Volumen 2. Número 2. Serie A
ISBN: 978-99939-0-055-9
ISSN: 2708-1141

CyberSecurity

Información & Privacidad

INCIBE Guatemala

Resumen de Conferencias

La importancia de la informática forense

Como un eslabón en el proceso de ciberseguridad

Hardening

como técnica de ciberdefensa a la infraestructura de red local

Informe de transformación digital

Caso de Estudio: Ingenio azucarero en Guatemala

La descomposición de la ciberseguridad

Factores que aportan valor.

CyberSecurity
Información & Privacidad

CyberSecurity

Información & Privacidad

Proyecto de:

Con financiamiento de:

INCIBE GT
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ISBN: 978-99939-0-055-9

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

Mayo – Agosto 2021

Nota del editor

La Ciberseguridad En La Actualidad

La transformación digital a nivel mundial ha incrementado considerablemente y la crisis sanitaria COVID-19 ha sido un acelerador importante en este crecimiento que se ha dado en todos los ámbitos en donde nos relacionamos.

Nos hemos visto obligados a cambiar y adaptar algunas de las actividades para poder continuar con el desarrollo normal de estas, durante este periodo hemos tenido el reto de integrar a nuestras conexiones de internet residencial, las actividades de carácter laboral en donde se establecen túneles de conexión hacia la red empresarial para continuar con el flujo habitual de nuestras funciones, así como en algunos casos establecer conexiones escolares; para mantener la educación a distancia de los niños.

Sin embargo, las conexiones domiciliares a pesar que nos han permitido mantenernos conectados a la oficina, en el tiempo han ido evolucionando hacia un ecosistema de interconexión con diferentes dispositivos que interactúan con internet o bien con otras tecnologías, a lo que hoy, conocemos como el internet de las cosas o IoT (por su siglas en inglés internet of things) lo cual nos ofrece facilidades que van desde tener dispositivos de ocio y entretenimiento como lo son los televisores; que pueden ser controlados por otros dispositivos a distancia, aparatos de comunicación celular, tablets, smartwatchs, hasta la automatización de diferentes funciones mecánicas o tecnológicas dentro del hogar, como controlar la iluminación a distancia, controlar dispositivos de seguridad como un sistema de cámaras, apertura o bloqueo de puertas, e integrar electrodomésticos de nueva generación a la misma red.

Si bien el internet de las cosas viene a facilitar las actividades cotidianas, su adopción nos deja riesgos adicionales, de los cuales los ciberdelincuentes están buscando aprovecharse para tomar control de ellos, por tal motivo es imperante su uso apropiado siguiendo las siguientes recomendaciones: Colocar contraseñas robustas, Utilizar herramientas de protección (en los dispositivos que aplique), evitar exponerse a utilizar softwares ilegales y No alterar las características de seguridad recomendadas por los fabricantes, Ya que se puede tener un impacto directo en la privacidad e integridad de la información y puede dejar puertas de comunicación abiertas hacia el internet, entre otras.

El compromiso de cada uno de nosotros como primera línea de defensa es fundamental para prevenir amenazas a la seguridad de la información, en complemento a las acciones que deben tomar los responsables en implementar las contramedidas tecnológicas identificadas en el ciclo de administración riesgos.

Jose Alfredo Urías

INDICE

Resumen de Conferencia

I Congreso De Investigación Y Desarrollo De Tecnologías En Latinoamérica y I Congreso Fuertes y Seguras

INCIBE Guatemala

I Congreso de Investigación y Desarrollo en Tecnologías y Ciberseguridad de América Latina y I Congreso Fuertes y Seguras

INCIBE Guatemala
info@incibe.gt
Aprobado: 20/marzo/2021.
Disponible en internet el 1 de mayo de 2021

Resumen: INCIBE Guatemala llevo a cabo su primer Congreso de Investigación y Desarrollo en Tecnologías y Ciberseguridad de América Latina el 29 de enero del presente año, donde se contó con la participación de varios investigadores y profesionales en el área de desarrollo y ciberseguridad de Guatemala, Argentina, Panamá y Chile quienes expusieron sus investigaciones y resultados de acuerdo con el eje tratado. Durante más de 5 horas los investigadores propusieron modelos que ayuden a mejorar la ciberseguridad en empresas, universidades y en personas para lograr un desarrollo y protección integral. Además el primer Congreso Fuertes y Seguras, que contó con la participación de 8 profesionales de Guatemala, Argentina y Ecuador que se realizó el 23 de abril, donde se discutieron varias temáticas sobre la presencia de las mujeres en las tecnologías y su búsqueda en la equidad de género, durante 4 horas las expositoras mostraron su punto de vista en temas de investigación y empoderamiento femenino.

Palabras Claves: ciberseguridad, investigación, desarrollo, tecnología, igualdad.

Abstract: INCIBE Guatemala held its first Congress on Research and Development in Technologies and Cybersecurity in Latin America on January 29 of this year, with the participation of several researchers and professionals in the area of development and cybersecurity from Guatemala, Argentina and Chile who presented their research and results in accordance with the axis discussed. For more than 5 hours, the researchers proposed models that help improve cybersecurity in companies, universities and people to achieve comprehensive development and protection. In addition, the first Strong and Safe Congress, which had the participation of 8 professionals from Guatemala, Argentina and Ecuador that was held on April 23, where various topics were discussed on the presence of women in technologies and their search for equity. gender, for 4 hours the speakers showed their point of view on research issues and female empowerment.

Desarrollo:

Durante el Primer Congreso de Investigación y Desarrollo en Tecnologías y Ciberseguridad de América Latina se expusieron temas de las tecnologías y ciberseguridad desde un punto de vista científico, mostrando estudios realizados por investigadores latinoamericanos acerca de la creación de modelos predictivos, metodologías propias y adaptables a casos de uso, creación de software o servicios de Inteligencia Artificial, Seguridad de sistemas, Brechas de Seguridad, estudios sobre riesgos tecnológicos en personas, Aprendizaje Maquina, entre otros para la solución de problemáticas basados en tecnologías y minimizar ataques informáticos, optimización de datos, entre otros. La inauguración del primer Congreso de Investigación y Desarrollo en Tecnologías y Ciberseguridad de América Latina estuvo a cargo del Ingeniero Camilo Gutierrez de ESET Latinoamérica Argentina con el tema “Aplicaciones prácticas de la teoría de grafos en los procesos de inteligencia de

amenazas" donde demostró al público la importancia de la integración de la inteligencia artificial al análisis de amenazas. Diego Muñoz de Sombre Blanco de Chile demostró en un taller las técnicas de enumeración para la post explotación de sistemas Windows. Lía Hernandez expuso el estado actual de la protección de los datos personales en el contexto centroamericano demostrando la falta de normativas en la mayoría de los países y como esto influye en la protección de la información de los habitantes de cada uno de los países centroamericanos.

Leli Zamorano y Emanuel Pacheco de la Fundación Katy Summer expusieron los resultados de su investigación llevada a cabo en Chile acerca del Ciberacoso y salud mental en jóvenes chilenos entre 15 y 29 años, demostrando la necesidad de realizar este tipo de estudios en los países participantes, ya que puede ayudar a minimizar el impacto de la educación en linea por temas de COVID. Pablo Barrera de Estrategia y Seguridad en Guatemala, expuso la Gestión de Incidentes desde una Perspectiva de Riesgos demostrando la importación de adoptar marcos o metodologías para una correcta administración de los riesgos tecnológicos con las empresas. Cristian Barria director del Centro de Investigación en Ciberseguridad (CICS) e investigador de la Universidad Mayor de Chile expuso su investigación "Amenazados" desde un contexto filosófico, mostrando a lo largo del tiempo la evolución de la ciberseguridad y su actual impacto en las actividades realizadas a diario y dentro de las organizaciones.

Yonatan Grajeda de Fortinet Guatemala, desarrolló su investigación Análisis y Tendencias de Ciberataques en América Latina por Fortiguard Labs, mostrando con la inteligencia artificial de Fortinet lleva a cabo el análisis de amenazas en tiempo real proveyendo a sus clientes los más altos estándares en protección cibernética. Por último Christian Nanne de Sistemas Aplicativos en Guatemala mostro las investigaciones que se realizan por parte de la empresa a lo largo de centroamérica y el caribe donde tienen presencia denominada "Analizando tendencias de brechas en la región" información valiosa para tener visibilidad sobre los ataques informáticos más comunes dentro de las organizaciones.

Desde INCIBE Guatemala específicamente su proyecto de Woman in Security se desarrolló su primer Congreso Fuerte y Seguras, donde buscaban que la experiencia de las expositoras pudiese mostrar su visión desde aspectos de su vida diaria hasta llegar a la profesional y como han logrado tener más presencia en estas épocas incluida la pandemia de Covid-19. El proyecto está enfocado en desarrollar un apoyo mutuo para lograr un cambio social y cultural, logrando así que más mujeres impacten en su entorno para construir una sociedad más tecnológica e innovadora.

Dicho Congreso tuvo la participación de 8 profesionales de Guatemala, Argentina y Ecuador donde desarrollaron temas de importancia para logar los objetivos de este. Devora Meza de Guatemala, desarrollo su tema "Violencia contra la Mujer a través de las TICs" (Tecnologías de información) brindado recomendaciones para mitigar este tipo de violencia contra las mujeres en estas épocas de pandemia. Lesly Machorro desarrolló la "Privacidad de Datos en la era de las ciber amenazas", logrando recopilar eventos actuales donde la privacidad de los datos se convierte en el blanco de ciber delincuentes que pretenden la utilización de estos para la usurpación de identidad entre otros.

Soledad Fuster de Argentina desarrolló la presentación de “Investigación sobre Prevención y Sensibilización de Violencia en linea contra la Mujer” y como los engaños de pederastas ocasiones riesgos en mujeres, desde su participación en Organizaciones en Argentina dio recomendaciones para lograr minimizar estos efectos negativos en la sociedad. Mariela Villamarín expuso su punto de vista sobre “Las huellas femeninas, y la participación de la mujer en la ciberseguridad” desde el inicio de la utilización de modelos matemáticos y el auge en las tecnologías.

Alba Guerrero desarrolló el tema desde un punto de vista del cambio climático y su relación con las ingenierías con “El rol de la mujer profesional en la construcción de una región más resiliente”, logrando demostrar el trabajo que se realiza en nivel centroamericano para minimizar el impacto del cambio climático en la región. Mildred Caballeros expuso su investigación sobre la Automatización de pruebas con algoritmos de Machine Learning y su aplicabilidad en la industria y la construcción de algoritmos para realizar tareas específicas.

Karen Dubón, realizó su tema desde la perspectiva de “La educación virtual, una oportunidad para las mujeres” mostrando herramientas disponibles para su utilización y permanecer activas en el ciber espacio, con ello recomendó la utilización de plataformas que ayuden a aumentar su conocimiento. Por último Nancy Perez abordo el tema de “Empoderamiento” desde una perspectiva de género y como la mujer desde el pasado no ha sido tomada en cuenta para pertenecer a una sociedad más activa, algo que en los últimos años ha cambiado para el bien de las mujeres ya que se han desarrollado proyectos para que tengan más presencia en política como academia.

Para INCIBE Guatemala fue un éxito contar con la participación de más de 500 personas en estos congresos que vienen a proveer puntos de vista distintos para los participantes.

Artículos

CyberSecurity
Información & Privacidad

La importancia de la informática forense como un eslabón en el proceso de ciberseguridad

The importance of forensic computers as a link in the cybersecurity processes

Fredy E. Sánchez Gálvez
email: frsanchez122@gmail.com

Recibido:6/enero/2021. Revisado: 12/marzo/2021. Aprobado: 23/marzo/2021.
Disponible en internet el 1 de mayo de 2021

Resumen: La ciberseguridad es un proceso que se encarga de proteger los activos informáticos, tales como computadoras, servidores y sistemas. Procura crear y mantener una infraestructura segura, tratando de no dejar brechas de seguridad. Pero ¿qué es lo que pasa si un sistema se ve comprometido por un ataque informático? ¿Cómo saber qué fue lo que sucedió? ¿Qué información estuvo comprometida? ¿Qué equipos estuvieron comprometidos? en estos casos es importante apoyarse de procesos investigativos que brinden con fundamentos lo sucedido y que permitan judicializar los resultados. Para ello está la informática forense la cual se encarga de buscar e identificar el origen de posibles ataques dirigidos hacia sistemas informáticos, identificar daños causados, analizar e interpretar resultados, proponer contramedidas que eviten que se repita un suceso de similar y finalmente presentar evidencia informática que puede ser utilizada en procesos judiciales.

Palabras Claves: ciberseguridad, informática forense, procesos, ataques.

Abstract: Cybersecurity is a process that is responsible for protecting computer assets, such as computers, servers and systems. Try to create and maintain a secure infrastructure, trying not to leave security gaps. But what happens if a system is compromised by a computer attack? How do you know what happened? What information was compromised? What teams were involved? In these cases, it is important to rely on investigative processes that provide justification for what happened and that allow the results to be prosecuted. For this, forensic computing is in charge of searching and identifying the origin of possible attacks directed at computer systems, identifying damage caused, analyzing and interpreting results, proposing countermeasures that prevent a similar event from being repeated and finally presenting computer evidence that can be used in legal proceedings.

Desarrollo:

La ciberseguridad como proceso para proteger los activos informáticos debe apoyarse de técnicas o disciplinas para mitigar riesgos, recuperar los procesos ante desastres, responder inmediatamente ante cualquier incidente de seguridad y por supuesto que permitan una investigación en distintos sistemas vulnerados o comprometidos, con el fin de obtener evidencia digital que pueda servir para realizar mejoras de los controles implementados o

bien para sustentarla como prueba ante un juez, cuando se ha concretado un delito, como por ejemplo la fuga de información, destrucción de registros o archivos, entre otros.
Durante el año 2020, se registraron cerca de 32,000 incidentes de seguridad informática y casi 4,000 filtraciones confirmadas en todo el mundo, según datos obtenidos del Data Breach Investigations Report (DBIR) de Verizon. La informática forense como disciplina desde el ámbito técnico-científico, sirve como apoyo a la administración de justicia y el derecho. (Ortíz, 2019). Es por ello por lo que la informática forense es un complemento importante en todo el proceso que comprende la ciberseguridad, mediante la cual se garantiza la integridad de registros y/o archivos que servirán como evidencia digital para la resolución de hechos cometidos en plataformas tecnológicas y para mejorar o robustecer los sistemas de seguridad informática de una organización.

Ciberseguridad y Defensa en Profundidad

Según Cisco "La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales" (CISCO). Además "La ciberseguridad no es una técnica, sino un proceso integral" (Monzón, 2018). Esta afirmación indica que la ciberseguridad no simplemente se trata de instalar un antivirus o instalar un equipo de monitoreo, sino que es todo un proceso en el cual se complementan equipos, personas, procesos, políticas normativas, manuales, planes de contingencias y de recuperación, entre otros.

Como una de las estrategias de ciberseguridad, la empresa Northrop Grumman publica en el año 2017, en la IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), un marco de defensa de ciberseguridad por capas, que ilustra los componentes de la defensa en profundidad, este arquitectura "obliga a un ciberdelincuente o bien a un adversario a vulnerar o vencer distintos controles de seguridad para poder tener acceso a los activos de información" (Ciberseguridad en Linea, 2020). La aplicación de estas capas, mediante marcos de trabajo, permite disminuir la brecha de seguridad de una infraestructura de red, tanto a nivel físico como lógico.

Este marco de defensa en profundidad permite proteger servidores, incrementar la posibilidad de rastrear o atrapar a un intruso (ciberdelincuente) y reducir en gran medida la perdida de información. Este se compone de al menos cinco perímetros de seguridad, que resguardan los activos de información críticos para una organización. Los perímetros de seguridad que componen el marco de defensa en profundidad son los siguientes: Seguridad Perimetral, Seguridad de Redes, Seguridad de Punto Final (endpoint), Seguridad de Aplicaciones y Seguridad de Datos

Asimismo hace referencia a la administración de políticas para la prevención y a las operaciones de monitoreo y respuesta. En el lado de Administración de Políticas para la

Prevención, abarca Gobierno de TI, marcos de trabajo para la administración del riesgo, pruebas de penetración, políticas de seguridad y cumplimiento, entre otros. Y por el lado de las Operaciones de Monitoreo y Respuesta, incluyen los paneles de administración de seguridad, sistemas integrados de aseguramiento de la información, los centros de operaciones de seguridad (SOC), centros de operaciones de seguridad de redes (NOC), respuestas ante incidentes, informática forense, entre otros.

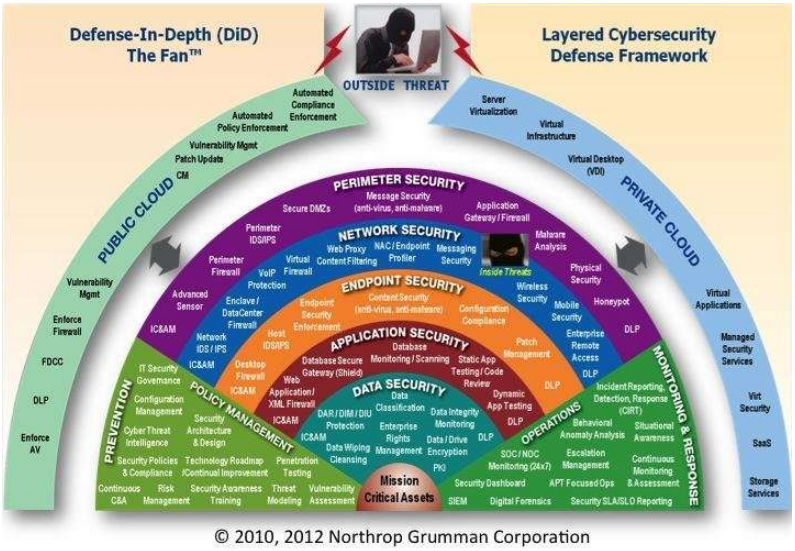


Imagen 1. Marco de Trabajo de Defensa en Profundidad

El Rol de La Informática Forense

La informática forense y la respuesta a incidentes informáticos son dos disciplinas que en muchas ocasiones se aplican al mismo tiempo, sin embargo existen diferencias que las separan totalmente.

La respuesta ante incidentes se denomina una disciplina que tiene como objetivo determinar el origen y el alcance de incidentes de seguridad, con lo que puede establecer mejoras para evitar que situaciones similares vuelvan a ocurrir. (Rubio Alamillo, 2020). Esta trata a toda costa de identificar el incidente, contenerlo, erradicarlo y por último realizar actividades de recuperación.

Por otro lado la informática forense, es una disciplina que no necesariamente busca interrumpir o detener un incidente de seguridad, sino que tiene por objetivo responder las siguientes preguntas: ¿cómo sucedió? ¿Cuáles fueron los activos informáticos vulnerados y comprometidos? ¿Cuáles fueron las causas? ¿Quién y cómo se ejecutó la vulnerabilidad? y ¿Qué información fue vulnerada? Por lo general su ámbito de trabajo es post-mortem, lo que quiere decir que se realiza en sistemas apagados o bien cuando ya ha pasado el incidente,

asimismo es esencial para la resolución de conflictos en procesos judiciales en donde estén relacionados dispositivos de procesamiento y/o almacenamiento digital.

Los modelos de trabajo para el análisis informático forense se resumen genéricamente en cuatro etapas o actividades:

1. **Identificar y Adquirir**: En donde se deben identificar aquellos dispositivos electrónicos de procesamiento y almacenamiento que pudieron haber sido afectados por un ataque de seguridad, generando una o más copias que sean lo más exactas posibles, para garantizar que el original no sea alterado accidental o intencionalmente.

Es importante hacer mención que en esta etapa se deben recolectar todas aquellas muestras que sean de relevancia para la resolución de un hecho, iniciando por los datos más volátiles como los registros de la caché y la memoria RAM, así como otros registros que permitan al analista obtener líneas de tiempo como los registros del sistema, listas de procesos activos, listas de puertos abiertos, programas instalados, programas desinstalados recientemente y otros artefactos del sistema que puedan apoyar la reconstrucción del hecho.

2. **Preservar**: En esta actividad todo elemento que es adquirido es sometido a sumas de verificación o comprobación a través de algoritmos hash para garantizar su identidad, integridad y autenticidad, desde su adquisición, hasta la presentación ante un juez, asimismo en esta etapa se inicia la cadena de custodia de todos y cada uno de estos elementos.

Generalmente en la informática forense se utilizan los algoritmos MD5 y SHA1, sin embargo, a pesar de habérseles generado colisiones, se aplican para garantizar que la copia forense de un dispositivo y su contenido sean totalmente íntegros y auténticos.

3. **Obtener**: Se refiere a obtener resultados a través de la búsqueda, restauración, localización y extracción de archivos o registros que pueden formar parte de la evidencia digital, sin dejar por un lado la interpretación de los resultados. En esta etapa es necesario aplicar distintos programas, métodos y la suspicacia del analista para la búsqueda e interpretación de los registros digitales a analizar, por ejemplo: la cantidad de usuarios activos en la computadora, la línea de tiempo del último inicio y cierre de sesión, bases de datos del sistema operativo, historial de navegación de internet, contenedores de correos electrónicos, entre otros.

4. **Presentar**: Es la etapa en donde se plasma en un informe técnico o ejecutivo, el resultado de los análisis realizados y que serán puestos a la vista de los interesados, y en muchas oportunidades a la vista de un juez cuando se judicialice el proceso.

En estas cuatro etapas se resumen todas las actividades a realizar por parte de los expertos en esta disciplina, quienes deben de tener conocimientos sobre sistemas operativos, sistemas de archivos, dispositivos móviles, técnicas de adquisición, técnicas de preservación, tener conocimientos en distintos programas forenses y estar plenamente conscientes de que los resultados obtenidos en muchas ocasiones tendrán que defenderse en un tribunal de justicia.

A pesar que existan marcos de trabajo como el de defensa en profundidad, existe la probabilidad de que ocurra un hecho que se deba investigar, por lo que siempre es importante la disciplina de la informática forense que permita reconstruir archivos, obtener líneas de tiempo, analizar registros, identificar el origen de posibles ataques dirigidos hacia sistemas informáticos, identificar daños causados a los activos de información, interpretar resultados y presentarlos como evidencia digital, para la aplicación de contramedidas de seguridad o para proponer como prueba en un proceso judicial.

Conclusiones

La ciberseguridad permite la prevención, mitigación y detección de posibles ataques informáticos, mientras que la informática forense, se encarga de investigar las causas del ataque, responder ¿cómo sucedió?, ¿cuáles fueron los activos informáticos vulnerados y comprometidos?, ¿cuáles fueron las causas?, ¿quién y cómo se ejecutó la vulnerabilidad?, ¿qué información fue vulnerada? y proponer contramedidas para evitar que se repitan dichas acciones.

La informática forense como parte de un proceso integral del marco de trabajo de defensa en profundidad, cumple una función vital en la ciberseguridad, aportando pruebas informáticas en procesos judiciales o proponiendo posibles mejoras y soluciones para mitigar riesgos latentes.

Referencias bibliográficas

AVAST. (2020). Avast. Obtenido de https://www.avast.com/es-us/business/resources/defense-in-depth

Ciberseguridad en Linea. (28 de 04 de 2020). Defensa en Profundidad Video. Obtenido de https://www.youtube.com/watch?v=VaRXah6KTTA&t=173s

CISCO. (s.f.). CISCO. Obtenido de https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

INCIBE. (29 de 12 de 2016). Inventario de activos y gestión de la seguridad en SCI. Obtenido de https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

INCIBE. (s.f.). Decálogo ciberseguridad empresas: Obtenido de https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_decalogo_ciberseguridad_metad.pdf

iniseg. (17 de 09 de 2019). INISEG. Obtenido de https://www.iniseg.es/blog/ciberseguridad/informatica-forense-digital/

Monzón, A. (2018). Curso de Introducción a la ciberseguridad, UMG Guatemala.

Ortíz, E. (2019). Evidencia Digital: Fundamentos aplicables para el abordaje de la Examinación. Research Gate, 10.

Rubio Alamillo, J. (28 de 05 de 2020). Perito Informático. Obtenido de https://peritoinformaticocolegiado.es/blog/diferencias-entre-la-respuesta-ante-incidentes-dfir-y-el-peritaje-informatico/

Semantic Scholar. (2017). Semantic Scholar.

VERIZON. (2020). Verizon. Obtenido de https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Wittkop, J. (09 de 02 de 2020). InteliSecure. Obtenido de https://www.intelisecure.com/what-is-data-protection/Peiró, J., & Soler, A. (5 de Mayo de 2020). EL IMPULSO AL TELETRABAJO DURANTE EL COVID-19 Y LOS RETOS QUE PLANTEA. Obtenido de https://www.ivie.es/wp-content/uploads/2020/05/11.Covid19IvieExpress.El-impulso-al-teletrabajo-durante-el-COVID-19-y-los-retos-que-plantea.pdf

Sobre el autor:

Ingeniero en Sistemas de Información y Ciencias de la Computación, M.A. en Seguridad Informática, Catedrático Universitario, Perito en Informática Forense, apasionado por el análisis Informático Forense, más de cuatro años de experiencia en el ámbito de la Informática Forense.

CyberSecurity
Información & Privacidad

Hardening como técnica de ciberdefensa a la infraestructura de red local

Assurance as a cyber defense technique to the local network infrastructure

Delia Merary Cristales Monterroso
email: dcristalesm@miumg.edu.gt

Recibido:25/noviembre/2020. Revisado: 4/enero/2021. Aprobado: 12/febrero/2021.
Disponible en internet el 1 de mayo de 2021

Resumen: Hardening es un término de seguridad informática que se utiliza para asegurar y fortalecer al máximo los sistemas de las tecnologías de información, mediante la aplicación de técnicas de ciberdefensa, a fin de mitigar o reducir la explotación de amenazas y vulnerabilidades que pueden ser provocadas por una falta de control. Por lo que es imprescindible que el equipo de seguridad comprenda los vectores de ataque para afrontar las amenazas a las que están expuestas las empresas. El hardening busca reducir la brecha de seguridad y el alcance de un ataque, en caso contrario podría desencadenar un ataque cibernético y en consecuencia provocar impactos económicos, reputacionales, contractuales etc., y entre los ataques más comunes por ejemplo el ransomware, phishing, denegación de servicios, exposición de datos etc.

Para la realización de este estudio se utilizaron diferentes estándares y marcos para procedimientos de hardening tanto en directrices de cumplimiento para certificación como en términos de configuraciones seguras, alineados en las buenas y mejores prácticas de configuración que ofrecen los estándares de seguridad internacionales como NIST, PCI - DSS, CIS control, ISO 27001, aplicando seguridad en todas sus capas a nivel de software , hardware, a nivel de usuario (aplicando el principio de menor privilegio), y que permitan fortalecer los mecanismos de defensa existentes a fin de eliminar cualquier posible explotación de vulnerabilidades en la red.

Palabras Claves: Hardening, ciberseguridad, ciberdefensa, NIST, CIS Controles, ISO 27001, PCI-DSS, vulnerabilidades, tecnologías de información.

Abstract: Hardening is a computer security term that is used to secure and strengthen information technology systems to the maximum, through the application of cyber defense techniques, in order to mitigate or reduce the exploitation of threats and vulnerabilities that can be caused by a lack of control. Therefore, it is essential that the security team understand the attack vectors to face the threats to which companies are exposed. Hardening seeks to reduce the security gap and the scope of an attack, otherwise it could trigger a cyber attack and consequently cause economic, reputational, contractual impacts, etc., and among the most common attacks such as ransomware, phishing, denial. services, data exposure etc.

To carry out this study, different standards and frameworks for hardening procedures were used both in compliance guidelines for certification and in terms of secure configurations, aligned with the good and best configuration practices offered by international security standards such as NIST, PCI -DSS, CIS control, ISO 27001, applying security in all its layers

at the level of software, hardware, at the user level (applying the principle of least privilege), and that allow to strengthen the existing defense mechanisms in order to eliminate any possible exploitation of vulnerabilities in the network.

Desarrollo:

La presente investigación se refiere al tema de hardening (que significa endurecer) la infraestructura de red local tanto a nivel físico como lógico como medida de protección ante ciberataques. Este consiste en asegurar los sistemas de TI antes que sean puestos en producción, mitigando vulnerabilidades potenciales, y que permita minimizar el impacto, mediante el uso de técnicas de endurecimiento a nivel de servicios red mediante la implementación y configuración segura de un firewall perimetral con capacidad de detección y prevención de intrusos, el monitoreo del tráfico de la red, el uso de protocolos que cifren las comunicaciones, segmentación física y lógica de la red, renovación de equipos que estén fuera de su vida útil (obsoletos), actualización de software, gestión de parches de seguridad, remediación de vulnerabilidades, deshabilitar servicios y puertos que no son necesarios y que de lo contrario permitan el intercambio de archivos, etc., así mismo aplicar controles restrictivos en la configuración y gestión de privilegios de usuarios tanto físico como lógico y que solo personas autorizadas puedan tener acceso a la información en función a sus responsabilidades.

Principalmente el hardening es una técnica de ciberdefensa, se constituye en los sistemas informáticos y la continuidad del negocio para evitar que sean interrumpidos por un ciberataque afectando la disponibilidad, integridad y confidencialidad de la información que podrían destruir, alterar o apropiarse de la información y que ésta es considerada uno de los activos más valioso de las empresas, por lo cual se debe proteger y clasificar de acuerdo con su nivel de criticidad. Por lo tanto el propósito de este estudio es dar a conocer este tema tan relevante y brindar recomendaciones para el fortalecimiento de toda la infraestructura de red, mediante la adopción de buenas y mejores prácticas que promueven las normas y estándares de seguridad como NIST, PCI-DSS, CIS controles etc.

Este articulo tiene como objetivo fomentar a que organizaciones implementen técnicas de hardening como parte de una estrategia de ciberdefensa para fortalecer toda su infraestructura de red, como medida de protección y prevención ante ciber ataques. Así mismo dar a conocer que existen estándares de seguridad que promueven la aplicación del endurecimiento a los sistemas de las tecnologías de información no solo como mejores prácticas sino en términos de cumplimiento para certificación PCI-DSS, que vela por corregir vulnerabilidades existentes, principalmente para proteger el robo o pérdida de información sensible de las organizaciones, asimismo brindar recomendaciones y procedimientos para el aseguramiento de la red a fin de reducir la superficie de ataques cibernéticos.

Materiales y Métodos.

Para la realización de este estudio se utilizaron diferentes referencias en documentos de estándares y normas internacionales distinguidas y muy utilizadas en la actualidad en términos de adopción de buenas prácticas como en certificación de cumplimiento.

Se tomaron de referencia las publicaciones de NIST SP 800-53 (2020) revisión 5, sobre Controles de seguridad y privacidad para organizaciones y sistemas de información, los CIS controles basada en las mejores prácticas de seguridad, así como los requisitos y procedimientos para el cumplimiento del estándar PCI – DSS (2018), considerando también los procedimientos para el endurecimiento a los sistemas de la norma ISO 27001 (2018).

Se les dio más importancia a los procedimientos de las publicaciones de NIST SP 800-53 dado que por ser una metodología completa, robusta y muy reconocida a nivel mundial, los CIS controles, el estándar PCI – DSS que es bastante estricto y que promueve la ciberseguridad basándose en el endurecimiento de los sistemas en todo el perímetro en un alto nivel para la protección de datos, adhiriendo directrices de cumplimiento y listas de verificación para su certificación.

Resultados

Se eligieron 4 documentos basados en publicaciones de estándares y normas internacionales.

Estándares y Normas	Cantidad de documentos	Porcentaje
NIST SP 800-53	1	25%
CIS Control	1	25%
PCI – DSS	1	25%
ISO 27001	1	25%
Total	4	100%

Tabla 1: Cantidad de documentos basados en estándares y normas Fuente: Elaboración propia

El porcentaje de los documentos seleccionados de los últimos 3 años, se distribuyeron de la siguiente manera: los documentos publicados en 2018 representan un 25%, documentos publicados en 2019 representa un 25% y documentos del 2020 presenta un 50%, por lo que respecta en todos sus aportes al tema de hardening.

Año de publicación	Cantidad de documentos	Porcentaje
2018	1	25%
2019	1	25%
2020	2	50%
Total	4	100%

Tabla 2: Cantidad de documentos por fecha de publicación. Fuente: Elaboración propia.

El análisis en estos documentos se contemplan todas las medidas necesarias y adecuadas al configurar y administrar los recursos de TI, para garantizar la disponibilidad, integridad y confidencialidad de la información.

Basados en los procedimientos y controles que ofrecen estos estándares, que abordan el endurecimiento a los sistemas, como un procedimiento de seguridad donde habilitar opciones de configuración es esencial para la seguridad por ejemplo, las cuentas predeterminadas deben cambiar de nombre o deshabilitarse, junto con cualquier funcionalidad predeterminada innecesaria, como los servicios del sistema que no se utilizan, y recomiendan cambiar configuraciones predeterminadas, que cada una de las cuales reduce la superficie de un intento ataque o la oportunidad de compromiso proporcionando instrucciones paso a paso para endurecer todos los sistemas.

NIST, CIS controles, ISO 27002 buscan un enfoque holístico para implementar, documentar y ajustar en un modo restrictivo todos los permisos, establecer configuraciones seguras de las tecnologías de información en los parámetros de configuración que se pueden cambiar en el hardware software o componentes de firmware y/o de sistema que afecten la postura de seguridad y privacidad o funcionalidad del sistema, la configuración del registro; a fin de aplicar estos controles para salvaguardar la información que se encuentra procesando, en tránsito o en reposo. Sin embargo en las tecnologías de la información la única constante es el cambio, es decir las nuevas aplicaciones, las actualizaciones de firmware, de sistema operativo, el hardware, y los nuevos usuarios hacen que el cambio sea inevitable y por eso la necesidad realizar auditorías, escaneos y remediar todas aquellas vulnerabilidades altas y críticas para maximizar la protección contra ciberataques.

Y para ello se describen algunos pasos para fortalecer los sistemas de las tecnologías de información en las diferentes capas.

- El hardening a nivel de la capa del perímetro de las tecnologías mediante la implementación firewall, servidores proxy así como la creación de reglas ACL´s seguras (White List), habilitar el modo stateful en el firewall a fin de monitorear los paquetes, conexiones activas y comprobar si estas con válidas, y a su vez ofrece mejorar la postura de ciberseguridad para

las redes al registrar al registrar información de la sesión como números de puerto o direcciones IP etc.

- El hardening a nivel de capa de servicio de red tales como segmentaciones de red tanto física como lógica y la aplicación del filtrado de paquetes entre VLAN ´s para garantizar que solo los sistemas autorizados puedan comunicarse, el uso de puertos que cifren las comunicaciones por ejemplo ssh y habilitar explícitamente los necesarios.

- El hardening a nivel de la capa del host aplicadas a las estaciones de trabajo mediante la aplicación de GPO´s, mantener al día las actualizaciones de SO, la remediación de vulnerabilidades, instalación de antivirus y garantizar que este se actualice, eliminar programas innecesarios y evitar instalación de aplicaciones no autorizadas.

A continuación se describe una tabla sobre las principales amenazas a las que están expuestos los activos críticos de las organizaciones y la solución a aplicarse.

Activo Afectado	Amenaza	Vulnerabilidad	Solución
Servidores	Sniffer	Transmisión no cifrada de datos críticos.	Cifrar las comunicaciones mediante uso de protocolos seguros
Servidores	Acceso no autorizado	Mal manejo de contraseñas (compartidas, inseguras o contraseñas por defecto)	Contraseñas robustas
Servidores	Bugs del sistema/configuración	Falta de actualización del SO o la versión es antigua y toca instalar una Nueva	Mantener sistemas actualizados y aplicar parches de seguridad
Servidores	Ejecución de código Arbitrario	Servidores sin aplicaciones de seguridad / Actualización de OS	Remediación de vulnerabilidades
Equipos de red	Ataque de fuerza bruta	Mal manejo de contraseñas (compartidas, inseguras o contraseñas por defecto)	Cambiar contraseñas por defecto, uso de contraseñas robustas y cifrarlas
Servidores	Denegación de servicios	Ataque al servidor y/o Mal dimensionamiento en los recursos	Monitoreo de recursos y definir umbrales de conexión
Servidores	Desbordamiento de buffer	Existen puertos asociados a servicios que no deben de estar a	Deshabilitar puertos y servicios innecesarios

		disposición de la red informática	
Servidores	Fallas en el hardware	Falta de mantenimiento en equipos Red que tienen más de 4 años de funcionamiento	Actualización de hardware
Host	Difusión de software no autorizado/sin licenciamiento	No se cuenta con política/herramienta que controle la instalación de software legítimo.	Eliminar programas innecesarios y evitar

Tabla 3: Tabla de amenazas y vulnerabilidades Fuente: Elaboración propia

Discusiones

Dado los diferentes estándares y marcos que se tomaron de referencia hay una correlación entre los controles y funciones de seguridad que aborda NIST CSF basados en las buenas prácticas de otros frameworks como los controles de CIS, la familia de controles de seguridad de NIST SP 800-53 y los controles que ofrece ISO 27002, no solo enfocados a la parte de certificación sino en la aplicación de técnicas hardening como buenas y mejores prácticas de tal manera que formen parte de una estrategia de ciberdefensa eficaz contra los ataques cibernéticos más comunes como lo son: phishing, ransomware, denegación de servicios, exposición de datos etc.

Algunas veces los cibercriminales no deben emplear técnicas sofisticadas para vulnerar sus redes derivado que sus niveles en términos de ciberseguridad son muy pobres. Asimismo, el aseguramiento de los sistemas en las tecnologías de información no son parte solo del departamento de TI, sino parte de todos los miembros de la organización en términos de ciberseguridad, y este procedimiento debe emplearse como un proceso cíclico de mejora continua.

Realizar una inversión económica para blindar la infraestructura de red, ya que “La ciberseguridad nunca tiene un costo mayor al daño que podemos sufrir por no hacer nada al respecto” (2020) Obtenido en: https://www.myideal-it.com/es/seguridad-y-privacidad/la-ciberseguridad-nunca-tiene-un- coste-mayor-que-el-dano-que-podemos-sufrir.

Muchas empresas incluso se dan a la tarea de redactar y aprobar de una política de hardening, mas no velan por el cumplimiento de esta, y esto debe ser en conjunto con auditorías internas para verificar que ha sido establecida y luego realizar un test de penetración para medir la efectividad de esta a fin de minimizar la probabilidad ocurrencia de las amenazas y la posible explotación de vulnerabilidades. Esta frase bastante oportuna para el estudio “Lo que no se define no se puede medir.

Lo que no se mide no se puede mejorar. Lo que no se mejora, se degrada siempre". (William Thomson Kelvin, Físico y Matemático 1824-1907).

En ausencia de legislación en términos de delitos cibernéticos en nuestro país, es importante que las empresas puedan implementar el hardening como un beneficio en la gestión de riesgos de TI.

Conclusiones

Luego de realizar el estudio se puede concluir que implementar cualquier estándar o marco de ciberseguridad en las organizaciones ayudará a fortalecer las infraestructuras críticas de las organizaciones, principalmente porque estos marcos abordan el tema de hardening como beneficio para mejorar sus niveles de ciberseguridad, mediante la adopción de controles, procedimientos que ayuden a disminuir la superficie de un ataque cibernético, cabe destacar que las tendencias de actividad maliciosa se enfocan en la exposición de datos de las empresas y para ello usan técnicas de ofuscación sofisticadas para lograr un ataque exitoso, pero viendo las amenazas como una oportunidad de mejora nace la necesidad de aplicar medidas de prevención y protección para salvaguardar los sistemas informáticos, a fin de cumplir los objetivos estratégicos de las organizaciones, ya que muchos de los procesos de negocio son dependiente de las tecnologías de información.

El beneficio que el lector obtiene el leer este articulo principalmente es poder llevar a cabo estos procedimientos a fin de conocer la postura actual de ciberseguridad que tienen en sus organizaciones y el conocer que existen varios frameworks de certificación en términos de ciberseguridad y de cumplimiento que promueven el uso de estas técnicas de ciberdefensa para mitigar amenazas y vulnerabilidades. Cabe recalcar que existen soluciones para reconocer el comportamiento que los atacantes usan para vulnerar redes, como por ejemplo IDS/IPS para detectar ataques inusuales y bloquear el tráfico de red malicioso en cada uno de los límites de la red de las organizaciones.

Recomendaciones

Se recomienda que para cualquier equipo informático antes de ser colocado en un ambiente de producción deba realizarse el procedimiento hardening establecido como parte de los controles internos de cada organización, donde se contempla el escaneo de vulnerabilidades de acuerdo con su funcionalidad y tipo de activo informático, y la respectiva remediación de todas aquellas vulnerabilidades altas y críticas, mediante la aplicación de hotfix, parches de seguridad.

Realizar un análisis de riesgo para determinar las amenazas y vulnerabilidades asociadas a los activos de información y aplicar las soluciones necesarias y medir la efectividad de tal manera que el riesgo residual sea tolerable a fin de evitar que se materialice una amenaza.

Documentar todas las modificaciones en los equipos informáticos por ejemplo (una nueva regla en el firewall, actualización de OS, firmware, aplicación de parches, permisos, etc.) esto con el objetivo de llevar un control de cambios entorno a la seguridad, y que haya una revisión oportuna de estas modificaciones para evitar dejar un agujero de seguridad que posteriormente pueda explotarse.

Referencias bibliográficas

CIS – Controles (2019) Controles de Seguridad y privacidad en TI para organizaciones V7.1 Obtenido en: https://www.cisecurity.org/controls/

Estándar PCI-DSS (2018) Normas de seguridad de datos - Requisitos y procedimientos de evaluación de seguridad V 3.2.1 Obtenido en: https://www.pcisecuritystandards.org/

Nist SP 800 - 53 (2020) Controles de seguridad y privacidad para Organizaciones y sistemas de información Obtenido en: https://csrc.nist.gov/publications/detail/sp/800- 53/rev-5/final

Joshua M. Franklin (2020) Relación entre controles CIS e ISO 27001 Obtenido en: https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/.

Sobre la autora:

Ingeniera en Sistemas de información y máster en seguridad informática egresada de la Universidad Mariano Gálvez de Guatemala, con más de 6 años de experiencia en diferentes áreas de TI para Atento de Guatemala, principalmente en implementación de soluciones de infraestructura tecnológica, servidores Windows y distribuciones Linux, telecomunicaciones, escaneo y remediación de vulnerabilidades para tema de certificación.

CyberSecurity
Información & Privacidad

Informe de transformación digital, caso de estudio: Ingenio azucarero en Guatemala.

Digital transformation report, case study: Sugar mill in Guatemala.

Pablo Benavente Chacón
email: pbenaventec@miumg.edu.gt
Recibido:25/noviembre/2020. Revisado: 10/febrero/2021. Aprobado: 3/marzo/2021.
Disponible en internet el 1 de mayo de 2021

Resumen: El 85% de los líderes de organizaciones de diferentes tipos de industrias en Estados Unidos consideran que en un plazo no mayor de dos años deberán realizar importantes inversiones en la transformación digital de sus empresas, esto para reducir la brecha con sus competidores o buscar mejores indicadores financieros para su estabilidad. El sector de la agroindustria no es ajeno a esta realidad, los procesos deben transformarse para ser más ágiles y eficientes. El objetivo de este estudio fue realizar un recorrido por ese proceso de transformación de un ingenio azucarero en Guatemala, desde la definición de la estrategia, la medición del conocimiento y la aceptación de los empleados para determinar un nivel de madurez digital y las probabilidades de éxito del proyecto. Con el objetivo trazado se utilizaron dos metodologías para medir el grado de madurez de transformación a un nivel cuantitativo derivado de un arquetipo que evalúa, estrategia, talento humano, canales digitales y tecnología. Para la medición cualitativa se aplicó un instrumento a empleados del ingenio para identificar un grado de compromiso con el proyecto y una percepción cualitativa de la situación.

Los resultados de ambas evaluaciones dieron cuenta de que el proceso tiene evidentes oportunidades de mejora. Se refleja una brecha considerable entre el desarrollo de canales y la tecnología ya implementada en el ingenio y la gestión de cultura y talento, sobre todo en los procesos de comunicación en todos los niveles del personal. El nivel de madurez se posicionó en un grupo denominado migrante digital y la aceptación en general por parte de los empleados está por encima del 30%. En conclusión, las oportunidades de mejora se centran en los niveles de cultura y talento, la percepción de que el proyecto puede generar una inestabilidad laboral es un temor evidente en gran parte de los empleados, reflejando que los empleados con más años de laborar son más celosos de compartir información que puedan ayudar a establecer mecanismos uniformes en el desarrollo de las actividades. Se determinó que el nivel avanzado de digitalización no es suficiente para una transformación como tal, pero sí que es una infraestructura tecnológica adecuada, capaz de soportar los cambios trazados en la estrategia y que la alineación de las otras dimensiones de transformación en los 4 años que quedan para la finalización del proyecto se puede alcanzar.

Palabras Claves: Agroindustria, Madurez digital, digitalización, automatización de procesos, innovación tecnológica.

Abstract: Approximately 85% of the leaders of different types of industry organizations in the United States consider that in an estimated period of two years they will have to make significant investments in the digital transformation of their companies, this to reduce the gap with their competitors or seek better indicators financial for its stability. The agroindustry sector is not alien to this reality, the processes must be changed to become more agile and efficient. The objective of this study was to review the changes into the digital transformation of one of the sugar mills in Guatemala, from the definition of the strategy, the measurement of knowledge and the acceptance of the employees to determine a level of digital maturity and the probability of success of the project. With the objective outlined, two methodologies were used to determine the level of maturity of the changes in quantitative range derived from an archetype that measures strategy, human talent, digital channels and technology. For qualitative measurement, an instrument was applied to mill employees to identify a degree of commitment to the project and a qualitative perception of the situation. The results of both evaluations showed that the process has clear opportunities for improvement.

A considerable gap is reflected between the development of channels and the technology already implemented in ingenuity and culture and talent management, especially in communication processes at all levels of personnel. The level of maturity was positioned in a group called digital migrant and general acceptance by employees is above 30%. In conclusion, the opportunities for improvement are focused on the levels of culture and talent, the perception that the project can generate job instability is an evident fear in a large part of the employees, reflecting that the employees with more years of work are more eager to share information that can help establish uniform mechanisms in the development of activities. It was determined that the advanced level of digitization is not enough for a transformation as such, but it is an adequate technological infrastructure, capable of supporting the changes outlined in the strategy and that the alignment of the other dimensions of transformation in the 4 years remaining for the completion of the project can be achieved.

Desarrollo:

El presente artículo es una reseña sobre la evaluación y seguimiento a una empresa con más de 60 años de funcionamiento en la industria azucarera, que se ha propuesto un plan de cinco años para la transformación digital. Entre los aspectos a desarrollar se consideró la necesidad de conocer el estado actual del uso de la tecnología en el ingenio azucarero y la forma en que el proyecto ha sido gestionado de manera que el talento humano sea parte fundamental en el proyecto y sea un crecimiento paralelo entre lo digital y los procesos.

Resulta relevante el análisis dado que el sector azucarero en Guatemala con sus exportaciones representa alrededor del 4% del PIB y en el año 2019 la producción tuvo un importante

crecimiento de 7.7%. Por esta razón, en los últimos años se ha incrementado la inversión en temas de tecnología, digitalización y optimización de los procesos involucrados implementando tecnologías que van desde internet de las cosas, drones, sensores hasta el análisis de big data.[1]

Por lo anterior es común que se confunda el uso de sistemas y algún tipo de automatización en el concepto de transformación digital, y aunque constantemente se encuentra este tipo de comparaciones la realidad es bastante diferente, una transformación digital implica que los sistemas ya existentes y las fuentes de datos previas, respondan a un solo almacén de información y esta sea la única fuente de toma de decisiones, sin procesos aislados y los manuales de procesos para cada una de las actividades relacionadas con el proceso productivo y administrativo de la empresa.

"La transformación digital es el proceso de cambio que una empresa ha de emprender para adaptarse al mundo digital, combinando la tecnología digital con sus conocimientos y algunos procesos tradicionales, para lograr diferenciarse y ser más eficiente, competitivo y rentable". (Cabezas, 2015). La transformación digital debe ir de la mano de una completa gestión de cambio, cambiar paradigmas y temores así el fortalecimiento del talento humano, sobre todo en culturas como la guatemalteca, en la que cualquier cambio grande implica una serie de temores injustificados. Para esto, indiscutiblemente debe haber una base tecnológica sólida pero además el personal involucrado debe ser "transformado" y estar comprometido en cambiar comportamientos y adquirir conocimientos, de manera que las actividades tradicionales que sigan vigentes después de la nueva definición de flujos y procedimientos administrativos puedan descansar sobre la infraestructura tecnológica y de manera conjunta alcanzar una exitosa optimización de procesos.[2]

El análisis se realizó con el interés profesional de conocer la situación actual del proyecto, segmentar las áreas del ingenio en las que la operación es más crítica de manera que en el inicio se puedan identificar puntos de mejora, así como determinar el nivel de madurez de la empresa y sus procedimientos de cara al proceso global de transformación digital.

Es por ello que el propósito del estudio es identificar y medir el grado de conocimiento de los empleados sobre el proceso de transformación digital en el ingenio, la gestión del cambio que se ha realizado para el proyecto, así como tener las métricas del desempeño de los empleados desde la definición de las etapas de la transformación digital y la definición clara de las tareas de los empleados, de manera que se puedan identificar puntos de mejora, el grado de madurez de transformación y el seguimiento de la comunicación del proyecto hasta el logro de las fases definidas en el alcance, sin que esto genere la percepción de inestabilidad laboral en la empresa.

Materiales y Métodos

Con la finalidad de cubrir los objetivos trazados en este estudio, se dividió en dos partes la metodología del mismo; por un lado, se recolectó información y datos de diferentes autores e instituciones en materia de transformación digital para tener una base contextual, llevando a cabo una recopilación y análisis de investigaciones académicas y empresariales extraídos de Google académico, y con ello priorizando de 1 a 10 una matriz para obtener datos relevantes del documento, como tipo de investigación, las fuentes importantes y su metodología de manera que permitiera obtener los datos más relevantes y así se evaluó la utilidad para la elaboración del artículo.

La segunda parte de la metodología se basó en la realización de una investigación descriptiva de manera empírica, cuyo mayor objetivo fue obtener un perfil cualitativo de la situación y su alcance fue desde la identificación de la muestra del objeto del estudio dentro del ingenio, la evaluación de un modelo de aplicación y madurez en transformación digital y el grado de aceptación del proyecto en el personal.

El proyecto de transformación digital en el ingenio se trazó para que se finalice en cinco años a partir del año 2020, en este proceso se priorizaron las áreas y empleados clave con funciones en los departamentos de: Campo, Laboratorio, Finanzas, Tecnología e Información, Recursos humanos y Tesorería del ingenio, por ser los departamentos en los que se genera más información, así como los elementos y flujos de mayor importancia en la cadena de valor de la producción de azúcar.

El instrumento fue aplicado a un total de 50 empleados, distribuidos de la siguiente manera:

Determinación de la muestra para aplicación del instrumento

Departamento	Cantidad	Masculino	Femenino
Campo	10	7	3
Laboratorio	10	5	5
Recursos Humanos	10	8	2
Finanzas	7	4	3
Tesorería	3	2	1
Tecnología de Información	10	10	0

Tabla 1: Elaboración propia.

Para la recolección de información se realizó una encuesta de 10 interrogantes y fue distribuida por medio de Microsoft Teams a las cuentas organizacionales de las personas identificadas en la muestra. El trabajo de campo se realizó con personal tanto en oficinas

centrales de Guatemala como en la planta en Masagua, Escuintla en el periodo comprendido entre septiembre a noviembre de 2020.

A partir de los datos obtenidos se procedió a realizar la respectiva etapa de análisis. Para esto, se hizo una descripción inicial de los hallazgos de forma general, posteriormente, se tabularon y procesaron cada una de las preguntas, realizando una agrupación tanto a nivel de procesos del ingenio y del proyecto de transformación digital. Para finalizar, con el objetivo de tener una mejor comprensión de los datos, los resultados fueron expresados gráficamente.

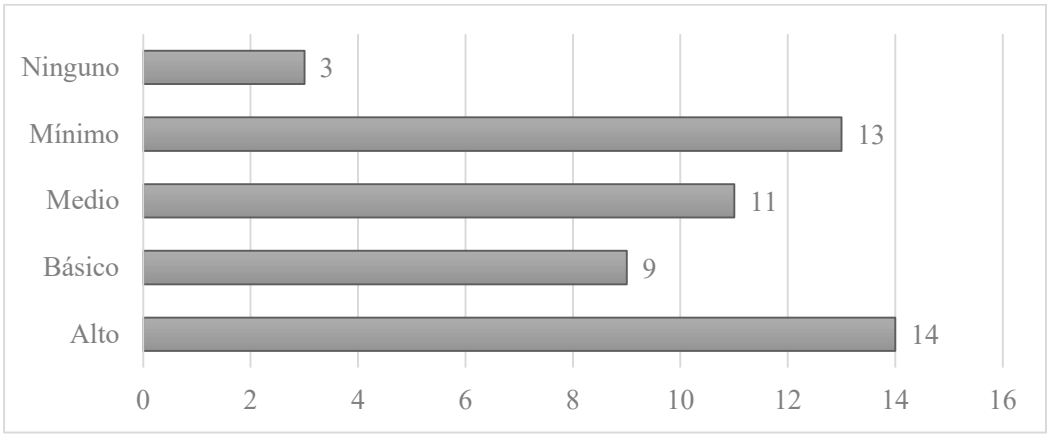


Ilustración 1. Elaboración propia

Importante información fue obtenida en cuanto a la cantidad de años que tiene un empleado de laborar en el ingenio, es inversamente proporcional al compromiso con la finalización del proyecto con éxito, además deja claro que también es visto como un riesgo para su estabilidad laboral dentro de la empresa.

El grado de compromiso se determinó interpretando las preguntas del instrumento en las que se consultó sobre si está dispuesto a brindar información muy particular que utiliza para realizar su trabajo, archivos independientes o fuera de los sistemas que le hacen tener un mejor control en sus actividades, compartir conocimiento y experiencias que no están en un proceso definido.

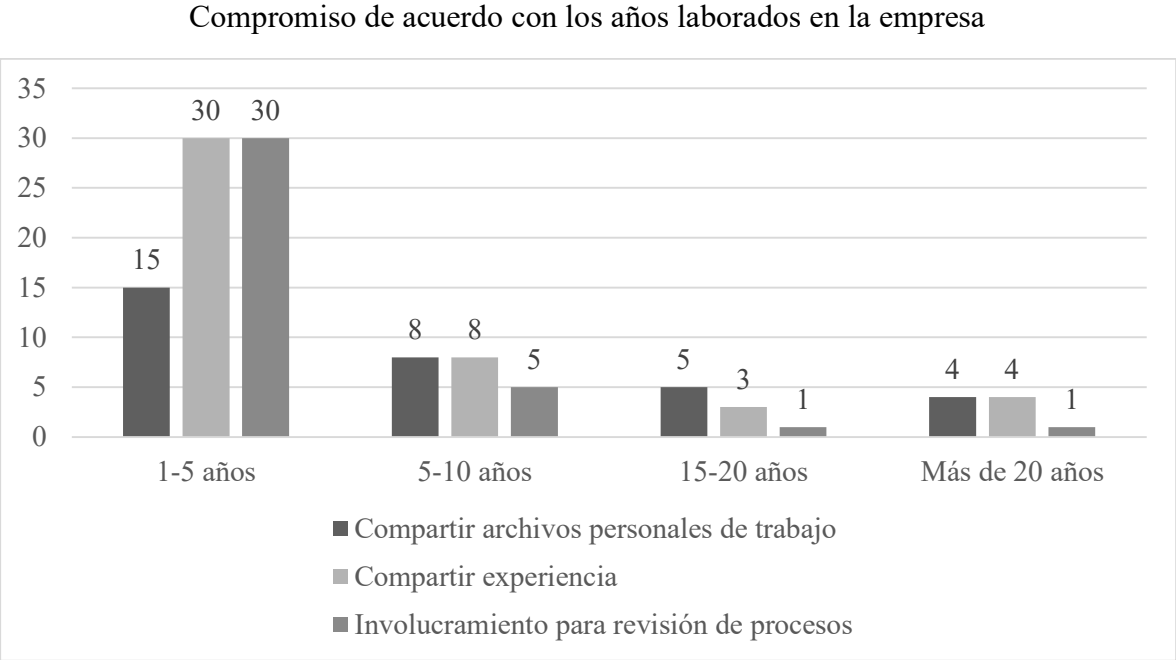


Ilustración 2. Elaboración propia

Resultados cuantitativos

Respecto a los grupos de madurez digital, podemos observar el puntaje obtenido en función de cada una de sus dimensiones, estos resultados se tabularon en la Tabla 1, tomando como base el modelo de madurez de 4 dimensiones (DUARTE A, 2020).[3]

Debido a que el ingenio ha iniciado con el proceso de transformación, las variables del grupo digital tienen un punteo bajo, los objetivos digitales y el conocimiento de los líderes digitales están plasmados en el plan del proyecto, por lo que se observa que son los únicos con punteo al respecto.

La dimensión de cultura y talento se ve con una madurez media, se cuenta con la apertura a nivel de líderes en los primeros elementos de ella, sin embargo existe mucha deficiencia en cuanto a comunicación a todos los niveles así como una pobre gestión del cambio de acuerdo a los resultados obtenidos.

En operación y tecnología se identificó el único punto alto en cuanto a la evaluación de dimensiones se refiere, esto es evidencia de los esfuerzos en cuanto a desarrollo,

automatización, seguridad de la información y el uso de mejores prácticas para la gestión de los servicios de TI.

Resultados de evaluación de nivel de madurez

	Digital	Migrante	Analógico	Total
Estrategia				
Estrategia digital	2.50	2.00	1.75	2.08
Objetivos digitales	3.00	2.50	1.75	2.42
Responsable de transformación	2.50	2.00	1.75	2.08
Adopción nuevas tecnologías	3.00	2.50	1.75	2.42
Cultura y talento				
Toma de decisiones	1.00	1.00	1.75	1.25
Metodologías ágiles	2.00	2.00	1.75	1.92
Tiempo para nuevos servicios	1.75	2.00	1.75	1.83
Líderes de cambio	2.00	2.50	1.75	2.08
Empleados frente a cambio	2.00	2.00	1.75	1.92
Gestión del cambio	2.00	2.00	1.75	1.92
Especialistas digitales	2.00	2.50	1.75	2.08
Desarrollo de habilidades	1.00	1.00	1.75	1.25
Canales digitales				
Medios web y móviles	3.00	2.50	1.75	2.42
Servicios por medios digitales	3.00	2.50	1.75	2.42
Redes sociales	3.00	2.50	1.75	2.42
Actualización de contenido	3.00	2.50	1.75	2.42
Medios de respuesta a los clientes	2.50	2.50	1.75	2.25
Operación y tecnología				
Automatización	2.00	2.50	1.75	2.08
Televisión	1.00	1.00	1.00	1.00
Servicio de telefonía	2.00	2.50	1.75	2.08
Seguridad de la información	2.00	2.50	1.75	2.08
Sistema de video vigilancia	2.00	2.50	1.75	2.08
Tecnologías digitales	2.00	2.50	1.75	2.08
Promedio Total				2.03

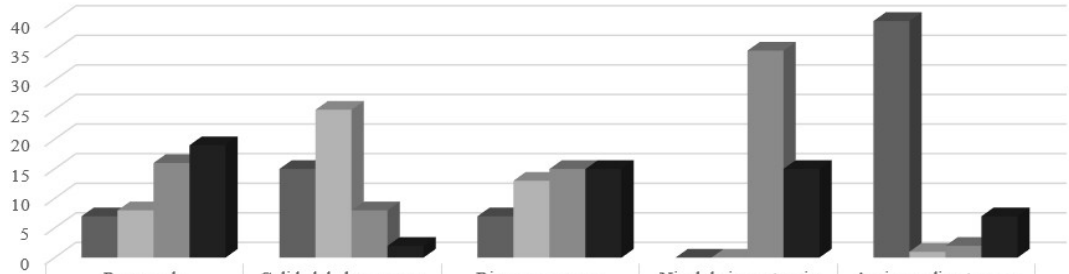
Tabla 2. Evaluación: elaboración propia

Resultados cualitativos

Los resultados enfocados en aspectos de medición a nivel de opinión y percepción de los involucrados directamente en el proyecto arrojaron el nivel de aceptación en un nivel medio, con un 30.4%.

Este dato se obtuvo sobre la evaluación de los hitos más importantes del proyecto, desde la definición de las etapas de la transformación digital, el trabajo en la definición de procesos por partes de la empresa consultora y el nivel de involucramiento e información en los que se han visto de alguna manera relacionados los empleados, desde sus inicios hasta la fase del primer año de iniciado.

Percepción de los empleados sobre el proyecto de transformación digital



	Proceso de comunicación desde la directiva a todas las áreas sobre el proyecto	Calidad de la empresa consultora para la definición de procesos	Riesgo que ve en perder su trabajo derivado de la transformación digital	Nivel de importancia que su trabajo tiene para el éxito del proyecto	Acciones directas que ha aportado al proyecto de transformación digital
Muy bajo	7	15	7	0	40
Bajo	8	25	13	0	1
Medio	16	8	15	35	2
Alto	19	2	15	15	7

Ilustración 3. Elaboración propia

Discusión

Un nivel de madurez da cuenta del estado en que se encuentra una empresa en función de un tipo de evaluación, de manera que la calificación esté basada en un conjunto de análisis que permitan ponderar de manera objetiva los aspectos evaluados y permita compararlos para concluir las condiciones de la situación actual en la empresa y a partir de ello tomar decisiones que permitan mantener la calidad en caso de un resultado positivo o de tomar medidas correctivas en pro de la búsqueda del alcance de los objetivos.

Indudablemente las condiciones de cada empresa de acuerdo con sus características de mercado, magnitud, giro, entre otras, requieren una evaluación adecuada, sin embargo, no

es un indicativo de que para cada caso se deba desarrollar un nivel de madurez completamente nuevo, se pueden utilizar arquetipos adecuados que hayan sido desarrollados con base en evaluaciones previas, al fin y al cabo la transformación digital y sus niveles tienen el mismo objetivo.

Para abordar el objetivo de identificar un nivel de madurez del proyecto de transformación digital, se tomaron en consideración varios métodos de evaluación, sin embargo, el modelo que permite ponderar de mejor forma en los resultados está basado en 4 dimensiones de evaluación: estrategia, cultura y talento, canales digitales y la operación y tecnología. Con las dimensiones identificadas se establecieron los métodos de ponderación de la siguiente manera:

Grupo	Puntaje	Estado de transformación
Digital	2.5-3.25	Significativo
Migrante Digital	1.75-2.50	Moderado
Analógico	1-1.75	Mínimo

Tabla 3. Fuente: (DUARTE A, 2020) (https://repositorio.unican.es/xmlui/bitstream/handle/10902/19076/DUARTELESMESANGELAMARCELA.pdf?sequence=1&isAllowed=y)

Estrategia

La dimensión de la estrategia determina si existe el compromiso y meta de llevar al ingenio a la transformación digital, permite brindar datos sobre la estrategia establecida, documentación sobre la misma y en este caso en particular posiciona al ingenio en el grupo de migrante digital con un 2.25 de ponderación. El encaminar los esfuerzos y recursos empresariales en un proyecto de esta magnitud debe realizarse siempre sobre la base de que la estrategia de transformación es la adecuada, por lo tanto, contar con un nivel de madurez superior al 1.75 es un indicativo de que el plan lo suficientemente adecuado para guiar a la organización en el proceso de cambio e implementación de la transformación, sobre todo porque en esta etapa se definieron los objetivos y alcances del proyecto así como la asignación de los recursos de inversión necesarios.

Cultura y talento

Se considera en la dimensión de cultura y talento una debilidad en el nivel de madurez, el puntaje obtenido de 1.78 en este rubro, posiciona esta área en un grupo muy cercano al analógico. Sin embargo, aún con lo preocupante del resultado obtenido, esta dimensión es más complicada de controlar, por el hecho de estar directamente relacionada con la cultura organizacional, en los aspectos de apertura de la dirección para involucrar a los empleados

en tomas de decisiones, uso de metodologías ágiles, estructura de liderazgo de cambio, y el desarrollo de las habilidades. [5]

Si evidentemente la transformación debe contar con una estructura tecnológica adecuada, este tipo de proyectos basan su éxito con la implicación de que el recurso humano tenga habilidades digitales para que pueda usar de la mejor manera las herramientas tecnológicas a su disposición. Sin embargo, el tema de habilidades tecnológicas en la cultura de América Latina ya ha sido objeto de estudio, debido a que se tiene la limitante del sector educación, es un problema real y que se hace más grande a medida que la tecnología avanza, pero las brechas de educación en territorios como el guatemalteco se mantienen.

Prueba de ellos son las estadísticas de graduados que en comparación con otros continentes son bastante inferiores, por ejemplo, en relación con graduados en alguna carrera de tipo científico en 2015, las ciencias sociales en América Latina representan el 54% (RICYT, 2015). Es decir que el tema digital es un problema aún cultural que requiere el compromiso a nivel de empresa para gestionar las habilidades desde los líderes generando un ambiente de aprendizaje, juntamente con la inversión, especialistas de automatización, científicos de datos, alianzas estratégicas con proveedores y expertos en seguridad informática.

Canales digitales

El puntaje de 2.38 obtenido para la dimensión de canales digitales es el reflejo de que es un buen momento para incluir a todo el ingenio en la transformación digital, las plataformas de intercomunicación, servicios Web y móviles, así como las redes sociales, son ahora una plataforma que se debe explotar sí o sí. En ese sentido el ingenio se coloca en el grupo de transformador digital con una tendencia a optimizar de mejor manera la comunicación con entidades reguladoras como ASAZGUA o clientes como EXPOGRANEL para la comunicación e intercambio de información que es importante para la toma de decisiones empresariales.

En evaluaciones de madurez para instituciones que se encaminan a la transformación digital, probablemente el tema de canales digitales sea el que se encuentra en mejores condiciones. Tal como se ha mencionado anteriormente es imprescindible una plataforma tecnológica que permita que todas las demás dimensiones se alineen de acuerdo con el plan para poder llegar a la transformación digital de la empresa. [4]

El ingenio no es ajeno a ello y la evaluación logró determinar que las áreas consideradas críticas para la operación, como campo, laboratorio, RRHH, finanzas y tesorería, cuentan con procesos definidos de trabajo con su respectivo sistema de software desarrollado a la medida, pero que módulo por módulo se están trasladando al ERP que permitirá tener un almacén de datos adecuado.

Operación y tecnología

La última dimensión que se evaluó en el modelo de madurez da cuenta de que es el segundo elemento con puntuación más baja, es la dimensión de operación y tecnología. Es relevante mencionar que los aspectos que hacen que el promedio de este rubro sea de 1.90 colocándolo apenas en el grupo de transformador digital, estén directamente relacionados con la seguridad informática. Los aspectos de automatización, sistemas de vigilancia, y tecnologías digitales están estrechamente relacionadas con la dimensión de canales digitales, por lo que han tenido un desarrollo adecuado con el crecimiento del ingenio. Caso contrario es el tema de la seguridad de la información, este aspecto importante aún sigue siendo visto como un mero costo a nivel de la operación pero que debe ser tomado en cuenta como uno de los pilares principales en el logro de la transformación digital.[6]

A medida que el proyecto de transformación se va acentuando, surge una cantidad considerable de activos de información a las que se debe conservar la integridad, disponibilidad y confidencialidad. Y es que en 2019 el gasto mundial en ciberseguridad superó los 124,000 millones de dólares con un incremento del 8.7% del 2018 (GARTNER, 2019), por lo que la seguridad de la información no es solo un requisito, es parte fundamental de las necesidades del negocio, ya que debe un pilar a considerar siempre de la cultura de la empresa, cuidar los activos no solo como responsabilidad de TI si no desde cualquier aspecto que pueda representar una vulnerabilidad o riesgo para la información.

Conclusión

En definitiva, el estudio de madurez en promedio de sus cuatro dimensiones entrega un 2.3 que coloca al ingenio dentro del grupo de migrante digital. Si se considera que el primer año del proceso de transformación está por concluir, cuando se han trazado 5 años, aún queda bastante por mejorar en los aspectos de cultura y talento, y las mejoras en tecnología.

El analizar de forma cualitativa algún aspecto de la organización puede representar un gran reto, sobre todo porque fácilmente se pueden caer en medidas y aspectos subjetivos. De aquí la importancia del arquetipo utilizado para poder aterrizar un modelo que brinde datos que permitan posicionar al ingenio en un grupo de acuerdo con los factores que fueron estudiados por dicho modelo.

Los resultados del estudio aplicado reflejan que el alcance del ingenio posee configuraciones que podrían colocarse de forma separada en niveles altos de digitalización, sin embargo, esto no puede traducirse como niveles de transformación digital, debido a que por el momento no hay una ruta marcada para la mera innovación. No obstante, es evidente el esfuerzo del ingenio en construir plataformas que posibilite la transformación digital y sobre esa línea se

deben alinear esfuerzos para que en corto plano mejorar las dimensiones de cultura y talento, estrategia y canales digitales.

La investigación refleja que tanto el nivel de conocimiento sobre el proyecto como la aceptación de este, en función de la calidad, más no de los objetivos, no es lo esperado por la directiva en este momento. Que los datos de la aceptación en parámetros de la importancia, calidad y desarrollo de la empresa, por parte de los empleados clave está en un punto medio y medio bajo.

Es evidente que no se ha comunicado de manera clara la importancia del proyecto más allá de la reunión de la salida en vivo del proyecto, por lo que no se ve un compromiso real de los involucrados, no se cuestiona los objetivos, en cualquier caso la implementación de la transformación digital es vista como algo que traerá mejoras a los procesos del ingenio, sin embargo, la manera en que se está realizando no es la adecuada, desde que, resultados interesantes de la investigación indican que la empresa consultora que apoya, hace uso de muy pocos estándares internacionales de procesos y los realizados hasta el momento no son de agrado y aceptación de las áreas involucradas.

Otro factor importante observado en los resultados es que, si está claro a nivel del ingenio que la labor de esta transformación no es exclusiva del departamento de TI, cuyo aporte en cuanto a tecnología y automatización es bien visto, los empleados coinciden en que todos estos recursos tecnológicos por sí solos no formarán una transformación completa si no se cambia la cultura y procesos actuales. En definitiva, la aceptación del proyecto y los objetivos de este tienen una aceptación alta, aunque el temor de la inestabilidad laboral se mantiene en un nivel considerable, sin embargo, la percepción general con el proyecto y la forma en que se está ejecutando es que no tiene la aceptación y compromiso esperados lo cual significa un riesgo alto para la finalización de este.

Referencias bibliográficas

[1] De los Ríos, E. (2017). Agrotransformación digital, 7 errores de aplicación. Obtenido noviembre 10, 2020, de https://www.linkedin.com/pulse/agro-transformaci%C3%B3n-digital-7-errores-de-aplicaci%C3%B3n-enrique/.

[2] Cuenca-Fontbona, J., Matilla, K. y Compte-Pujol, M. (2020). Transformación digital de los departamentos de relaciones públicas y comunicación de una muestra de empresas españolas. Obtenido noviembre 1, 2020, de https://www.researchgate.net/publication/339835087_Transformacion_digital_de_los_departamentos_de_relaciones_publicas_y_comunicacion_de_una_muestra_de_empresas_espanolas/.

[3] Duarte A. (2020). Transformación digital sector Hotelero de Santander. Obtenido octubre 28, 2020, de https://repositorio.unican.es/xmlui/bitstream/handle/10902/19076/DUARTELESMESANGELAMARCELA.pdf?sequence=1&isAllowed=y.

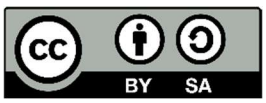
[4] Martínez J. (2016). LA TRANSFORMACIÓN DIGITAL Y SU REPERCUSIÓN EN LAS EMPRESAS. Obtenido octubre 20, 2020, de https://riunet.upv.es/bitstream/handle/10251/68911/MART%C3%8DNEZ%20-%20LA%20TRANSFORMACI%C3%93N%20DIGITAL%20Y%20SU%20REPERCUSI%C3%93N%20EN%20LAS%20EMPRESAS.pdf?sequence=7.

[5] Katz R. (2018). Capital humano parala transformación digital en América Latina. Obtenido noviembre 10, 2020, de https://www.cepal.org/es/publicaciones/43529-capital-humano-la-transformacion-digital-america-latina.

[6] Merchán T., Salazar A. (2018). PROPUESTA TECNOLÓGICA DE TRANSFORMACIÓN DIGITAL PARA CONVENIOS CON PROVEEDORES DEL AREA CATEGORIAS EMPRESA DIFARE S.A. Obtenido noviembre 10, 2020, de http://repositorio.ug.edu.ec/handle/redug/36898.

Sobre el autor:

Ingeniero en Sistemas de Información y Máster en Seguridad Informática en la Universidad Mariano Gálvez de Guatemala, con 13 años de experiencia en área de Tecnologías de Información en proyectos que incluyen los procesos de análisis, desarrollo e implementación de Sistemas de Información para las áreas de Finanzas y Cadena de Suministros. Conocimientos de consultoría e implementación de buenas prácticas para la gestión de servicios de tecnología como ITIL e ISO 20000. Actualmente, consultor y administrador en SAP Business One dentro de la organización que incluye actividades como: Consultoría Interna para SAP Business One para las organizaciones a través del análisis de soluciones y requerimientos que surgen como parte de los distintos procesos de negocio. Mantenimiento y soporte de SAP frente a actualizaciones de versiones, incidentes y nuevas funcionalidades y Administración principal de accesos y configuraciones dentro de SAP.



CyberSecurity
Información & Privacidad

La descomposición de la ciberseguridad, factores le que aportan valor

The decomposition of cybersecurity, factors that add value

Gumercindo Armando Monzón Escobar
Email: armandomon.zone@gmail.com

Recibido:1/noviembre/2020. Revisado: 15/enero/2021. Aprobado: 15/febrero/2020.
Disponible en internet el 1 de mayo de 2021

Resumen: Actualmente se habla acerca de la ciberseguridad desde su importancia, implementación, seguimiento, desarrollo, concienciación entre otros más, pero se olvida realmente el valor que ofrece y como es que esta debe de adaptarse desde nuestra vida privada hasta en la organización donde se labora, desde varios puntos de vista se ha tenido la idea equivocada de creer que el eslabón más débil de todo la plataforma tecnológica es solo el usuario final, esto porque no se toman de base otras variables que se deben de considerar para minimizar los riesgos dentro de la empresa, ya que si, el responsable de la seguridad de la información no tiene la visibilidad y madurez para ir minimizando riesgos internos como en el ciberespacio poca o nula será su reacción y respuesta ante estos.

Algunos estudios han podido mostrar información relevante acerca de lo que se piensa sobre la seguridad cibernética, pero no todos orientados a proponer un conocimiento científico para reproducirlo y aplicar métodos de la ciencia formal. El presente estudio nos lleva un poco más a comprender la ciberseguridad desde una descomposición de factores que aporten visibilidad sobre una gestión integral de la plataforma tecnológica.

Palabras Claves: ciberseguridad, método científico, procesamiento de la información, análisis, estadística.

Abstract: Currently they talk about cybersecurity from its importance, implementation, monitoring, development, awareness among others, but the value it offers is really forgotten and how it must adapt from our private life to the organization where it works, From various points of view, there has been the wrong idea of believing that the weakest link in the entire technological platform is only the end user, this because other variables that must be considered to minimize the risks within the company, since if the person in charge of information security does not have the visibility and maturity to minimize internal risks, such as in cyberspace, little or no reaction will be to them.

Some studies have been able to show relevant information about what is thought about cybersecurity, but not all of them aimed at proposing scientific knowledge to reproduce it and apply formal science methods. This study takes us a little more to understand cybersecurity from a decomposition of factors that provide visibility on an integral management of the technological platform.

Desarrollo:

El problema de estudiar algo que no se conoce totalmente podría darnos resultados parciales o equivocados sobre el tema que investigamos, en este caso la ciberseguridad debe de verse como un todo y descomponerse para realizar un análisis exacto de cada una de sus variables para segmentarla en fases y entenderla. Cuando se iniciaron con los estudios en El Teorema Inconcluso en el Proceso de la Seguridad de la Información (TIPSI) en el año 2017 se tenían algunas variables que podrían afectar los pilares que hasta ese momento se investigaban basados en la presentación del IX Congreso Iberoamericano de Seguridad Informática, SIIA: Sistema Integral de Inteligencia de Amenazas Aplicado al Cyber Dominio de Leobardo Hernández y Carlos Ayala expuesta en la Universidad Técnica de Ambato por la Dirección de Investigación y Desarrollo en Argentina, en esta se proponía una descomposición de la ciberseguridad de una manera generalizada, los factores estudiados fueron el internet, el perímetro, la red interna y el punto final.

Como parte de este estudio se pudieron identificar variables que podrían apoyarnos a determinar si nuestro conocimiento empírico sobre ciberseguridad podría dar algún valor, entonces escuche a alguien decir ¿conocimiento empírico en ciberseguridad? Si yo tengo muchas certificaciones técnicas o mi conocimiento sobre la gestión, mejora continua, riesgo, optimizaciones entre otros aspectos los manejo a la perfección y otros más que podríamos ir agregando, con todo esto el conocimiento técnico adquirido no debería de limitar nuestro conocimiento científico, porque al parecer es allí de donde proviene nuestro problema.

Como parte de los hallazgos presentados en el TIPSI se propuso aplicar matemática a los factores conocidos de la ciberseguridad como una nueva estrategia para conocer su importancia. Pero todo dependerá a quien le consultemos, es decir, al que gestiona el firewall lo más importante será su “firewall” (en español cortafuegos), sus servicios, su optimización y así más detalle de este, pasando por cada puesto disponible dentro de la organización que tenga relación con tecnologías.

Entonces nos hacemos la pregunta ¿qué es lo más importante para la empresa desde el punto de vista en ciberseguridad?, si nos basamos en metodologías la mayoría confirma que la ciberseguridad es quien debe de aportar factores para cumplir los objetivos de la empresa, pero si tomamos a la ciberseguridad como un rompecabezas nos damos cuenta de lo complejo del tema porque debemos de desmenuzar todo eso que nosotros llamamos ciberseguridad.

El Dr. Cristian Barria expuso magistralmente en el Primer Congreso de Investigación y Desarrollo en Tecnologías y Ciberseguridad de América Latina en el año 2021 sobre el tema de Amenazas en la Ciberseguridad logrando realizar una correlación de eventos a través del tiempo y la relación con la seguridad que conocemos hasta el momento, todo esto nos lleva a pensar que conforme conocemos más de ciberseguridad nos damos cuenta de que es necesario ir gestionando más aspectos del mismo.

La creación de un modelo de predicción no es más que la recolección de información para análisis y presentación de resultados, para ello, en el año 2018 luego del análisis de 50 empresas en Guatemala, se propuso la creación formal de La Evaluación Continua del Riesgo Informático –ECORI- y la Implementación de una Estrategia de Ciberseguridad, certificada en el Registro de la Propiedad Intelectual del Ministerio de Economía de Guatemala aprobada durante el año 2020.

El objetivo, conocer las cargas matemáticas de cada uno de los factores estudiados, a que me refiero con esto, conocer el valor de cada aspecto relacionado a la ciberseguridad, por ejemplo ¿alguien podría indicarme que es más valioso para una empresa, el backup o el antivirus? Tal como lo indicaba resultará prioritario para el administrador determinar, analizar y preocuparse de esta pregunta, que podría ser una de las muchas que podemos hacernos al hablar de ciberseguridad. La investigación conllevo muchas exposiciones para dar a conocer el modelo matemático base en el I Congreso de Cibersociedad de la Universidad de las Ciencias Informáticas UCI en la Habana Cuba a finales del año 2017, además en el OWASP Latam Tour 2018 del Capítulo Guatemala donde se presentó el "Sistema Integral de Inteligencia de Amenazas aplicado al Cyber dominio". En el mismo año se presentó como una clase magistral en el Posgrado de Seguridad Informática de la Universidad Mariano Gálvez donde se puedo validar el modelo en varias empresas. El modelo ECORI fue madurando ya que se pudo establecer que se encontraban más variables conforme se investigaba más de ciberseguridad, durante el año 2019 se presentó inicialmente en el ISACA DAY 2019 Capitulo Guatemala en el eje de Riesgos y Auditoria, además fue aprobada su publicación en el IEEE (Instituto de Ingeniería de Eléctricos y Electrónicos de Estados Unidos) con el nombre Management in the Continuous Assessment of Computer Risk, and Agile Project, y presentada en el IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX). Su desarrollo a constituido un nuevo enfoque para conocer el grado de madurez de las empresas.

Durante el ISACA DAY Edición Virtual del año 2020 se apoyó al capítulo Guatemala con la generación del I Reporte sobre el Estado de la Seguridad Latinoamérica, tecnologías, seguridad, riesgo y auditorias, en donde se aplicó el modelo para generar tendencias sobre la información recabada en su congreso, apoyando así las teorías de descomposición de la ciberseguridad.

Para tener una idea sobre este tema durante el año 2020 se presentó en el Congreso de la Secretaria Nacional de Ciencia y Tecnología CONVERCIENCIA 2020, el tema "La seguridad de la información en época del Covid-19" donde se propuso un árbol del problema que puede ayudar a determinar precisamente hacia donde se enfoca la ciberseguridad. Aunque se podría pensar que es un tema aislado lo importante en esta imagen es determinar las causas de nivel 1 y 2 del modelo desarrollado para su explicación

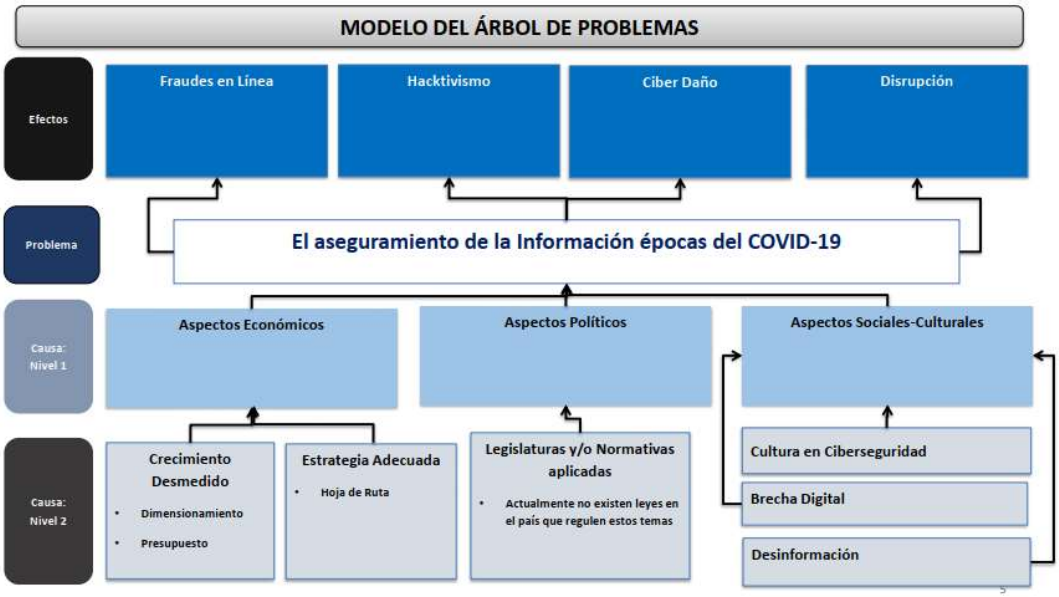


Figura 1. Modelo de Árbol de Problema. Fuente: Elaboración propia.

Basados en lo anterior, tomamos de base cuales podrían ser las causas que se están investigando para luego medir sus efectos, por ejemplo, si deseamos minimizar el ciber daño que está afectando a nuestra organización, alguien podría pensar enfoquémonos adquiriendo nueva tecnología para gestionar este riesgo, el punto de vista es válido porque técnicamente es importante, pero ¿estamos tomando los aspectos relevantes para minimizar y controlar este riesgo? Es decir, ¿hemos pensado si el efecto es un daño cibernético, económico, físico, político, psicológico y/o emocional o daños reputacionales que afectan a la empresa y más que eso si este es simultaneo, en cascada o latente? Ya que en esa línea debería de ir la implementación de la nueva tecnología, políticas, procesos y/o procedimientos que deseamos adquirir o mejorar dentro de la organización.

Desarrollo

Hablar de ciberseguridad se ha vuelto algo común en nuestra vida cotidiana y vemos como más profesionales adoptan las buenas prácticas a su conocimiento, desde la utilización de metodologías para un desarrollo seguro, proyectos agiles en ciberseguridad y sumado a esto las metodologías formales o informales que nos brindan visibilidad sobre los riesgos tecnológicos dentro de la organización, la inclusión de otras áreas que han agregado esta nueva capa a sus actuales procesos, como la medicina, la auditoria, infraestructuras críticas y otras más.

Vemos que algunos investigadores han propuesto una tabla periódica de ciberseguridad donde se propone una descomposición basada en: Seguridad IoT/IIoT, Seguridad de Red y Punto Final, Inteligencia de amenazas, Seguridad Móvil, Detección Perimetral, Seguridad en la Nube, Seguridad del Engaño, Visibilidad continua de la red, encriptación cuántica, remediación de riesgos, seguridad de sitios web, investigación continua de la ciberseguridad y algunas otras que son de importancia para la ciberseguridad, tal como lo muestra la imagen solo se recomiendan marcas de fabricantes para lograr una adopción de tecnologías según la escena global de ciberseguridad para minimizar los riesgos, mas no así, las cargas factoriales para entender lo que se proponía al inicio de este artículo.

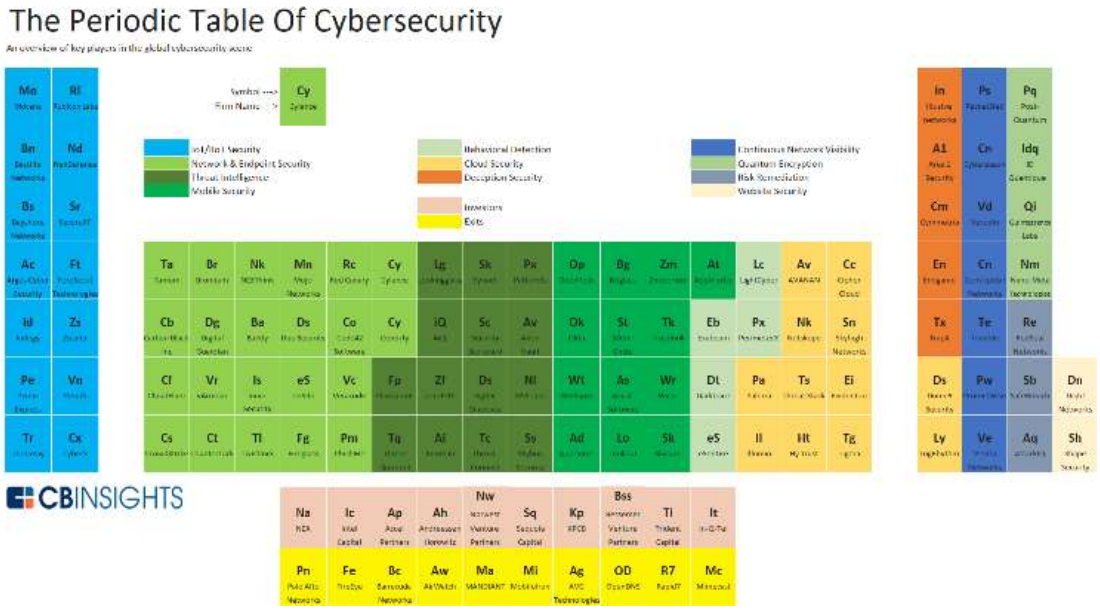


Figura 2. Tabla Periódica de Ciberseguridad. Fuente: CBInsights.

Quizá el aspecto más importante no es conocer el tipo de tecnología sino más bien su importancia dentro de la empresa, porque el gobierno de la seguridad de la información pone énfasis en la cultura organizacional y en los procesos, métodos, herramientas y técnicas de seguridad que constituyen todos ellos la estrategia de seguridad.

Otro tema fundamental en esta descomposición es saber que la convergencia de la información como criterio también propone que se tomen en cuenta a las personas, los procesos, la información y las tecnologías, todas ellas incluidas dentro del modelo matemático para lograr una ecuación que sea la suma de todas las variables posibles para lograr exactitud en este modelo.

Ahora bien, un ejemplo real para conocer las cargas factoriales de las variables analizas podrá mostrarnos lo siguiente:

		Componente			
		1	2	3	4
1	Disponibilidad de los Servicios	.086	.211	-.188	-.128
2	Acuerdo de niveles de Servicio	.363	.553	-.141	.055
3	Redundancia de Enlaces	.023	.400	.017	-.094
4	Preparacion de la Proteccion	.265	.214	.321	.127
5	Respuesta y deteccion de amenazas	.371	-.004	.069	.020
6	Bitácoras de eventos	.078	.658	-.048	.192
7	Firewalls de equipo final	-.071	.770	.172	-.015
8	Acceso a puestos de trabajo	.161	.768	.265	.282
9	Configuración de dispositivos	.290	.690	-.029	.387
10	Contratos disponibles	-.093	.659	.109	.217
11	Acuerdos de Confidencialidad	.034	.740	-.180	-.058
12	Monitoreo y Reportería	-.368	.468	.029	-.430
13	Cifrado de equipos final e internos	-.061	.415	.050	.418
14	Monitoreo de software y hardware	-.176	.103	-.024	.627
15	Herramientas de Monitoreo	-.008	.004	.631	-.133
16	Controles de Seguridad	-.095	-.083	.752	-.160
17	Politicas de Acceso Web	.133	-.017	.679	.339
18	Acceso Remoto	.126	.095	.672	.385
19	Centro de Datos	-.442	-.192	.559	.214
20	Ciberinteligencia	.546	.528	-.347	-.134

Tabla 1. Componentes del punto final. Fuente: Elaboración Propia.

En este caso, de 20 variables analizadas observamos que la que tiene más peso son los firewalls de equipo final, seguidas del acceso a equipos de trabajo y los controles de seguridad, hasta llegar a la de menor carga factorial que es la disponibilidad de los servicios, lo que nos lleva a pensar que esto va más enfocado a una seguridad de equipos finales, con esta tabla no se confirma que si un enlace no está disponible o un servidor no tiene balanceada la carga no se impacte a la empresa, más bien, debe de adaptase a su entorno y esto es complejo de determinar. Lógicamente la ciberseguridad no puede verse como un todo, sino la descomposición de ese todo de acuerdo con lo indicado a continuación:

Matriz de componente rotado[a]

		Componente			
		1	2	3	4
1	Perfiles del Puesto	.507	-.228	.335	-.133
2	Capacitación	.844	.069	-.036	.099
3	Evaluación de Desempeño	.847	.071	-.086	.083
4	Compromiso de Confidencialidad	.638	.216	-.055	-.317
5	Código de Etica	.342	.184	.247	-.612
6	Respaldos	.695	.099	.482	.152
7	Manejabilidad	.614	.058	.200	.584
8	Cultura de Ciberseguridad	.467	.367	-.296	.385
9	Sistema de administración de la seguridad de la Informacion	.169	.362	-.240	.454
10	Monitoreo de la seguridad de Red	.085	.425	-.043	.176
11	Plataforma	.426	.225	.344	.497
12	Software	.128	.216	.365	.141
13	Almacenamiento	.107	.172	.581	-.215
14	Integración de Telefonia	.004	-.155	.743	.079
15	Control de aplicaciones	-.082	.142	.478	.506
16	Centralización de aplicaciones	.079	-.035	.102	.599
17	Comité de riesgos y seguridad	.168	.619	.013	-.041

Tabla 2. Componentes principales. Fuentes: Elaboración propia.

Matriz de componente rotado[a]

		Componente			
		1	2	3	4
1	Ciberseguros	-.403	.020	.611	.207
2	Sandboxing	.130	.229	.772	-.080
3	Ciber inteligencia	-.022	.001	.541	.309
4	Ofuscacion de aplicaciones	.350	.204	.682	.034
5	Deshabilitacion de servicios sin utilizar	.532	.565	.224	.177
6	Forzar integridad	.493	.146	.192	.390
7	Planeacion y direccion	.271	.348	.413	-.021
8	Politicas de seguridad	.263	.005	.717	-.058
9	Gestion de Incidentes	.566	.085	.361	-.379
10	Verificacion de servicios	.782	.266	-.011	-.062
11	Analisis de redes	.726	.319	-.102	.034
12	Monitoreo del ecosistema	.646	.416	-.085	-.061
13	Informacion de amenazas	.738	.128	.246	.168
14	Ciber inteligencia estratégica	.096	.139	.235	.150
15	Ciber inteligencia operacional	.156	.331	.501	-.232

Tabla 3. Componentes adicionales. Fuente: Elaboración propia.

Nota: Por conceptualización todas las tablas no están detalladas, ya que en total el modelo adopta la utilización de más de 70 variables y 250 criterios de investigación, es por ello por lo que si usted no observa alguno este puede estar contenido dentro de las mismas.

Si bien algunas variables han sido organizadas según los cuadros anteriores, es importante comentar que todo pertenece a la creación del modelo y su asignación de acuerdo a su homogeneidad. Es decir, muchas normativas asignan criterios a un título o factor sin determinar exactamente si el mismo tiene relación matemática o no, y esto es lo complejo porque no deberían de duplicarse factores para realizar un análisis de riesgos, muchos no estarán de acuerdo, pero para poder demostrar cada una de las variables estas se procesan independientes y el modelo matemático apoya a determinar su organización y peso.

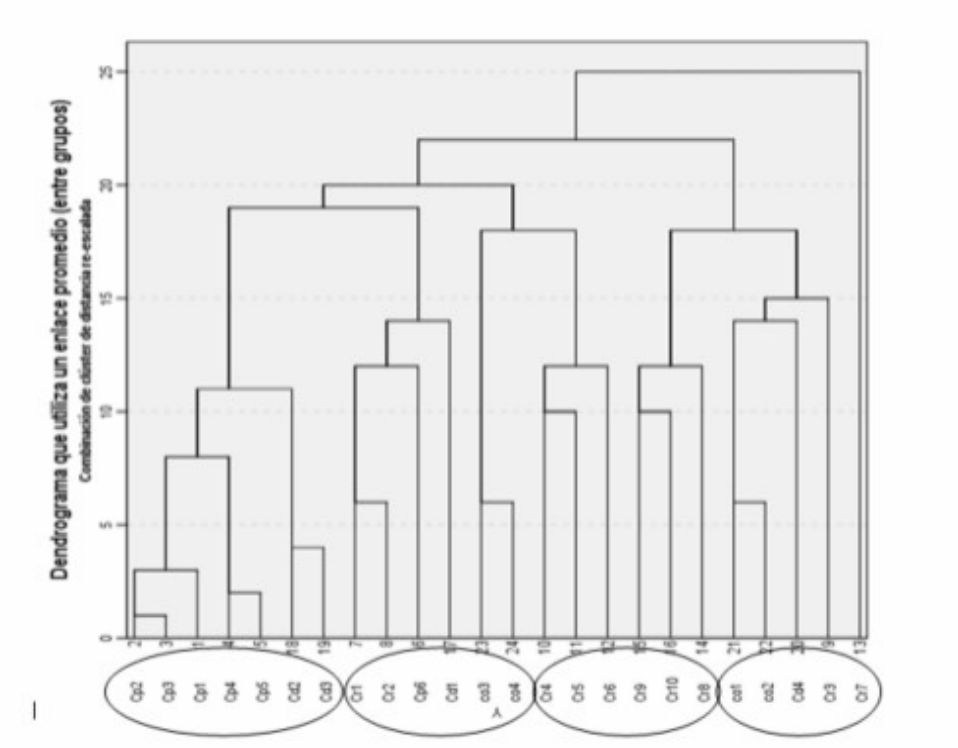


Figura 3. Análisis de variables. Fuente: Elaboración propia.

Conclusiones:

Para finalizar es importante recalcar que la descomposición de una estrategia de seguridad de la información traerá mayor conocimiento tanto técnico como científico para la empresa. El modelo no nació siendo de predicción más bien solo como una ayuda a tener visibilidad sobre la toma de decisiones relacionado con la ciberseguridad, pero estudios últimos han

podido comprobar su aplicabilidad con metodologías como NIST, El uso de COBIT basándose en NIST, la evaluación que realizó la Superintendencia de Bancos de Guatemala en el año 2020 para la medición de Ciber resiliencia en entidades afectas a las normativas de Guatemala. Por ello la importancia de generar una matriz de riesgos para mejorar la comprensión de estos y proponer un vector que determine sus cargas de riesgo.

Para todo ello la propuesta es aplicar modelos matemáticos que apoyen a las empresas en la toma de decisiones, ya que, si bien estamos enfocados en temas técnicos para la mitigación de riesgos es importante también basarnos en metodologías que aporten madurez a las actividades del día a día.

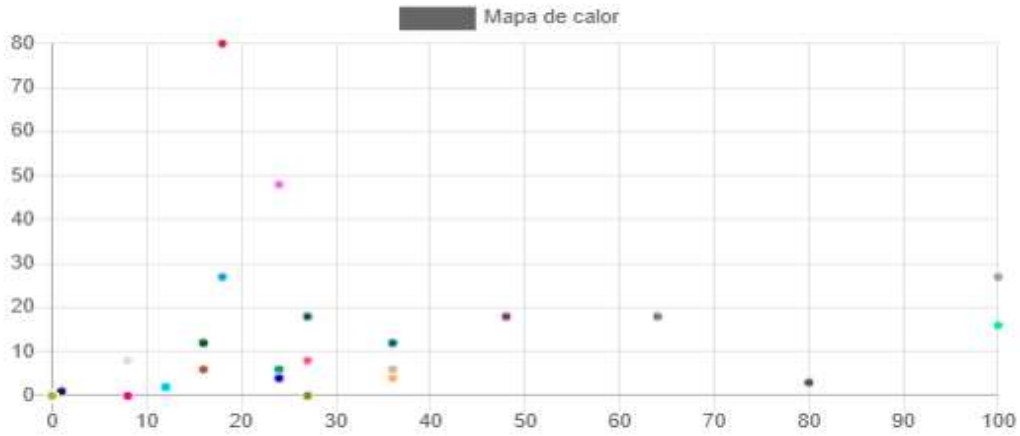


Figura 3. Mapa de Calor. Fuente: Elaboración propia.

Referencias bibliográficas

1. CYBER SECURITY MAGAZINE (2021). https://csecmagazine.com/2020/12/31/converciencia-guatemala/

2. ESCOBAR, A. M. (21 de 2 de 2017). slideshare.net. Obtenido de El teorema inconcluso en el proceso de la Seguridad de la Información: https://es.slideshare.net/armandomonzon/el-teorema-inconcluso-del-proceso-de-laseguridad-de-la-informacion

3. FINANTIAL STABILITY BOARD. (2018). Obtenido de fsb.org: http://www.fsb.org/2017/10/fsbpublishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/

4. G7. (2018). Obtenido de Fundamental Elements of Cybersecurity for the Financial Sector: https://www.fin.gc.ca/n17/docs/g7-1017-eng.pdf

5. GARTNER. (2017). Obtenido de Continuous Adaptive Risk And Trust Assessment.: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-thedigital-age/

6. GLOBAL SIGN. (1 de mayo de 2018). Obtenido de Globasign.com: https://www.globalsign.com/en/ssl-information-center/what-are-certificationauthorities-trust-hierarchies/

7. IEEE Xplore Management in the continuous assessment of computer risk, an agile Project. https://ieeexplore.ieee.org/abstract/document/8976980

8. ISACA.ORG. (2018). Obtenido de ISACA.ORG: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

9. MARTIN, L. (2018). The Ciber Kill Chain. Obtenido de Lockheed Martin: lockheedmartin.com114

10. MINGOB GUATEMALA. (2018). Obtenido de Ministerio de Gobernacion: http://mingob.gob.gt/wp-content/uploads/2018/06/version-digital.pdf

11. NIST. (2018). Obtenido de National Institute of Standard and Technology: https://www.nist.gov/

12. ORGANISATION INTERNATIONALE DE NORMALISATION. (2018). Obtenido de ISO.ORG: https://www.iso.org

13. SLIDESHARE (2018). Sistema Integral de Inteligencia de Amenazas aplicado al Cyber Dominio. https://es.slideshare.net/armandomonzon/owasp-guatemala-2018

Sobre de los autores:

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

CyberSecurity
Información & Privacidad

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. Dedique al final un párrafo para hacer resaltar las conclusiones más relevantes del trabajo.

Conclusiones: 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 2,021.

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