados

Como parte del análisis realizado hacia el tema de inyección SQL, se logra obtener desde Google Trends, las tendencias de búsqueda de este tema, como se logra observar que se ha mantenido en los mismos márgenes, lo cual indica que la búsqueda sobre la mitigación de este riesgo potencial no ha aumentado su volumen, dando pauta a la falta de interés al momento sobre temas de seguridad al desarrollar sistemas web.

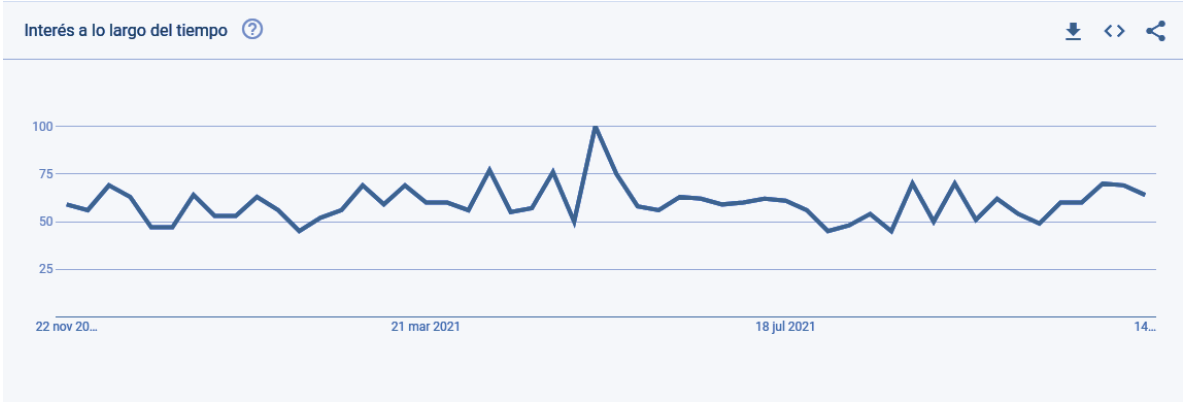


Ilustración 1: Tendencia de búsqueda
Fuente: https://trends.google.es/trends/explore?q=%2Fm%2F02lrkx

Ilustración 2: Tendencia de búsqueda por país.
Fuente: https://trends.google.es/trends/explore?q=%2Fm%2F02lrkx

Con base en estos resultados, se decide realizar una encuesta a personas que se encuentran en el campo del desarrollo y también en la parte de seguridad tomando en cuenta la tendencia antes observada, para lo cual se obtuvieron los resultados siguientes:

Como se observa un 46.9% de los encuestados realmente cree que las evaluaciones de seguridad son necesarias y se sugieren que se deben realizar de forma trimestral, para que no exista un tiempo amplio sin realizar las evaluaciones respectivas.

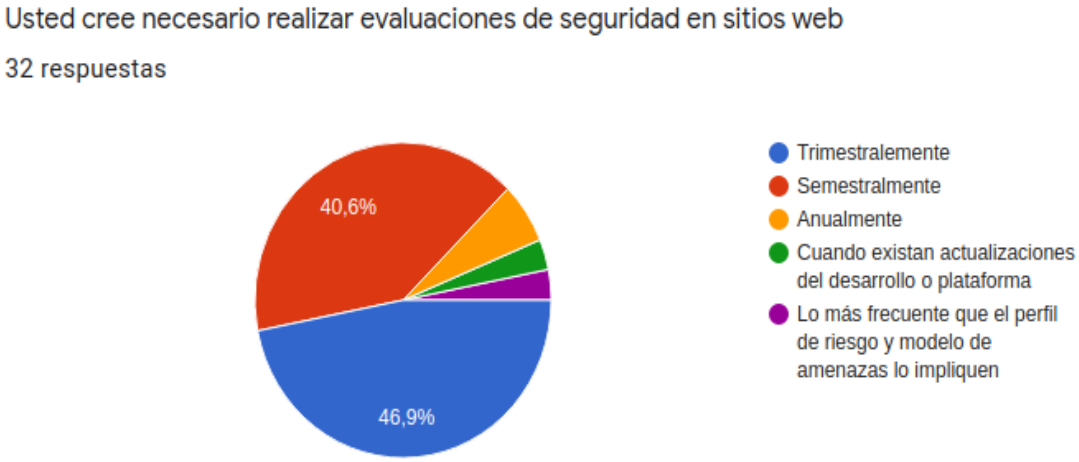


Ilustración 3: Representación gráfica de los resultados obtenidos a través de las encuestas realizadas.
Fuente: https://forms.gle/drmG5ZpumnycJsw68

En cuanto al entorno laboral, el 53.1% de los encuestados afirma que ha existido involucramiento de parte de sus empresas para lograr que sean entornos seguros y que los esfuerzos han permitido encontrar todo tipo de falencias en el campo de la seguridad.

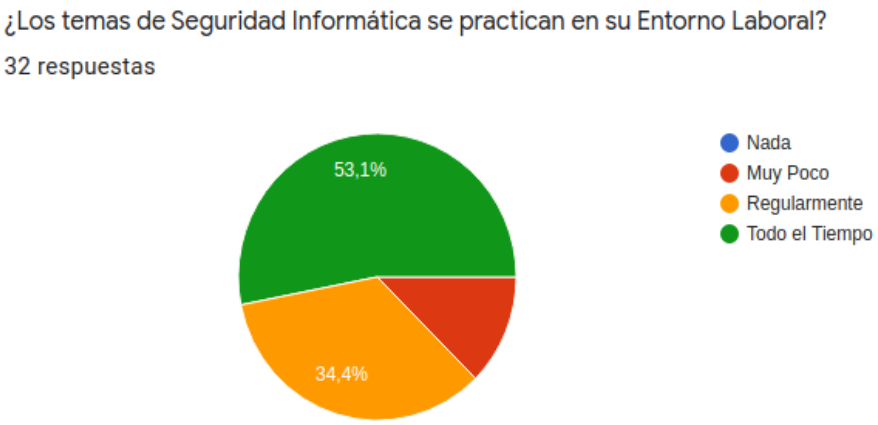


Ilustración 4: Representación gráfica de los resultados obtenidos a través de las encuestas realizadas. Fuente: https://forms.gle/drmG5ZpumnycJsw68

Respecto a la lógica y buenas prácticas de programación, el 46.9% indica que la falta de conocimientos al momento de manejar un desarrollo seguro respecto a SQL inyección radica en los mismos programadores, por lo que es importante la capacitación constante respecto al apartado de seguridad y el mismo desarrollo seguro.

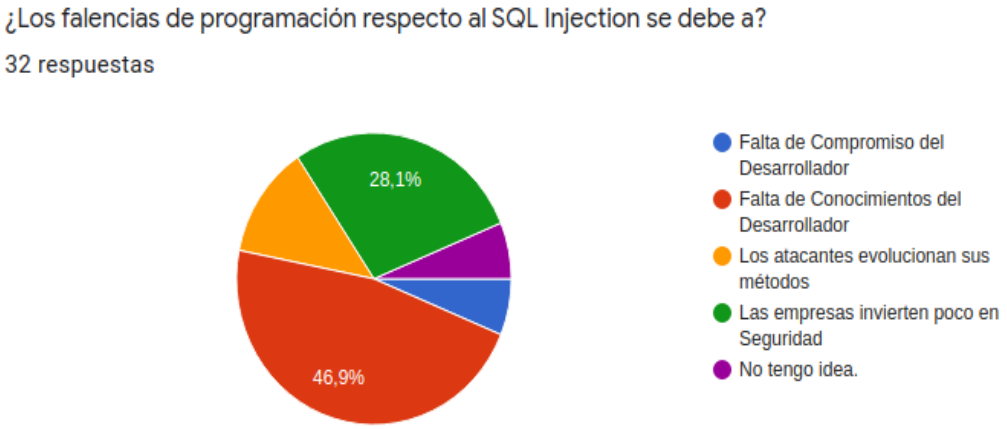


Ilustración 5: Representación gráfica de los resultados obtenidos a través de las encuestas realizadas. Fuente: https://forms.gle/drmG5ZpumnycJsw68

Tras conocer los resultados de la encuesta realizada a los diferentes grupos de personas, tanto del área de desarrollo como de seguridad, se determina que en ambos grupos se cuenta con conocimientos básicos sobre el tema de SQL inyección y los riesgos que este conlleva, pero que carece de interés, tanto la mitigación, como el mantenerse actualizados sobre dicho tema, esto último se encuentra enfocado a la parte del desarrollo, dado que, es el tema de seguridad lo último que se suele tomar en cuenta, por lo cual lo vuelve un proceso engorroso y demasiado laborioso.

Discusión

Según los resultados, se encontraron un número de variables asociadas a inyección SQL, las cuales desempeñan un rol importante y significativo, tanto en el desarrollo web como también en la seguridad informática que implica una página web. Así la falta de conocimiento y prácticas seguras para llevar a cabo un desarrollo seguro, sumando la poca inversión a la seguridad informática en las organizaciones hacen que la mayoría de los sitios web no cumplan con las medidas necesarias para tener un desarrollo seguro incrementando la vulnerabilidad de ataques por inyección SQL qué son generados con mayor frecuencia ya que los atacantes evolucionan sus métodos generando impacto en la continuidad del negocio.

A pesar de que un ataque de inyección SQL conlleva una serie de procedimientos no tan complejos para contrarrestarlo según su nivel de criticidad, es necesario contemplar desde un inicio mantener metodologías que apoyen el desarrollo y reduzcan o mitiguen este tipo de amenaza. Por lo tanto, es importante destinar parte de los recursos operacionales y económicos del área encargada para invertir en mejorar todo lo que involucra el desarrollo web y su entorno físico y lógico ya que como es bien conocido en la rama de sistemas informáticos, para tener un ambiente seguro, controlado, disponible correctamente y de manera confiable, se debe contar con todo el equipo necesario y capacitado eficientemente en los diferentes roles que se desempeñan para cumplir con el objetivo.

Conclusiones

Los modelos de desarrollo seguro deben ser implementados desde la concepción de un proyecto de desarrollo web, el omitir esta consideración puede causar el incremento futuro de costes para la organización, e incluso repercutir en afectaciones a la imagen y reputación de la organización, por causa de pérdidas o filtraciones de información sensible.

La capacitación y concientización de los desarrolladores es uno de los aspectos más importantes en la rama de seguridad informática, se debe poseer un enfoque objetivo y escalar, que permita la consolidación de una buena cultura institucional, así como la obtención de resultados, sin privarse de la aplicación de buenas prácticas en el desarrollo de sistemas.

Es indispensable considerar que llevar a cabo buenas prácticas desde el origen del desarrollo web, implica no solo generar software de gran valor, sino también incrementar el nivel de seguridad para toda la organización, reduciendo las vulnerabilidades o amenazas como la inyección SQL que se aprovecha de brechas no contempladas en el sitio.

El hecho de considerar las tendencias sobre cibercriminalidad es vital, especialmente el tema de seguridad en plataformas web, pues debe ser un tema por abordar en cada proyecto que involucre desarrollo, lo anterior como consecuencia del incremento en el uso de las plataformas web que se utilizan en actividades cotidianas.

Consideraciones Finales

Para mantener un entorno de seguridad proactivo en las aplicaciones web, se debe considerar la implementación de servicios de monitorización de aplicaciones, los cuales notifiquen, en tiempo real, ataques informáticos a plataformas críticas. Esto permitirá intervenir de manera oportuna ante incidentes informáticos y evitar daños mayores.

Se deben efectuar los estudios necesarios para el análisis de riesgos informáticos que puedan afectar a la organización a través del tiempo, así como el establecimiento de planes de contingencia tomando en cuenta los parámetros variables para la toma de decisiones.

Contemplar que, para tener un entorno adecuado, tanto para el desarrollo, como la seguridad de las aplicaciones web, se debe tener el equipo físico, lógico y operacional adecuado con niveles adecuados de habilidades, capacidades y conocimientos, lo que requiere de inversión económica según los resultados que se quieran obtener.

Debemos tomar en cuenta que la mejora continua para los procesos de seguridad y el desarrollo web, deben ir de la mano para lograr servicios con los que se logre ofrecer productos de calidad y que sean confiables para el uso de las personas que interactúan con ellos.

Referencias bibliográficas

Camacho, M. (2018). Facultad de Ingeniería, Universidad de la República Uruguay - Sistema de monitoreo de aplicaciones web e infraestructura. Obtenido en: https://www.colibri.udelar.edu.uy/jspui/bitstream/20.500.12008/19639/1/tg-sabatella.pdf

Ciberseguridad.com (2021). Guías de Ciberseguridad Web - Desarrollo Seguro. Obtenido en: https://ciberseguridad.com/guias/desarrollo-seguro/

Boo, J. (2014). Mejora continua en el desarrollo de software. Obtenido en: https://comunidad.iebschool.com/weboolog/2014/11/25/mejora-continua-en-el-desarrollo-de-software/

García, J. (2010). Seguridad Informática - Análisis y control de riesgos de seguridad informática: control adaptativo. Obtenido en: https://acis.org.co/archivos/Revista/105/JMGarcia.pdf

Marulanda, J. (2018). Aplicación de la metodología OWASP para mejoramiento de la seguridad en el sistema E-commerce siembraviva.com. Obtenido en: repository.unad.edu.co/bitstream/handle/10596/20479/1060648494.pdf

Mazza, H. (2020). Gestión Estratégica en TIC - Gestión Estratégica de Recursos Informáticos. Obtenido en: http://www.sustentum.com/sustentum/pubs/geri.pdf

Singh, S. (2019). Pentest-Tool Blog - Ataques comunes del tipo Inyección SQL. Obtenido en: https://pentest-tools.com/blog/sql-injection-attacks

OWASP Foundation (2021). Ataques Web - Inyección SQL. Obtenido en: https://owasp.org/www-community/attacks/SQL_Injection

OWASP Foundation (2021). OWASP Cheat Sheet Series - SQL Injection Prevention Cheat Sheet. Obtenido en: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html [7]

Sobre los autores:

Sebastian Samayoa, Ingeniero en Sistemas de la Universidad Mariano Gálvez, Master en Seguridad Informática, con experiencia en el departamento de tecnologías de la información en el ámbito de las telecomunicaciones de Guatemala.

Dulce Alvizures, Ingeniera en Sistemas de la Universidad Mariano Gálvez, Master en Seguridad Informática, con experiencia en el departamento de tecnologías de la información en el sector bancario de Guatemala.

Josué Morataya, Ingeniero en Sistemas de la Universidad Mariano Gálvez, Master en Seguridad Informática, con experiencia en el departamento de tecnologías de la información en el sector agroindustrial de Guatemala.

Kevin Guerra, Ingeniero en Sistemas de la Universidad Mariano Gálvez, Master en Seguridad Informática, con experiencia en el departamento de tecnologías de la información en el sector de electrificación de Guatemala.

CyberSecurity
Información & Privacidad

Aplicabilidad de dominios y controles de Ciberseguridad en ciudades inteligentes

Applicability of domains and controls of Cybersecurity in smart cities

Armando Monzón Escobar
Armandomon.zone@gmail.com

Recibido:15/agosto/2021. Revisado: 20/septiembre/2021. Aprobado: 15/octubre/2021.
Disponible en internet el 1 de enero de 2022

Resumen: La ciencia formal en ciberseguridad se ha expandido no solo a aspectos técnicos sino más bien estratégicos, y es que las empresas buscan basarse en metodologías para aplicarlas dentro de sus procesos internos, consecuentemente a esto ahora las políticas referentes a tecnologías de la información ya no son estáticas (seguridad de la información, seguridad informática y ciberseguridad), porque también estamos conscientes de su aplicabilidad en cada ámbito de las TICs, por esto es necesaria la protección de todas las zonas dentro de las plataformas digitales y las que se expanden hasta los servicios que están en la nube. Quizá la parte más compleja de la aplicabilidad de los dominios y/o controles de la ciberseguridad es que pueden variar entre metodologías o buenas prácticas porque dependerá del seleccionado o podrá ser válido tomar controles de varios marcos de referencia para generar nuestra propia metodología interna, claro está que el tamaño de la organización y/o el nivel de madurez que estas tengan para adoptarlas parcial o totalmente será factor importante para una aplicabilidad real de todo este procesos. Empresas multinacionales basan su protección empresarial en marcos disponibles como la familia de la ISO/IEC 27001:2013, COBIT, las directrices de COSO o NIST SP 800-53, CIS, CARTA, la Cadena de la Progresión de la Amenaza, la Evaluación Continua del Riesgo Tecnológico por solo nombrar algunos, hasta su evaluación con el Modelo de Madurez de Capacidades de Ciberseguridad y el Ciclo de Deming como complemento, pero cada uno de estos con un objetivo específico, ya que sabemos que al hablar de marcos sobre ciberseguridad se expanden a cada una de las áreas tecnológicas dentro de la organización. Con lo indicado anteriormente el conjunto de acciones que la organización tomará como base para la aplicabilidad de dominios y controles deberán ser priorizados y analizados para determinar su efectividad y con ello mejorar el nivel de ciberseguridad basado en la misión y visión de la organización a corto, mediano y largo plazo.

Palabras Claves: ciberseguridad, marcos, controles, madurez, amenazas.

Abstract: The formal science in cybersecurity has expanded not only to technical aspects but rather to strategic ones, and it is that companies seek to base themselves on methodologies to apply them within their internal processes, consequently to this now the policies restraints to information technologies no longer are static (information security, computer security and cybersecurity), because we are also aware of their applicability in each area of ICTs, for this

reason it is necessary to protect all areas within digital platforms and those that extend to the services that are in the cloud. Perhaps the most complex part of the applicability of cybersecurity domains and / or controls is that they may vary between methodologies or good practices because it will depend on the selected one or it may be valid to take controls from various frames of reference to generate our own internal methodology. It is clear that the size of the organization and / or the level of maturity that they have to adopt them partially or totally will be an important factor for a real applicability of this entire process.

Many of the multinational companies base their business protection on available frameworks such as the ISO / IEC 27001: 2013 family, COBIT, COSO guidelines or NIST SP 800-53, CIS, CARTA, Chain of Threat Progression, the Continuous Evaluation of Technological Risk to name a few, until its evaluation with the Cybersecurity Capabilities Maturity Model and the Deming Cycle as a complement, but each of these with a specific objective, since we know that when talking about frameworks on cybersecurity expand to each of the technological areas within the organization.

With the aforementioned, the set of actions that the organization will take as a basis for the applicability of domains and controls should be prioritized and analyzed to determine their effectiveness and thereby improve the level of cybersecurity based on the mission and vision of the organization in the short term, medium and long term.

Introducción

Las estrategias corporativas se deben de basar en marcos que ayuden a conocer el estado actual, análisis de brecha, la hoja de ruta y aplicabilidad de las políticas, procedimientos y procesos internos. Para iniciar con alguna metodología podemos tomar cualquier de los marcos disponibles – y es que esto para muchas empresas con grados de madurez alto, fueron aplicados años atrás, para otras no lleva más de algunos meses, para otras están en proceso de análisis y algunas más que están aún planeando realizar estas actividad- por ello estar cociente de estos aspectos dentro de la empresa es relevante.

Si deseamos la aplicabilidad de controles lo deseado seria conocer el estado actual de la organización en materia de ciberseguridad, es por ello por lo que podemos basarnos en controles básicos, controles fundacionales hasta llegar a los controles organizaciones que aportaran bases sólidas a la organización para aumentar su capacidad de control de riesgos tanto interno como externos.

Los controles básicos van desde conocer el inventario de los dispositivos, software, hardware autorizados y no autorizados, el control de privilegios administrativos, la configuración

seguridad de todos los dispositivos de hardware (dispositivos móviles, computadoras, portátiles, estaciones de trabajo hasta servidores) y software, hasta llegar a un mantenimiento, monitoreo y análisis de bitácoras para temas de auditoría interna, se resalta que estos controles básicos son importantes para determinar el estado actual en la organización.

Los controles fundacionales están en un nivel medio ya que se toman aspectos como, la protección del correo electrónico y navegación web, la defensa contra programas de código malicioso con antivirus o XDR, la limitación y control de puertos de red, protocolos y servicios con ayuda de plataformas NAC, la capacidad de recuperación de datos, la configuración segura de los equipos de red, tales como firewall, enrutadores, etc., el aumento en la defensa de las zonas disponibles dentro de la organización, la protección de datos, el control de acceso físico y lógico, los controles de acceso inalámbrico hasta llegar al monitoreo y control de cuentas, observamos que el nivel de exigencia para estos controles son mayores y acá es donde reside el tema de determinar el nivel de madurez de las organización para cumplir con cada uno de ellos.

Los controles organizacionales van orientados a implementar un programa de concienciación y capacitación en seguridad de datos, ciberseguridad entre otras, la seguridad del software de aplicación, la respuesta y gestión de incidentes, las bases para una continuidad del negocio hasta llegar a pruebas de penetración controladas.

Imagen 1Estructura de Controles CIS. Fuente: CIS Controls. 2021

Se recalca que solo se estiman algunos de los controles que se pueden utilizar, pero esto dependerá de la organización para adoptarlos e implementarlos, en muchos casos solamente es necesario la actualización de sus políticas, procedimientos y/o procesos para la mejora continua de estos.

Con lo anterior se puede planificar una presentación ante la alta gerencia sobre el estudio o proyectos que enmarcaran los pasos a detalle para lograr una gestión en ciberseguridad real, tomando de base que este proceso debe de ser de acuerdo con los procesos internos de la organización para realizar el análisis de brecha, la hora de ruta y aplicabilidad de los procedimientos.

Desarrollo

Para el Oficial de Seguridad de la Información planificar la estrategia para la gestión de los riesgos vinculados que los activos de información dentro de la organización es todo un desafío, ya que representa una planificación real de todas las acciones de protección en serán utilizadas en un futuro y que, a su vez, se tengan actualizadas y verificadas para poder monitorizarse a lo largo de ciclo de vida. Sin embargo, por la disponibilidad de varios marcos, el CISO deberá aprovechar lo mejor de cada uno de estos o en el mejor de los casos solo seleccionar uno específico para cumplir con lo que este requiere y poder establecer una línea de trabajo (hoja de ruta) consistente y práctica para abordar los riesgos de ciberseguridad dentro de la organización.

Los grupos de implementación de los controles de CIS (Center for Internet Security) (Center for Internet Security, 2021) son un conjunto prescriptivo y prioritario de mejores prácticas en seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance, y apoyar el cumplimiento en ya que en la actualidad existen múltiples marcos, adicional a los controles básicos, fundamentales y organizaciones también se priorizan los Grupos de implementación (IG) ya que se toman aspectos sobre el perfil de riesgo y de los recursos que se dispongan.

El grupo de controles de Implementación 1 (IG1) están basados en que las organizaciones con recursos limitados, en las que la sensibilidad de los datos es baja, tendrán que aplicar los Sub-Controles que típicamente entran en la categoría IG1. El grupo de implementación 2 (IG2) define que las organizaciones cuentan con recursos moderados y un mayor riesgo de exposición por manejar activos y datos más sensibles e importantes tendrán que implementar los controles de IG2 junto con los de IG1. Estos Sub-Controles se enfocan en ayudar a los equipos de seguridad a gestionar información sensible de clientes o empresas.

El grupo de implementación 3 (IG3) establece a las organizaciones maduras con recursos importantes y una alta exposición al riesgo para el manejo de activos y datos críticos necesitan implementar los Sub-Controles de la categoría IG3 junto con los de IG1 e IG2. Los Sub-Controles que ayudan a reducir el impacto de los ataques dirigidos de adversarios sofisticados normalmente entran en la categoría IG3.

Estableciendo un detalle de cada uno de estos controles CIS los básicos se definen en: Control 1: Inventario y control de activos de hardware, Control 2: Inventario y control de activos de software, Control 3: Gestión continua de vulnerabilidades, Control 4: Uso controlado de los privilegios administrativos, Control 5: Configuración segura para el hardware y el software

de los dispositivos móviles, laptops, estaciones de trabajo y servidores y por ultimo Control 6: Mantenimiento, monitoreo, y análisis de logs de auditoría.

Ahora los controles Fundamentales se definen en: Control 7: Protección de correo electrónico y navegador web, Control 8: Defensas contra malware, Control 9: Limitación y control de puertos de red, protocolos y servicios, Control 10: Funciones de recuperación de datos, Control 11: Configuración segura para dispositivos de red, tales como firewalls, routers y switches, Control 12: Protección perimetral, Control 13: Protección de datos, Control 14: Control de acceso basado en la necesidad de saber, Control 15: Control de acceso inalámbrico y por último el Control 16: Monitoreo y control de cuentas. Como observamos el nivel de control va aumentando en estos controles fundamentales, es por ello que los niveles de madurez de las organizaciones van aumentando en complejidad, pero también en inversión de la alta gerencia para cada uno de controles.

Los controles Organizaciones a pesar de ser menos representan un aumento en el nivel de madurez tanto de la empresa en aspectos de gestión de ciberseguridad como del propio CISO (Escoteiros, 2021)para administrar todos los recursos tecnológicos dentro de la organización, dentro de estos tenemos el Control 17: Implementar un programa de concienciación y capacitación en seguridad integrado para identificar, desarrollar y capacitar a los colaborares dentro de la organización para aumentar su habilidades sobre riesgos tecnológicos, Control 18: Seguridad del software de aplicación, si bien la ciberseguridad es una capa adicional en temas de desarrollo, es importante también tomar en cuenta metodologías OWASP para minimizar el impacto de riesgos de explotación de vulnerabilidades, el Control 19: Respuesta y gestión de incidentes, con esto desarrollar e implementar un sistema de gestión de incidentes. Por último, el Control 20: Pruebas de penetración y ejercicios de equipo rojo (red team) para realizar pruebas controladas periódicamente para poder identificar vulnerabilidades o brechas dentro de la organización.

APLICAR CIS a un entorno de Ciudades Inteligentes

La ciberseguridad como se indicaba anteriormente es un aspecto que ha representado un desafío para las organizaciones y su interacción con los ecosistemas de las futuras ciudades inteligentes donde la infraestructura juega un papel importante en la interconectividad entre distintas plataformas tecnológicas que brindaran servicios a sus habitantes. No obstante, la misma disponibilidad de estas plataformas como conexión inalámbrica, servicios de monitoreo con cámaras ip, dispositivos IOT para monitorizar carga vehicular, cantidad de contaminación, saturación de oxígeno, humedad entre otros, hacen que la superficie de ataque

sea cada vez más grande logrando en un determinado momento afectar todo el entorno tecnológico por no asegurar correctamente toda esta infraestructura.

Los ciber adversarios o ciber delincuentes buscaran causar daños a las infraestructuras para obtener un rescate de toda o parte de la infraestructura, es por ello que estos servicios se vuelven un objetivo para este tipo de ciber ataques y la adopción de marcos como CIS para minimizar el impacto que este represente.

Ya (Libelium, 2020) ha expuesto más de 50 sensores que podrían estar disponibles en una ciudad inteligente y aunque no se detallan los riesgos inherentes dentro de esto se puede observar que la superficie de ataque es lo bastante grande para tener distintos tipos de ataques.

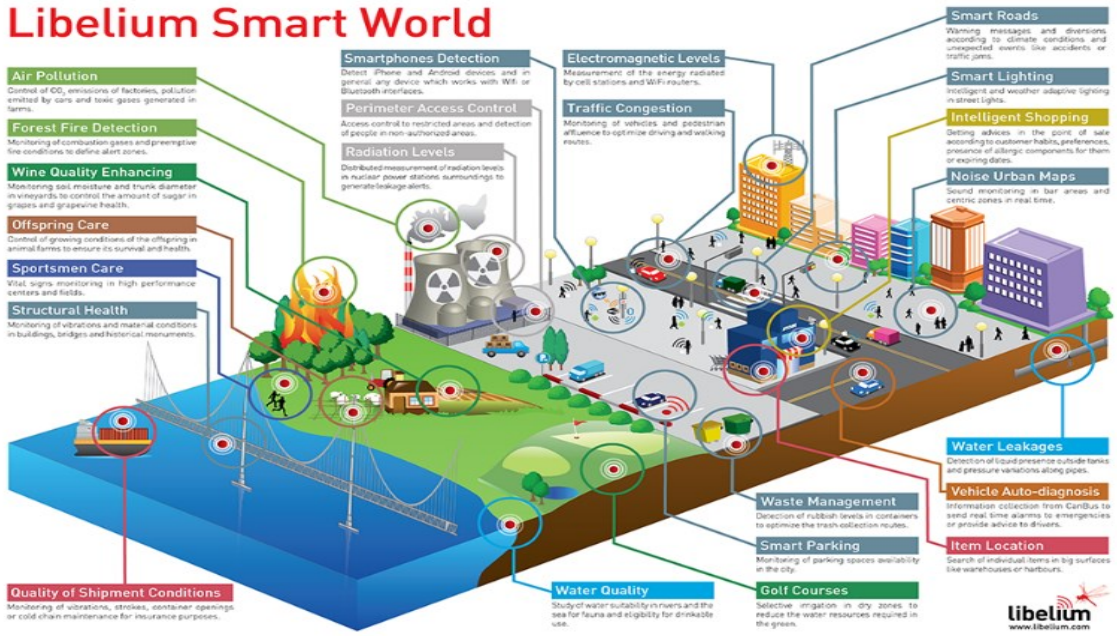


Imagen 2 Sensores para un mundo inteligente. Fuente: Libelium. 2020

La cantidad de vulnerabilidades de los sistemas (ZDNet, 2021), se ven desde 2 puntos de vista, la primera por desconocimiento de los técnicos sobre el aseguramiento de los equipos y la otra las propias de los sistemas (hardware/software), en este contexto las plataformas se enfrentan a vulnerabilidades humanas que se pueden materializarse en aspectos de ciber ataques por no tener un control sobre cada uno de estos dispositivos.

Ahora bien, la ciber inteligencia debe de verse desde varios puntos de vista para minimizar ataques como la estrategia, la técnica, la operacional y por último la táctica estos en el ámbito técnico, pero se olvida lo que se exponía anteriormente, y era básicamente la ciber

inteligencia emocional que afecta a los responsables de asegurar las plataformas tecnológicas ya que se enfrentan a otros factores como estrés laboral, desgaste emocional, problemas personas, etc., y esto puede impactar en el aseguramiento de toda esta plataforma tecnológica de ciudades inteligentes.

Ya en un estudio realizado por ISACA Guatemala y el Instituto Nacional de Ciberseguridad de Guatemala (Incibe Guatemala, 2021) se demostraba que el aumento de carga laboral hace que los colaboradores muestren un estado de agotamiento mental, emocional y físico haciendo que se sientan molestos o enojados con sus compañeros de trabajo, con sus propias actividades laborales que se extienden hasta los clientes a cauda de la Covid-19 (CEPAL, 2021), es por este tipo de aspectos que la ciber inteligencia emocional también debe de jugar un papel importante en cómo realizar la conectividad segura de plataformas en las nuevas ciudades inteligentes. Todo este proceso no es solamente técnico sino más bien un conjunto de estrategias que aportaran madurez a la infraestructura.

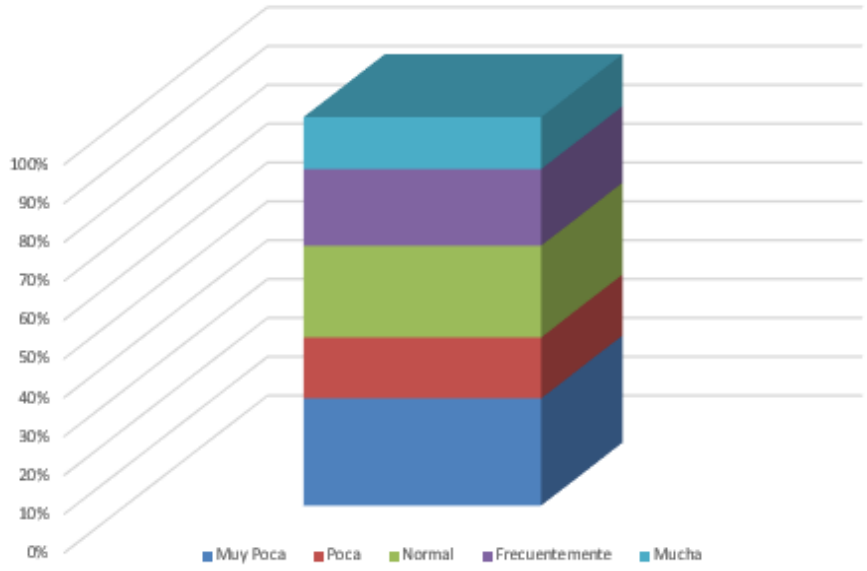


Imagen 3 Estado de molestia. Fuente: INCIBE Guatemala. 2021

Las tecnologías de la información pretenden que los sistemas sean estables y confiables pero una salud mental en los responsables de la seguridad de la información hará que todos estos estén configurados de la mejor forma y adaptados a las necesidades de las nuevas ciudades inteligentes.

Cada uno de los controles CIS deben de ir enfocados a analizar todo el entorno de una ciudad inteligente y lograr una transformación digital que aporte el empleo de las tecnologías de

información y comunicaciones, la automatización y control en edificios, una planificación urbana eficiente, la posibilidad urbana en el transporte público sostenible, la gestión inteligente de residuos sólidos, open data entre otros. Es por ello que al conocer el entorno tecnológico, sus plataformas, sus versiones y posibles vulnerabilidades por estar expuestas a una gran cantidad de personas se tendrá mayor conocimiento de la exposición que se realiza y su nivel de riesgo.

Conclusión

La estructura tecnológica debe verse como una estrategia de principio a fin, donde todos los actores deben de proponer soluciones para tener la misma estable y cumplir con la disponibilidad, integridad y confidencialidad de la información que se procesa dentro de estas plataformas. Con esto, la adopción de procesos desde la identificación, la protección, la detección, la respuesta y por último la recuperación de todos los sistemas. Es lógico imaginar que solo se necesita el presupuesto para invertir en las ciudades inteligentes, pero esto debe de ir más allá, y es generar una planificación previa de todo el entorno tecnológico que se implementará y su crecimiento en "n" cantidad de años, ya que una vez implementada la infraestructura un crecimiento desmedido hará que se obvien procesos de seguridad y esto podría afectar a toda la plataforma inteligente de las nuevas ciudades.

Por el momento es importante conocer acerca de la situación actual de proyectos implementados y tener una postura de como minimizar un impacto catastrófico en toda la plataforma tecnológica para la protección de los activos digitales desde el hardware al software y conocer el nivel de responsabilidad si utilizamos plataformas SAAS, IAAS, PAAS, entre otras. (RedHat, Consultado 2020).

Referencias bibliográficas

Celebrating Abraham Wald's Birth Centenary. (19 de Agosto de 2006). Obtenido de Taylor Francis Online:https://www.tandfonline.com/doi/abs/10.1081/SQA-120030191?scroll=top&needAccess=true&journalCode=lsqa20

Center for Internet Security. (Enero de 2021). Obtenido de https://www.cisecurity.org/controls/

CEPAL. (14 de Octubre de 2021). Obtenido de https://biblioguias.cepal.org/c.php?g=159524&p=7672119

Escoteiros. (22 de Junio de 2021). Obtenido de https://www.escoteiros.org/que-es-ciso-funciones/

Incibe Guatemala. (Julio de 2021). Obtenido de https://incibe.gt/investigaciones/

Libelium. (9 de septiembre de 2020). Obtenido de https://www.libelium.com/libeliumworld/top_50_iot_sensor_applications_ranking/

RedHat. (Consultado 2020). Obtenido de https://www.redhat.com/es/topics/cloud-computing/iaas-vs-paas-vs-saas

ZDNet. (12 de Abril de 2021). Obtenido de https://www.zdnet.com/article/these-new-vulnerabilities-millions-of-iot-devives-at-risk-so-patch-now/

Sobre el autor:

Gumercindo Armando Monzon Escobar, es investigador y profesor universitario con especialidad en tecnologías y ciberseguridad.

CC BY SA

CyberSecurity
Información & Privacidad

Ciberseguridad en Centros Educativos Públicos de Guatemala, un mecanismo para la protección de niños, niñas y adolescentes en el ciberespacio

Cybersecurity in Public Educational Centers of Guatemala, a mechanism for the protection of children and adolescents in cyberspace

Oscar E. Castro Juárez
ocastroj@miumg.edu.gt

Recibido:10/agosto/2021. Revisado: 22/septiembre/2021. Aprobado: 20/noviembre/2021.
Disponible en internet el 1 de enero de 2022

Resumen: En el presente artículo se abordó la idea de enseñar ciberseguridad en centros escolares, dando inicio con conceptos y definiciones que son importantes de comprender como por ejemplo el ciberespacio y los riesgos a los que se enfrentan los niños, niñas y adolescentes dentro del mismo, se hizo una revisión de los distintos elementos que permiten identificar la situación actual en cuanto al nivel de seguridad en el ciberespacio y la forma en la que es abordada por distintas organizaciones públicas.

Palabras Claves: ciberseguridad, ciberespacio, educación, riesgos, niños, niñas, adolescentes.

Abstract: In this article, the idea of teaching cybersecurity in schools was addressed, starting with concepts and definitions that are important to understand, such as cyberspace and the risks that children and adolescents face within it. Made a review of the different elements that allow identifying the current situation in terms of the level of security in cyberspace and the way in which it is approached by different public organizations..

Introducción

El ciberespacio es un ambiente donde pueden realizarse distintas actividades con diversidad de propósitos. Entre las personas que se pueden encontrar en él, se incluyen niños, niñas y adolescentes. Este grupo es uno de los más vulnerables, ya que el ciberespacio contiene dentro de sí muchos riesgos para los cuales no tienen los conocimientos necesarios o las herramientas suficientes para defenderse. En una encuesta realizada por la Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas evidenció que dentro de los riesgos que más afectan a los niños, niñas y adolescentes en Guatemala se encuentran: el grooming, sexting, sextorsión y ciberbullying.

En Guatemala se han generado materiales en formato físico y digital con contenidos que buscan informar a niños, niñas, adolescentes, padres, tutores y educadores, sobre los riesgos del ciberespacio y cómo poder identificarlos. Sin embargo, sigue sin abordarse el tema en los centros escolares de forma integral, de tal manera que les permita a los niños, niñas y adolescentes asimilar los conceptos según su nivel. Tomando en consideración que, entidades

como el Ministerio Público, Ministerio de Gobernación, Ministerio de Educación y la Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas pueden unir esfuerzos para la elaboración de planes y estrategias a implementar en los centros escolares, utilizando como instrumento orquestador la Estrategia Nacional de Seguridad Cibernética de Guatemala.

Asimismo, es importante contar con el conocimiento de la población sobre estos temas, para fomentar la cultura de ciberseguridad, con el fin de crear un ambiente más seguro en el ciberespacio.

Materiales y Métodos

En el año 2017 fue lanzada la campaña "Me Conecto Sin Clavos", la cual ofrece material informativo orientado a niños, niñas, adolescentes y adultos en general. Dicha campaña tiene como finalidad proteger a los niños y adolescentes al navegar en el ciberespacio, para ello ofrece distintos materiales, los cuales se pueden clasificar en: videotutoriales, juegos, comics, afiches, guías para educadores, líderes comunitarios y mensajes de audio (Orantes, 2017).

Según (Fundación Sobrevivientes y UNICEF, 2016), uno de sus objetivos es que la campaña pueda ser implementada en centros educativos para promover comportamientos de prevención y seguridad en línea. El objetivo de la investigación fue determinar los beneficios, la aceptación de la población y esfuerzos que realizan distintas entidades enfocadas a la enseñanza de Ciberseguridad en los centros escolares de Guatemala para la protección de los niños, niñas y adolescentes en el ciberespacio.

Por medio del enfoque metodológico documental explorativo, utilizado para la realización de esta investigación se recolecto información de distintas fuentes y medios con el fin de conocer y analizar la realidad a la que se enfrentan los niños, niñas y adolescentes al navegar en el ciberespacio. En la revisión del material, se clasificó en dos: fuentes primarias y fuentes secundarias. Teniendo un mayor peso la fuente primaria.

Según (Biblioteca Universidad de Alcalá, 2011), las fuentes primarias contienen información nueva y original pudiendo ser de distintos tipos: libros, periódicos, documentos oficiales de instituciones públicas, entre otros. Y las fuentes secundarias contienen información organizada, producto de análisis o reorganización que hace referencia a documentos primarios.

Las fuentes primarias obtenidas para el estudio se establecieron en 5 años máximo (entre 2017 y 2021), como periodo de análisis. Estas a su vez, correspondieron a información relevante sobre encuestas, estadísticas, definiciones relacionadas con ciberseguridad y los riesgos del ciberespacio que afectan a los niños, niñas y adolescentes actualmente en Guatemala.

Adicionalmente, fue realizada una encuesta en apoyo a la investigación, la cual fue elaborada en dos bloques, el primero de ellos tiene como propósito los siguientes aspectos: 1. Establecer si la población tiene asimilados los conceptos de ciberseguridad y ciberespacio, 2. Determinar si tienen conocimiento que existen riesgos para los niños, niñas y adolescentes al navegar en el ciberespacio, 3. Conocer la disposición sobre el uso de herramientas físicas o digitales para la protección de los niños, niñas y adolescentes en el ciberespacio y 4. Conocer la disposición para aceptar que en los centros escolares se enseñe ciberseguridad. El tipo de pregunta utilizado fue dicotómica.

El segundo bloque de la encuesta correspondió a preguntas de tipo politómicas (o categorizadas), teniendo como propósito lo siguiente: 1. Establecer la concepción sobre el grado de responsabilidad que tiene el gobierno para la enseñanza de ciberseguridad en centros escolares, 2. Determinar la responsabilidad de los padres o tutores en la enseñanza de ciberseguridad y 3. Conocer la percepción que se tiene sobre el nivel de seguridad con el que cuentan actualmente los niños, niñas y adolescentes al navegar en el ciberespacio.

Además, se utilizó una muestra representativa de 152 personas para la realización de la encuesta, dichas personas corresponden a residentes del departamento de Guatemala, mayores de 18 años. No se hizo distinción entre personas con o sin hijos ya que se considera importante tener la opinión de la población en general.

Materiales y Métodos

En este apartado se mostrarán los resultados obtenidos de las distintas fuentes de información, tanto primaria como secundaría. Haciendo una valoración de estas. También serán evaluados los resultados que fueron obtenidos a través de la encuesta realizada.

Estadísticas en Guatemala

A través de una encuesta que fue realizada a 400 padres de familia el (Fondo de las Naciones Unidas para la Infancia & Fundación Sobrevivientes, 2021) identificó que el 70% (280) que corresponde a padres, madres y tutores, desconocen de las técnicas con las cuales pueden engañar y seducir a menores en internet.

Una encuesta realizada por (OGDI, 2018) a 1651 estudiantes del nivel básico y bachillerato de la Ciudad Capital dio como resultado que el 30.41% de estudiantes (502) han sido víctimas de sexting y sextorsión, 24.89% (411) robo de identidad y 34.40% (568) han sufrido del acoso cibernético. A raíz de la pandemia de la Covid-19 se generaron nuevos retos para el sistema educativo del país. Uno de ellos es el regreso a clases, para lo cual la propuesta fue: realizar clases híbridas (Mutz, 2020), con esto, se expone a los niños, niñas y adolescentes aún más al ciberespacio y los riesgos que este conlleva (Ortiz, 2020).

Por ello, el (Ministerio de Educación, 2021) desarrolló una guía con el nombre de "Protocolos para el regreso a Clase – Para docentes de centros educativos", en la cual fue abordado el tema de ciberseguridad, estableciendo puntos de referencia para los educadores.

Resultados de la encuesta

En esta sección se mostrarán de forma gráfica y descriptiva los resultados de la encuesta realizada a 152 personas.

Tabla 1

Pregunta: ¿Sabe usted en qué consiste la ciberseguridad?

Sí	No
98	54

Fuente: Elaboración propia

El resultado indica que el 64.5% de los encuestados sí entiende el concepto de ciberseguridad.

Tabla 2

Pregunta: ¿Sabe usted qué es el ciberespacio?

Sí	No
98	54

Fuente: Elaboración propia

La intención con esta pregunta fue la de identificar qué porcentaje de encuestados entiende o está familiarizado con el concepto de ciberespacio. Dando como resultado que un 64.5% sí tiene nociones sobre el tema.

Tabla 3

Pregunta: ¿Sabe usted cuáles son los riesgos a los que se enfrentan los niños, niñas y adolescentes al navegar por el ciberespacio?

Sí	No
90	62

Fuente: Elaboración propia

Con las dos preguntas anteriores, se pudo determinar que más del 50% de los encuestados entiende o sabe en qué consiste la ciberseguridad y el ciberespacio. Sin embargo, la cantidad de personas que conocen los riesgos a los que se pueden enfrentar los

niños, niñas y adolescentes en el ciberespacio decreció un 5.3% con respecto a los temas abordados anteriormente.

Tabla 4

Pregunta: De tener hijos, ¿estaría de acuerdo en que se les enseñe ciberseguridad en el centro escolar al que asistan?

Sí	No
138	14

Fuente: Elaboración propia

El 90.8% de los encuestados estuvo de acuerdo en que se enseñe ciberseguridad en centros escolares.

Tabla 5

Pregunta: De tener hijos, ¿estaría de acuerdo en utilizar herramientas que permitan protegerlos al navegar por el ciberespacio?

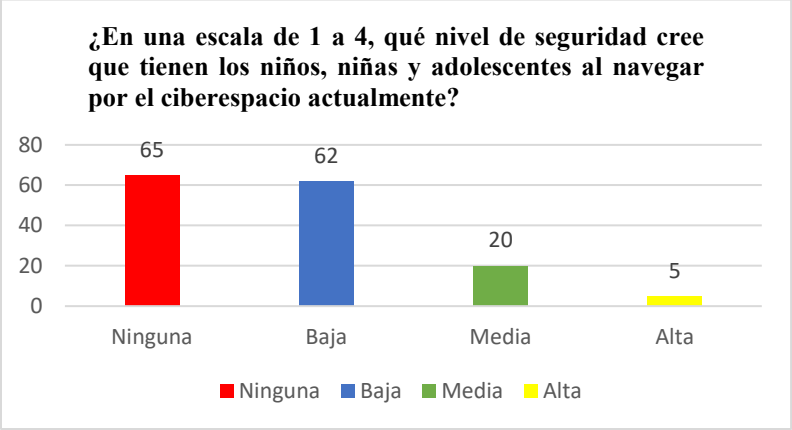
Sí	No
136	16

Fuente: Elaboración propia

La gráfica muestra que el 89.5% de personas estuvo de acuerdo en utilizar herramientas para la protección de los niños, niñas y adolescentes en el ciberespacio.

Figura 1

Seguridad al navegar en el ciberespacio

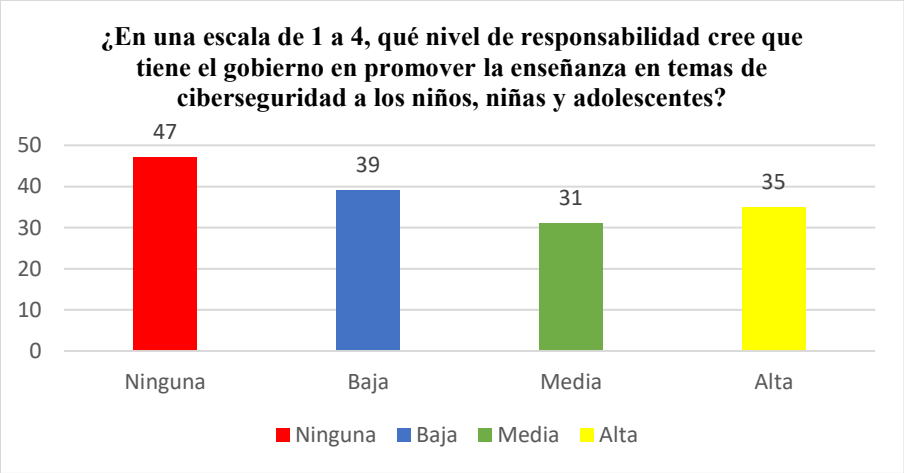


Fuente: Elaboración propia.

Esta pregunta tenía como finalidad establecer la percepción sobre el nivel de seguridad que tienen los niños, niñas y adolescentes al navegar en el ciberespacio. El 83.6% de los encuestados considera el nivel de seguridad como bajo o ninguno.

Figura 2

Responsabilidad del gobierno en temas de ciberseguridad



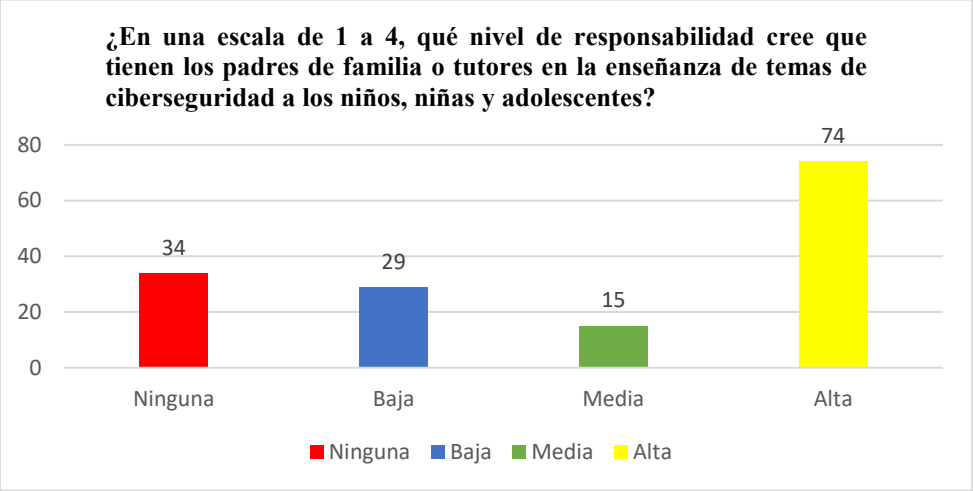
Fuente: Elaboración propia.

Esta pregunta tenía como propósito identificar qué porcentaje de los encuestados considera al gobierno como responsable de la enseñanza de ciberseguridad a los niños, niñas y adolescentes. Más del 50% de los encuestados consideró que el gobierno tiene ninguna o baja implicación.

Sin embargo, es importante tomar en cuenta que este al ser un tema que puede afectar la integridad física y mental de los niños, niñas y adolescentes sí le concierne al estado de Guatemala garantizar y velar por su seguridad.

Figura 3

Responsabilidad de padres o tutores en temas de ciberseguridad



Fuente: Elaboración propia.

Esta pregunta fue planteada con la hipótesis de que los padres y tutores son responsables de educar a los niños, niñas y adolescentes que estén bajo su responsabilidad en temas de ciberseguridad.

Esta hipótesis se confirma, ya que el 58.6% considera que sí son responsables con un nivel de implicación alto – medio.

Discusión

A través de las distintas fuentes que se han analizado con anterioridad, se puede observar que los niños, niñas y adolescentes son vulnerables a delitos de ciberseguridad. Siendo los más comunes en Guatemala la sextorsión, sexting, grooming y el cyberbullying. El contenido que se ha generado a través de la compaña "Me Conecto Sin Clavos" es útil como punto de partida para generar conciencia tanto para niños, niñas, adolescentes, educadores y público en general, pero puede no ser suficiente.

Es importante que se considere la enseñanza de ciberseguridad a través del sistema educativo con métodos y estrategias en las cuales se haga uso de tecnología y recursos que faciliten la práctica para la asimilación de los conceptos. Adicionalmente, es indispensable formar a los docentes en este tema, para que sean ellos quienes faciliten el conocimiento. Según el (Centro de Investigaciones Económicas Nacionales, 2020) a través de la propuesta ¡pongámosle turbo al aprendizaje!, indican que es necesario que los docentes puedan formarse en el uso de

tecnologías para el aprendizaje, lo que también permitiría que faciliten conocimientos de ciberseguridad.

Sin embargo, estos esfuerzos pueden llegar a tener poco alcance por distintos factores, como lo puede ser el desinterés o ignorancia por parte de alguno de los grupos específicos, para ello es importante que a través del Ministerio de Gobernación y Ministerio de Educación se elabore una propuesta de Ciberseguridad a incluir dentro del Currículo Nacional Base, esto como un enfoque integral a través de recursos digitales y físicos que pueda guiar a los niños, niñas y adolescentes a cómo estar alertas ante situaciones de peligro en el ciberespacio y a cómo generar ambientes seguros desde los dispositivos que utilizan para navegar por el ciberespacio.

Para ello es importante que se desarrollen y articulen planes de estudio en los que se realicen actividades y se ejemplifiquen casos prácticos que estén apegados a la realidad y a la evolución de las técnicas que utilizan los delincuentes para afectar a los menores. Según (Morán, 2019), la repetición es un mecanismo eficaz que permite consolidar lo estudiado. La Estrategia Nacional de Seguridad Cibernética debe funcionar como artefacto con el cual el Ministerio de Educación y el Ministerio de Gobernación tomen las acciones necesarias para la enseñanza de ciberseguridad en los centros educativos.

El bienestar de los niños, niñas y adolescentes al navegar por el ciberespacio es tema transversal a distintos ministerios, como lo es el Ministerio de Educación, Ministerio de Gobernación y Ministerio Público. Tomando en cuenta que pueden ser vulnerados sus derechos individuales y derechos humanos, deberían contar con una educación integral sobre ciberseguridad que les apoye en su desarrollo y crecimiento.

También debe de tomarse en consideración lo establecido en la Ley de Protección Integral de la Niñez y Adolescencia en los artículos 36, 41, 42, 53, 54, 59, 80 y 81, en conjunto establecen que debe ser proporcionada una educación integral, la promoción de derechos y las obligaciones del estado para formar y proteger a los niños, niñas y adolescentes (Congreso de la República de Guatemala, 2003).

Revisión de literatura

Ciberespacio: Según (EcuRed, 2021), el ciberespacio puede entenderse como un espacio no físico que nace a raíz de la unión de equipos de cómputo para formar una red. Produciendo así, un intercambio de información en tiempo real o diferido permitiendo diferentes tipos de actividades, como pueden ser jugar, trabajar, estudiar, comprar, explorar, o simplemente, compartir.

Ciberseguridad: La ciberseguridad consiste en mecanismos que se utilizan para la protección de sistemas, redes y programas de ataques digitales. Aborda aspectos que pueden ser englobados en personas, procesos y tecnología. Las prácticas de ciberseguridad evitan que delincuentes accedan, modifiquen o destruyan información confidencial con la cual puedan extorsionar o perjudicar a la persona o empresa que es blanco de sus actividades (CISCO, 2021).

Riesgos del ciberespacio: Según (Mendoza, 2018), los 10 riesgos más comunes a los que se enfrentan niños, niñas y adolescentes en el ciberespacio son: 1. Abuso sexual, 2. Ciberbullying, 3. Explotación sexual, 4. Exposición a contenidos nocivos, 5. Grooming, 6. Materiales de abuso sexual generado por computadora, 7. Publicación de información privada, 8. Paliza feliz, 9. Sexteo y 10. Sextorsión.

Ministerio de Gobernación Guatemala: Es la entidad encargada de velar por la seguridad del país. Se centra en cinco ejes, siendo los siguientes: 1. Seguridad, 2. Apoyo al sector justicia, 3. Gobernabilidad democrática, 4. Adaptación y fortalecimiento institucional, 5. Desarrollo y actualización tecnológica (Ministerio de Gobernación, 2020).

Estrategia Nacional de Seguridad Cibernética: El propósito de la estrategia es la de responder a la evolución que han tenido los ataques cibernéticos, siendo estos más sofisticados, la protección de los datos personales y atendiendo a la seguridad nacional como consecuencia de la dependencia del gobierno con el uso de las TICS (García-Belenguer, s.f). En junio del 2018 fue presentada la Estrategia Nacional de Seguridad Cibernética de Guatemala a cargo del expresidente Jimmy Morales, Ministerio de Gobernación y el Cuarto Viceministerio de Tecnologías de la Información y Comunicación (IPANDETEC, 2018).

Ministerio de Educación: Por ley, es la entidad que se encarga de velar por la coordinación y ejecución de las políticas educativas determinadas por el sistema educativo del país. También es el ente encargado de garantizar la calidad y la cobertura de la prestación de servicios educativos públicos y privados (Contreras, 2019).

Secretaría Contra la Violencia Sexual, Explotación y Trata de Personas: La secretaría Contra la Violencia Sexual, Explotación y Trata de Personas (SVET) es un ente que forma parte de la Vicepresidencia de la República. Su función principal es la elaboración de herramientas que permitan la lucha contra la violencia sexual, explotación y trata de personas (Global Database on Violence against Women, 2018).

Ley de Protección Integral de la Niñez y Adolescencia: Su propósito es el de lograr el desarrollo integral y sostenible de la niñez y adolescencia en Guatemala (Congreso de la República de Guatemala, 2003).

Referencias bibliográficas

Aroche, K. (10 de 09 de 2021). Historia del Currículo Nacional Base de Guatemala. Obtenido de Guatemala.com: https://aprende.guatemala.com/cultura-guatemalteca/historia-del-curriculo-nacional-base-de-guatemala/

Biblioteca Universidad de Alcalá. (05 de 04 de 2011). Fuentes de Información. Obtenido de Biblioteca Universidad de Alcalá: http://www3.uah.es/bibliotecaformacion/BPOL/FUENTESDEINFORMACION/tipos_de_fuentes_de_informacin.html

BitLife. (25 de 06 de 2019). Cibserseguridad: una cuestión de cultura. Obtenido de Bit Life: https://bitlifemedia.com/2019/06/ciberseguridad-una-cuestion-de-cultura/

Centro de Investigaciones Economicas Nacionales. (12 de 2020). ¡Pongámosle turbo al aprendizaje! Una propuesta para la Educación de Guatemala. Obtenido de cien: https://cien.org.gt/wp-content/uploads/2020/12/DocumentoPropuestaPongamosleTurboalaEducacionVF.pdf

CISCO. (04 de 10 de 2021). ¿Qué es la ciberseguridad? Obtenido de cisco: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Congreso de la República de Guatemala. (15 de 07 de 2003). DECRETO NUMERO 27-2003. Obtenido de OAS: https://www.oas.org/dil/esp/ley_de_proteccion_integral_de_la_ninez_y_adolescencia_guatemala.pdf

Constitución Política de la República de Guatemala. (17 de 11 de 1993). Obtenido de Minfin: https://www.minfin.gob.gt/images/downloads/dcp_marcolegal/bases_legales/Constitucion_politica_de_la_republica_de_guatemala.pdf

Contreras, L. (18 de 07 de 2019). Ministerio de Educación cumple hoy 147 años de fundación. Obtenido de Agencia Guatemalteca Nacional: https://agn.gt/archivo/ministerio-de-educacion-cumple-hoy-147-anos-de-fundacion/

Currículo Nacional Base Guatemala. (2021). Currículo Nacional Base Guatemala. Obtenido de Currículo Nacional Base Guatemala: https://cnbguatemala.org/

EcuRed. (2021). Ciberespacio. Obtenido de EcuRed: https://www.ecured.cu/Ciberespacio

Fondo de las Naciones Unidas para la Infancia & Fundación Sobrevivientes. (2021). Conoce las Campañas de Prevención. Retrieved from Me Conecto Sin Clavos: https://meconectosinclavos.net.gt/campanas/

Fundación Sobrevivientes y UNICEF. (2016). Guía de implementación "ME CONECTO SIN CLAVOS". Obtenido de Sobrevivientes: http://www.sobrevivientes.org/docs/conecto_sin_clavos/_no-implementacion_estrategia%20(incluye%20redes).pdf

García-Belenguer, G. (s.f.). Programa de Seguridad Cibernética. Obtenido de Organización de los Estados Americanos: https://www.itu.int/en/ITU-D/Regional-Presence/Americas/Documents/EVENTS/2016/15551-EC/10A.pdf

Global Database on Violence against Women. (15 de 02 de 2018). Secretaría contra la Violencia Sexual, Explotación y Trata de Personas. Obtenido de Global Database on Violence against Women: https://evaw-global-database.unwomen.org/en/countries/americas/guatemala/na/secretaria-contra-la-violencia-sexual-explotacion-y-trata-de-personas

IPANDETEC. (02 de 07 de 2018). La Estrategia Nacional de Seguridad Cibernética en Guatemala . Obtenido de ipandetec: https://www.ipandetec.org/2018/07/02/la-estrategia-nacional-de-seguridad-cibernetica-en-guatemala/

Izquierdo, E. (01 de 07 de 2019). ¿En qué consiste la Estrategia de Ciberseguridad Nacional? Obtenido de Nexteducacion: https://www.nexteducacion.com/en-que-consiste-la-estrategia-de-ciberseguridad-nacional/

Mendoza, M. Á. (17 de 05 de 2018). 10 principales amenazas que enfrentan niños y adolescentes en Internet. Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2018/05/17/principales-amenazas-enfrentan-ninos-adolescentes-internet/?utm_source=pocket_mylist

Ministerio de Educación. (01 de 2021). PROTOCOLO PARA EL REGRESO A CLASES - Para docentes de centros educatviso. Obtenido de Mineduc: https://aprendoencasayenclase.mineduc.gob.gt/images/sampledata/asimages/regreso-a-clases/PROTOCOLO-Docentes-de-centros-educativos.pdf

Ministerio de Gobernación. (01 de 03 de 2018). Estrategia Nacional de Seguridad Cibernética. Obtenido de Ministerio de Gobernación de Guatemala: https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf

Ministerio de Gobernación. (14 de 01 de 2020). Valores y Objetivos. Obtenido de Ministerio de Gobernación: https://mingob.gob.gt/valores-y-objetivos/

Morán, E. (19 de 05 de 2019). La práctica y la repetición como base del aprendizaje. Obtenido de smartick: https://www.smartick.es/blog/educacion/psico/practica-repeticion-aprendizaje/

Mutz, V. (01 de 12 de 2020). Ciclo escolar 2021 será con clases híbridas . Obtenido de República: https://republica.gt/2020/12/01/ciclo-escolar-2021-sera-con-clases-hibridas/

OGDI. (23 de 07 de 2018). Observatorio Guatemalteco de Delitos Informaticos. Obtenido de Observatorio Guatemalteco de Delitos Informaticos: https://ogdi.org/estadisticas

Orantes, V. (18 de 05 de 2017). Lanzan campaña #MeConectoSinClavos para proteger a los niños en Internet. Obtenido de Guatevision: https://www.guatevision.com/historico/lanzan-campana-meconectosinclavos

Organización de los Estados Americanos. (2018). Lineamientos para el empoderamiento y la protección de los derechos de los niños, niñas y adolecentes en Internet en Centroamérica y República Dominicana". Washington: OEA.

Orozco, A. (16 de 10 de 2016). Redes sociales rompen conducta. Obtenido de PrensaLibre: https://www.prensalibre.com/guatemala/comunitario/redes-sociales-rompen-conducta/

Ortiz, J. (12 de 2020). Violencia que los niños, niñas y adolescentes han atravesado durante la pandemia del COVID-19. Obtenido de nuestravozacolores: http://nuestravozacolores.org/wp-content/uploads/2020/12/INFORME-REGIONAL-GUATEMALA-2020.pdf

Ramos, S. (16 de 03 de 2021). Inscripción de estudiantes se reduce 14.6% en 2021 . Obtenido de República: https://republica.gt/2021/03/16/guatemala-inscripcion-estudiantes-reduce-14-6-por-ciento-2021/

unicef. (2019, 06). Niños, niñas y adolescentes en línea - Riesgos de las redes y herramientas para protegerse. Retrieved from unicef: https://www.unicef.org/guatemala/informes/ni%C3%B1os-ni%C3%B1as-y-adolescentes-en-l%C3%ADnea

Sobre el autor:

Ingeniero en sistemas, con estudios en Seguridad Informática. Actualmente laborando para una empresa del sector financiero y con más de 5 años de experiencia en el ámbito de desarrollo de aplicaciones. Persona curiosa, que siempre está aprendiendo sobre temas de desarrollo de software, arquitectura de aplicaciones y la capa de seguridad de estas.

CC BY SA

Donaciones

Mas Información

paypal.me/incibegt

info@csecmagazine.com

CyberSecurity
Información & Privacidad

LINEAMIENTOS PARA LA PUBLICACIÓN DE ARTÍCULOS

Lineamientos Generales

Los artículos aceptados que se publicarán en la revista Cybersecurity – Información y Privacidad- corresponden a:

- Artículos con los resultados de proyectos de investigación que se hayan llevado a cabo.
- Artículos invitados, solicitados directamente al autor, por el Editor o el Comité Editorial.
- Artículos de síntesis y opinión que unifiquen e interpreten el avance del conocimiento en un tema.
- Ensayos y trabajos.
- Resúmenes y acotaciones sobre conferencias, seminarios, talleres y foros.
- En los números especiales de la Revista, patrocinados por un proyecto, podrán publicarse los artículos en idioma inglés.

Proceso de revisión de pares: El proceso de revisión por pares queda a cargo del Consejo Científico y entrará a funcionar de acuerdo con las responsabilidades señaladas para tal órgano.

Derechos de autor: El autor cede gratuitamente sus derechos sobre los artículos enviados a la Revista para el único propósito de que sean editados, publicados e impresos o reimpresos en la Revista Cybersecurity Magazine (impresa o digital). El autor podrá publicar posteriormente sus artículos en otros medios a condición de que señale la publicación previa en la revista. Los autores, juntamente con su artículo, remitirán el formulario de cesión de derechos de propiedad intelectual correspondiente.

Plagio: El Plagio será sancionado con la no publicación del artículo y en caso de haber sido publicado con la aclaración en el número próximo más cercano del problema encontrado y el señalamiento del autor de la infracción ética. El Consejo Editorial tomará cualquier medida complementaria que estime necesaria.

Envío electrónico: La revista recibirá las contribuciones de los autores únicamente por correo electrónico a la dirección que aparezca en la convocatoria para los autores y se enviará en un archivo de formato Word de Microsoft el cual se deberá enviar a la siguiente dirección: cfa@csecmagazine.com.

Limitaciones en la extensión de los artículos: Los artículos, deberán contener entre 4,000 a 10,000 palabras (incluidas las citas y pies de página). Excepcionalmente el Consejo Editorial podrá autorizar la publicación de artículos de mayor extensión.

Revisión de los artículos: Los artículos serán analizados cuidadosamente por los Pares Revisores para asegurar que su calidad es suficiente para ser publicados. La revisión se podrá hacer por los métodos de "ciego simple" o "doble ciego".

Los artículos deben de cumplir:

1. Exhibir coherencia conceptual, profundidad en el dominio de la problemática abordada.

2. Estar escritos en un estilo claro, ágil y estructurado de acuerdo con la naturaleza del texto; con base al modelo APA 6ta. Ed.

3. La extensión mínima del artículo será de 2 páginas con un máximo de 10, letra tamaño 12, tipo Arial, interlineado 1.5, márgenes de 3 centímetros, hoja tamaño carta.

5. Presentar carta firmada por el autor, según formato anexo, indicar la cobertura temática del artículo de acuerdo con la clasificación según la especialidad.

6. Los manuscritos para su publicación deben incluir:

Título. Debe escribirlo en mayúscula y negrilla, no contener fórmulas ni abreviaturas, ser breve y consistente con el trabajo. En idioma español y en inglés.

Nombre de los autores. Se escribe el primer nombre, la inicial del segundo nombre si lo hay, seguido del apellido. Cuando existe más de un autor, se separan con comas. Se debe indicar con un asterisco la persona a la que puede dirigirse la correspondencia. Además de un extracto del resumen de su experiencia laboral, profesional, adicionando una foto de estudio a color, correo electrónico y redes sociales (LinkedIn)

Nombre de la institución y dirección. Para indicar la afiliación de cada autor use superíndices en el nombre del autor. Para el autor que lleva el asterisco se debe indicar, la dirección completa, teléfono, fax y correo electrónico, a donde pueda dirigirle la correspondencia. Esto solo aplica si representa a una empresa y ha establecido un contrato de publicidad en la revista.

Resumen en español. No debe exceder de 250 palabras. Debe contener los principales resultados y conclusiones haciendo énfasis en los logros alcanzados. Como los resúmenes son copiados directamente de las bases de datos por los interesados, deben contener en forma abreviada el propósito del estudio y las técnicas experimentales, los resultados e interpretaciones de los datos. Los términos relevantes importantes para comprender el contenido del artículo. Se debe entender con facilidad sin tener que recurrir al texto completo.

Introducción. No es necesario incluir toda la literatura sobre el tema en esta sección. Se debe describir el planteamiento general, con la información necesaria en forma concisa, haciendo referencia a los artículos directamente relacionados y que se considere indispensable para el

desarrollo del tema y que permita al lector encontrar a otros investigadores del campo, relacionados con el problema o interrogante planteada por el autor. No se deben, por lo tanto, incluir revisiones amplias de la bibliografía.

Materiales y métodos: Si existen secciones diferenciadas, deben indicarse con encabezados pertinentes (por ejemplo, síntesis, muestreo, preparación de muestras, etc.). La explicación de los métodos experimentales debe hacerse con los suficientes detalles para que otros investigadores puedan repetirla. La descripción de equipos y reactivos sólo se debe incluir cuando sean específicos o novedosos. Se debe evitar la descripción de procedimientos aplicados con anterioridad por otros autores, pero se debe citar la bibliografía pertinente. Si existen modificaciones a procedimientos ya publicados, se deben incluir los detalles de esta.

Desarrollo (Cuerpo del Trabajo): El desarrollo del tema debe exponerse claramente, el objetivo del artículo debe de ayudar a los lectores a que puedan entender y analizar el trabajo.

Resultados de discusión. Presente los resultados en forma clara y concisa, en lo posible en uno de los siguientes formatos: texto, tablas o figuras. Evite duplicar la presentación de los resultados en tablas y figuras. La discusión debe proporcionar una interpretación de los resultados en relación con trabajos previamente publicados y no debe contener repetición considerable o amplia de la sección de resultados o reiteración de lo dicho en la introducción. La información escrita en el texto debe ser citada, pero no se debe repetir en detalle lo ya expuesto. En la discusión es permitida la especulación, pero debe estar bien fundamentada. inal un párrafo para hacer resaltar las conclusiones más relevantes del trabajo.

s: Presente los resultados en forma clara y concisa, en lo posible en uno de los siguientes formatos: texto, tablas o figuras. Evite duplicar la presentación de los resultados en tablas y figuras. La discusión debe proporcionar una interpretación de los resultados en relación con trabajos previamente publicados y no debe contener repetición considerable o amplia de la sección de resultados o reiteración de lo dicho en la introducción. La información escrita en el texto debe ser citada, pero no se debe repetir en detalle lo ya expuesto. En la discusión es permitida la especulación, pero debe estar bien fundamentada. Dedique al final un párrafo para hacer resaltar las conclusiones más relevantes del trabajo.

Bibliografía. Listado de las fuentes bibliográficas citadas en el artículo en orden alfabético, según el apellido del primer autor, utilizar el modelo APA 6ta. Ed.

POR MOTIVOS DE DERECHOS DE AUTOR, ARTICULOS PUBLICADOS EN OTRAS PLATAFORMAS NO SE TOMARÁN EN CUENTA PARA EVITAR TEMAS LEGALES, A MENOS QUE EL AUTOR INDIQUE CLARAMENTE QUE ES PROPIETARIO DE DICHA INVESTIGACION.

La Editorial

cfa@csecmagazine.com

CyberSecurity
Información & Privacidad

Ciudad de Guatemala, de 2,022.

A:

Coordinadora de la Revista Cybersecurity

Presente.

Yo, _____de nacionalidad _____

Identificación No. _____

correo electrónico_____: Teléfono: _____,

Hago constar que el artículo con título:

Acerca de una investigación con el nombre:

Que presento es original y nunca ha sido publicado en otra revista, medio escrito o electrónico y tampoco ha sido presentado a arbitraje en otra revista impresa o digital.

Además, acepto las normas de la revista, en cuanto a procedimiento, formato y demás procedimientos indicados en los lineamientos para publicación de artículos.

_____

Firma

CyberSecurity
Información & Privacidad

Magazine
CyberSecurity
Información & Privacidad

AUCI invita a participar en la

Convocatoria de Artículos de Ciberseguridad en la

Revista Digital Cybersecurity – Información & Privacidad

(CFA)

Si eres investigador y/o tienes un artículo sobre ciberseguridad y/o las tecnologías de la información de tu autoría, envíanos tu resumen para poder analizarlo y posteriormente publicarlo.

cfa@csecmagazine.com

Magazine

CyberSecurity

Información & Privacidad