Volumen 2. Número 1. Serie A

ISBN: 978-99939-0-055-9

CyberSecurity

Información & Privacidad

Redes Neuronales Convolucionales

Un enfoque basado en la Ciberseguridad

Auditoría de TI y los sesgos cognitivos

Aspectos humanos que pueden interferir con las auditorias.

El Futuro de la ciber inteligencia de amenazas.

Combinación de intención, capacidad y oportunidad

Seguridad de Base de Datos

Garantizar la protección de las bases de datos

Implementación de buenas prácticas en los proyectos de tecnología

Un reto más allá de las metodologías

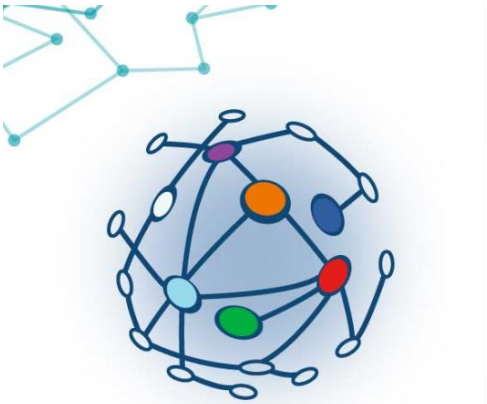
Educación para usuarios sobre seguridad de la información

Concientización sobre las amenazas de seguridad de la información

CyberSecurity

Información & Privacidad

Proyecto de:



ISBN: 978-99939-0-055-9

Publicación de la Asociación Universitaria en Ciencias de la Investigación (AUCI)

Dirección General

AUCI Guatemala

Junta Directiva

2019-2021

Cybersecurity Magazine - Información *y Seguridad*

Universidad Mariano Gálvez de Guatemala
Ing. Daniela de Villatoro
Ing. Criss Velasquez
Ing. Juan Soto
Ing. Armando Monzón

Diseño:
Ing. Darwin Fuentes

Mayo – Agosto 2020

Nota del editor

La ciberseguridad no es solo la ingeniería sino también es la gestión de las personas, procesos, datos, objetos y los aspectos legales que estén disponibles en nuestras regiones.

El conocimiento humano no se detiene, y ahora vemos que son varios profesionales los que nos escriben para presentar sus artículos, esta es una noticia muy buena para todos nuestros lectores, porque pueden conocer los puntos de vista de nuestros autores, sabemos de varios estudios que indican que la escasez de profesionales en seguridad afecta negativamente a los gobiernos, organizaciones, clientes y personas, lo cual lleva a violaciones de datos más frecuentes y costosas. Además esta brecha está amenazando la competitividad de los países de América latina porque no cuentan con profesionales capaces de afrontar los riesgos tecnológicos día a día. Cybersecurity Magazine ofrece a sus lectores experiencias de los autores que aplican procedimientos y metodologías como mejores prácticas en su preparación para afrontar ciber ataques, pero también la conceptualización de temas que pueden ser adoptados en nuestras empresas.

Entendemos que el conocimiento de los expertos en la ciberseguridad es un proceso de mejora continua y que deben de evolucionar tanto las habilidades humanas como técnicas para estar al ritmo de este mundo tecnológicamente cambiante. La fórmula para el conocer más de ciberseguridad es estudiar, preguntar y participar.

Criss

Artículos

(En orden de aparición)

CyberSecurity
Información & Privacidad

Redes Neuronales Convolucionales en la Ciberseguridad

Convolutional Neural Networks in Cybersecurity

Diego Pellecer Ochoa
email: dd.pellecer@gmail.com
Linkedin: Diego Pellecer
Recibido:10/diciembre/2019. Revisado: 20/febrero/2020. Aprobado: 15/marzo/2020.
Disponible en internet el 10 de Abril de 2020

Resumen: Vivimos en un mundo donde hay una guerra que pasa desapercibida para muchas personas, aquellos que realmente tienen conciencia de ella, toman medidas para contrarrestar la amenaza que representa para las organizaciones en las que trabajan, la guerra cibernética, donde cibercriminales buscan violar los sistemas de información de múltiples compañías en cualquier parte del mundo, para obtener la mayor cantidad de información y usarla a su favor, datos confidenciales, intercambiando el valor que esto representa por dinero, el malware que fabrican explotan vulnerabilidades en medios tecnológicos que utilizan en el día a día, y a medida que pasa el tiempo se vuelven amenazas más inteligentes, las redes neuronales convolucionales, son un tipo de inteligencia artificial, con los mecanismos del deep learning puede analizar malware y clasificarlo como amenazas, lo que beneficiaría a las instituciones a protegerse de ataques tecnológicos.

Palabras Claves: malware, ciberseguridad, guerra, riesgos, tecnológia.

Abstract: We live in a world where there is a war that goes unnoticed by many people, those who really are aware of it, take measures to counter the threat it represents for the organizations they work in, cyber warfare, where billions of cybercriminals seek violate the information systems of multiple companies anywhere in the world, to obtain the greatest amount of information and use it to their advantage, confidential data of people from all over the world, exchanging the value that this represents, for money, thanks to malware that manufacture, exploit vulnerabilities in technological means that they use on a daily basis, and as time passes, they become more intelligent threats, convolutional neural networks, are a type of artificial intelligence, with the mechanisms of deep learning can analyze malware and classify it as threats, which would benefit institutions to protect its image.

Desarrollo:

Las redes neuronales convolucionales, son uno de los tipos de arquitectura más conocidas del deep learning usada en la actualidad, el cual sirven para procesar imágenes y videos, gracias a esta arquitectura es posible desarrollar sistemas para la clasificación de imágenes, reconocimiento de objetos en escena, identificación de rostros, desarrollo de vehículos autónomos y en la salud en la detección de enfermedades a gran precisión. La idea central de una red convolucional es detectar patrones de entradas, con la característica de que los datos de entrada son imágenes.

Este tipo de arquitectura imita la forma en la que el cerebro procesa las imágenes en la corteza visual, la corteza visual se subdivide en distintas capas, la capa V1, al interpretar las imágenes estas neuronas se especializan en procesar patrones básicos, como líneas o bordes, en

distintas partes del objeto, entonces, luego de ser procesada es trasladada a la capa V2, en donde se analizan formas, en la capa V4, el grupo de neuronas es capaz de detectar ojos, nariz y boca, y la parte inferior temporal (IT) ya es capaz de identificar un rostro.

Una convolución es una operación matemática, en la que su función es la conjunción entre funciones. La red convolucional representa digitalmente las imágenes por medio de matrices desde 0 a 255 correspondiente a cada pixel, las imágenes son llevadas a capas convolucionales, que, a su vez, entrena en gran cantidad los filtros que se especializan en extraer distintas características de una imagen. Los datos de entrada, son los pixeles de una imagen. Si se cuenta una imagen con 741 pixeles de alto y 700 de ancho, equivale a 518,700 neuronas. Una red convolucional puede capturar con éxito las dependencias espaciales y temporales en una imagen a través de la aplicación de filtros relevantes. La arquitectura se adapta mejor al conjunto de datos de la imagen debido a la reducción en el número de parámetros involucrados y la reutilización de la información. En otras palabras, la red puede ser entrenada para comprender la sofisticación de una imagen.

La seguridad informática es el conjunto de políticas, técnicas, tecnologías y procesos que funcionan juntos para proteger la confidencialidad, integridad y disponibilidad de recursos informáticos. Existen mecanismos de defensa cibernética a nivel de datos. Hay una gran cantidad de herramientas, como firewalls, software antivirus, intrusión sistemas de detección (IDS) y sistemas de protección contra intrusos (IPS), que funcionan en sitio, para evitar ataques y detectar infracciones de seguridad. Sin embargo, muchos adversarios todavía tienen una ventaja, solo se necesita encontrar una vulnerabilidad en los sistemas que necesitan protección. En la actualidad, el número de personas con acceso a Internet ronda los 4.156 millones en todo el mundo, esto es, alrededor del 54% de la población mundial. Como el número de conectados a internet aumenta, la superficie de ataque también aumenta, lo que lleva a un mayor riesgo de ataque. Además, los atacantes se están volviendo más sofisticados, desarrollando exploits de día cero y malware que evaden medidas de seguridad, lo que les permite persistir durante largos períodos sin previo aviso. Hazañas de día cero son ataques que no se han encontrado previamente pero que a menudo son variaciones de un ataque conocido. Para exacerbar el problema, se están comercializando los mecanismos de ataque, lo que permite una distribución rápida sin necesidad de un entendimiento para desarrollar exploits. Además de defenderse contra externas amenazas, los defensores también deben protegerse contra las amenazas internas de individuos o entidades dentro de una organización que hace mal uso de su acceso autorizado.

A lo largo del ciclo de vida de un ataque, hay indicadores de compromiso; incluso puede ser significativo signos de un ataque inminente. El desafío está en encontrar estos indicadores que pueden distribuirse en todo el entorno, hay grandes cantidades de datos de aplicaciones, servidores, dispositivos smart y otros recursos cibernéticos generados por máquina a máquina y de persona a máquina. Los sistemas de defensa cibernética están generando datos voluminosos, como la información de seguridad. Sistema de gestión de eventos (SIEM), que a menudo abruma al analista de seguridad con alertas de eventos. El uso de la ciencia de datos en ciberseguridad puede ayudar a correlacionar eventos, identificar patrones y detectar comportamiento anómalo para mejorar la postura de seguridad de cualquier programa de

defensa. Estamos empezando a ver surgimiento de sistemas de defensa cibernética que aprovechan el análisis de datos. Por ejemplo, intrusión en la red. Los sistemas de detección (NIDS) que inspeccionan las transmisiones de paquetes, están evolucionando, a partir de sistemas basados en firmas, que detectan ataques conocidos a sistemas basados en anomalías que detectan desviaciones de un "normal" perfil de comportamiento..

Las redes neuronales convolucionales es una tecnología ideal para abordar el volumen y la velocidad del entorno de amenaza actual. Hoy en día, los delincuentes informáticos utilizan la automatización para generar y entregar malware nuevo a escala global a un ritmo de casi un millón por día. En contraste, nuestras defensas de amenazas tradicionales basadas en firmas son de naturaleza manual y se ven obsoletas.

Uno de los principales desafíos de seguridad informática hoy en día es la amenaza interna, que resulta en el robo de información o la explotación de vulnerabilidades inconscientemente. Las motivaciones y comportamientos de las amenazas internas varían extensamente; sin embargo, el daño que pueden causar internamente es significativo. Un vector de características que comprende un resumen de los registros del sistema para cada usuario podría ser creado para cada día y alimentado una red neuronal convolucional, creado para cada usuario con la salida objetivo siendo el vector de características del día siguiente. Cuando una predicción difiere dramáticamente de los datos de un día determinado, Se produce una anomalía. El uso de modelos separados para cada usuario significa que los modelos no tienen que tener en cuenta para el amplio comportamiento normal de todos los usuarios.

Sin embargo, existe un factor el cual debe de analizarse, el costo implícito de una clasificación errónea en el dominio de seguridad informática es un grave problema. Los falsos positivos en la clasificación de malware y la detección de intrusos molestan operadores de seguridad y obstaculizar la remediación en caso de infección real. En la detección de phishing, pueden hacer que no se entreguen mensajes importantes y legítimos para finalizar usuarios. Por el contrario, al no detectar malware, una intrusión en la red o un correo electrónico de phishing puede comprometer a toda una organización.

Las redes neuronales convolucionales aprende con base a su experiencia. Es una tecnología muy sofisticada y compleja, la cual no debe ser implementada solo en un campo especifico, si no en varios, para poder detectar malware se necesita contrastar múltiples fuentes de información, para que el algoritmo este lo suficientemente preparado para el análisis de patrones de vulnerabilidades y así evitar los ataques de día Zero.

La detección de intrusos tiene como objetivo descubrir actividades ilícitas dentro de una computadora o una red a través de sistemas de detección de intrusiones (IDS). Los IDS de red se implementan ampliamente en redes empresariales modernas. Estos sistemas se basaban tradicionalmente en patrones de ataques conocidos, pero las implementaciones modernas incluyen otros enfoques para la anomalía, detección de amenazas y clasificación basada en aprendizaje automático. Dentro del área de detección de intrusiones más amplia, dos problemas específicos son relevantes para nuestro análisis: La detección de botnets y de Algoritmos de Generación de Dominio (DGA). Una botnet es una red de máquinas infectadas

controladas por atacantes y mal utilizadas para conducir múltiples actividades ilícitas. La detección de botnets tiene como objetivo identificar las comunicaciones entre máquinas infectadas dentro de la red monitoreada y el comando y control externo servidores, a pesar de muchas propuestas de investigación y herramientas comerciales que abordan ante estas amenazas, todavía existen varias de ellas.

Referencias bibliográficas

Heartbleed, «Heartbleed,» [En línea]. Available: http://heartbleed.com/.

Checkpoint, «Live Cyber Threat Map,» [En línea]. Available: https://threatmap.checkpoint.com/.

A. Monzon, Interviewee, Redes Neuronales Convolucionales en la Ciberseguridad. [Entrevista]. 4 11 2019.

*G. Moreno, «*statista,» 28 05 2018. [En línea]. Available: https://es.statista.com/grafico/13903/cuantos-usuarios-de-internet-hay-en-america-latina/.

C. d. l. R. d. G. g, «Iniciativa que dispone aprobar Ley de Prevención y Protección contra la Ciberdelincuencia.,» [En línea]. Available: https://www.congreso.gob.gt/detalle_pdf/iniciativas/5614.

*S. d. Bancos, «*Reglamento para la Administración del Riesgo Tecnológico,» 2011.

*Britos, «*ENTRENAMIENTO DE REDES NEURONALES BASADO EN ALGORITMOS EVOLUTIVOS,» 2005.

R. E., « Introducción a las Redes Neuronales Artificiales.,» 2005.

M. Rodriguez, « Desarrollo de una interfaz gráfica de redes neuronales usando matlab,» 2009.

F. Tancano, « Introducción a las redes neuronales artificiales. Grupo de Inteligencia Artificial.,» 2003.

*J. Cowley, «*Redes neuronales convolucionales, Utilizar Python para implementar una red sencilla que clasifica dígitos escritos a mano,» IBM, 2018 12 7. [En línea]. Available: https://www.ibm.com/developerworks/ssa/lib rary/cc-convolutional-neural-network-visionrecognition/index.html. [Último acceso: 4 11 2019].

Y. LeCun, Deep Learning, Bengio, and G. Hinton, 2015.

F. M. K. B. T. A. B. R. &. M. A. M., Anomaly Detection in the Cloud: Detecting Security Incidents via Machine Learning, Gander, 2012.

Sobre el autor:

Desarrollador de Software, en los últimos años se ha dedicado a realizar sistemas de seguridad para el control de acceso lógico y BPM, apasionado a la ciberseguridad e Innovación, Ingeniero en Sistemas de Información y Ciencias de la Computación y Maestría en Seguridad Informática

El futuro de la ciber inteligencia de amenazas.

The future of cyber threat intelligence

Víctor Hugo Agustín Matzar Donado
email: vhamd14@gmail.com
Recibido:22/febrero/2020. Revisado: 10/marzo/2020. Aprobado: 22/marzo//2020.
Disponible en internet el 10 de Abril de 2020

Resumen: La inteligencia de amenazas cibernéticas está centrada principalmente en la recopilación de información sobre los ataques actuales e históricos potenciales que amenazan la seguridad de la organización así como también en el análisis de la información recopiladas, la inteligencia de amenazas ayuda a las empresas a ahorrar el costo financiero requerido para remediar desastres cibernéticos después de un ataque.

Palabras Claves: Ciberseguridad, inteligencia artificial, amenaza, ataques, ciber delincuentes.

Abstract: Cyber threat intelligence is primarily focused on gathering information about current and potential historical attacks that threaten the security of the organization as well as analyzing the information collected, threat intelligence helps companies save cost. financial requirement to remediate cyber disasters after an attack.

Desarrollo:

La ciber inteligencia se usa actualmente para identificar toda aquella información de interés para la empresa, datos sensibles que puedan haber sido comprometidos, definir e identificar a los atacantes, los detractores de la marca o simplemente alertar para prevenir un posible incidente cibernético.

Un punto importante en el cual debe fijarse la empresa en temas de ciberseguridad es que no se debe comprar tecnología de inteligencia de amenazas sin que esta inversión esté alineada con una visión a largo plazo para la gobernanza corporativa o los negocios comerciales de la empresa, aunque cada vez más empresas empiezan a centrarse en desarrollar una capacidad de inteligencia de amenazas más robusta y tecnológica para responder a las preguntas específicas de su giro de negocio. Para cada organización se deben conocer las amenazas ya que lo que puede ser una amenaza para unos, puede que no sea amenaza para otros giros de negocio.

Para que la amenaza exista, tiene que haber una combinación de intención, capacidad y oportunidad. Según lo indica el autor, estos factores deben existir para que la amenaza sea real para la organización, de no existir cualquier factor, esta amenaza no debe considerarse como una preocupación de ese momento. Una empresa con ciberseguridad debe tener bien identificados sus activos, su infraestructura, sus procesos y los profesionales de ciberseguridad que protegen la empresa, si alguno de los puntos anteriores no están bien definido, se facilitan las oportunidades para los atacantes, teniendo bien definidos estos aspectos dentro de la empresa, se procede a identificar a los posibles atacantes, de no lograr identificar a los posibles atacantes la empresa no podrá reconocer cuales son las intenciones de los atacantes.

Mediante la inteligencia de amenazas se analiza y recopila la información de la intención, capacidad y oportunidad de los agentes maliciosos frente a la empresa, alguien debe estar atento a los indicadores, puede ser el proveedor o consultor que le brinda los servicios de ciberseguridad a la empresa o algún profesional de la ciberseguridad que trabaje para la empresa, de cualquier forma la toma de decisión frente a los agentes maliciosos debe ser inmediata, si nadie monitorea la herramienta de inteligencia de amenazas cibernéticas únicamente se estarán generando volúmenes de datos sobre amenazas, intenciones y capacidades sin que la información sea provechosa pues no se toma decisiones en base a ella.

Cuando una empresa con inteligencia de amenazas cibernéticas tiene la capacidad de recopilar, analizar y consumir información de amenazas a su medida, la inteligencia de amenazas puede proporcionarle a la empresa opciones estratégicas y tácticas para acciones concretas que impacten positivamente la ciberseguridad de toda la empresa.

Desde algún tiempo atrás los sectores gubernamentales y financieros están liderando la integración de la inteligencia de amenazas cibernéticas en sus organizaciones, debido al giro de negocio de estas organizaciones su ciberseguridad es mucho más robusta y compleja que la mayoría de las empresas, esto contribuye a que se desarrollen mejores prácticas en ciberseguridad que puedan ser adoptadas por todo tipo de empresas.

Las empresas que adquieran una herramienta de inteligencia de amenazas cibernéticas poco a poco estarán cambiando su postura de seguridad reactiva, actuar una vez se han vulnerado los activos, para pasar a una postura proactiva que reducirá de gran manera los ataques exitosos de los agentes maliciosos o cibercriminales, las empresas verán la importancia de conocer a fondo su propio entorno para lograr una ciberseguridad proactiva.

Otra virtud de la inteligencia artificial en la ciberseguridad es que se pueden realizar tareas repetitivas reduciendo la intervención humana y por consiguiente los posibles errores que puedan cometer los humanos. Este cambio en las empresas hará que los profesionales de la ciberseguridad puedan enfocarse en tareas más valiosas y estratégicas dejando las tareas repetitivas para las máquinas y la inteligencia artificial.

Aplicar inteligencia predictiva para apoyar la inteligencia de amenazas implicará que la empresa esté lista para predecir o anticiparse a nuevas amenazas y ataques haciendo la ciberseguridad de la empresa predictiva y orientada al futuro. Los ataques históricos en la empresa deben ser almacenados, identificados y etiquetados de la mejor manera para que la inteligencia artificial pueda aprender a partir de las consecuencias pasadas y se pueda predecir e identificar amenazas con mucha más rapidez.

Los cibercriminales también pueden utilizar la inteligencia artificial para realizar sus ataques, por esto es necesario que se implemente en las empresas lo antes posible el uso de la inteligencia artificial ya que la inteligencia de amenazas cibernéticas que se utiliza actualmente en Guatemala es reactiva y basada en reglas y análisis humano, lo que conlleva en un atraso significante frente a las nuevas herramientas utilizadas por los cibercriminales.

El internet de las cosas viene a aumentar más dispositivos a los cuales proteger en la empresa y para lo cual la inteligencia artificial puede apoyar con tareas básicas y repetitivas de ciberseguridad en estos dispositivos, para las empresas contratar un profesional de ciberseguridad es algo costoso y no existen muchos profesionales calificados por lo que se hace más difícil impedir los ataques a las redes e impedir que sea violada la integridad de los datos durante los próximos años.

La inteligencia de amenazas cibernéticas en los países desarrollados y en grandes empresas de Guatemala está siendo orientado poco a poco hacia la inteligencia artificial, con patrones de comportamiento, analítica predictiva, aprendizaje automático y otros enfoques pero para la mayoría de las empresas guatemaltecas el futuro más cercano sería implementar la inteligencia de amenazas cibernéticas basada en reglas y en inferencias de los profesionales de ciberseguridad. Otra orientación a futuro de la inteligencia de amenazas es que se pueda compartir la información crucial de amenazas entre las diferentes empresas del mismo giro de negocio de forma estandarizada y con información relevante.

En Guatemala las empresas deben alinearse hacia el uso de la inteligencia artificial no solo en el área de negocios si no también en la ciberseguridad, gracias al rápido crecimiento en las infraestructuras de internet en el país se prevé que se aumenten los ataques por medio de la red desde otros países, para combatir estos ataques masivos las empresas deben poseer inteligencia de amenazas robustas y con inteligencia artificial para contrarrestar casi en tiempo real estos ataques y amenazas.

El futuro general de los análisis de amenazas cibernéticas en cuanto a la inteligencia artificial es que estos sean capaces de simular las inferencias y tomar decisiones como las de los profesionales humanos de ciberseguridad con más experiencia y en una escala mayor defendiendo de múltiples ataques.

Referencias bibliográficas

Acosta, C. R. (20 de febrero de 2018). Inteligencia de amenazas cibernéticas. Obtenido de Seguridad de América: https://www.seguridadenamerica.com.mx/noticias/articulos/14727/inteligencia-de-amenazas-ciberneticas

Houston, M. (20 de junio de 2018). ¿Es la Inteligencia Artificial el futuro de la Ciberseguridad? Obtenido de Houston Tech Solutions: https://mrhouston.net/blog/inteligencia-artificial-y-futuro-de-ciberseguridad/

Columbus, L. (14 de julio de 2019). Why AI Is The Future Of Cybersecurity. Obtenido de Forbes: https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#7b91787d117e

Hernandez, M. (27 de febrero de 2020). Inteligencia Artificial, la herramienta más prometedora para la defensa cibernética. Obtenido de Forbes Centroamérica: https://forbescentroamerica.com/2020/02/27/inteligencia-artificial-la-herramienta-mas-prometedora-para-la-defensa-cibernetica/

Deolitte. (2019). Inteligencia cibernética. Obtenido de Deolitte: https://www2.deloitte.com/content/dam/Deloitte/cr/Documents/risk/doc/2019-Inteligencia-Cibernetica.pdf

International, K. (2013). Cyber threat intelligence and the lessons from law enforcement. (Vol. 121412).

Serrano, A. (29 de junio de 2018). Inteligencia Artificial: el futuro de la ciberseguridad. Obtenido de AT Sistemas: https://www.atsistemas.com/es/blog/inteligencia-artificial-el-futuro-de-la-ciberseguridad

Banafa, A. (27 de marzo de 2018). Inteligencia Artificial en ciberseguridad. Obtenido de Open Mind BBVA: https://www.bbvaopenmind.com/tecnologia/inteligencia-artificial/inteligencia-artificial-en-ciberseguridad-retos/

Marty, R. (1 de noviembre de 2018). AI in Cybersecurity: Where We Stand & Where We Need to Go. Obtenido de Dark Reading: https://www.darkreading.com/threat-intelligence/ai-in-cybersecurity-where-we-stand-and-where-we-need-to-go/a/d-id/1330787*?*

Sobre el autor:

Analista en modelación y predicción de datos, con más de 7 años de experiencia, Profesional de Ingeniería en Sistemas de la Información y de la Maestría en Seguridad de Sistemas de Información, tiene cursos sobre el manejo de big data e inteligencia artificial con Python y R. En su carrera profesional ha laborado en diferentes roles de ingeniería como desarrollador y analista de datos. Actualmente se desempeña como analista en modelación y predicción de datos regional para Corporación Banco Industrial en Guatemala y Banco BanPaís en Honduras.

CyberSecurity
Información & Privacidad

Auditoría de TI y los sesgos cognitivos

IT audit and cognitive biases

Jeniffer Mazariegos
email: jeniffer6@gmail.com
Linkedin: Jeniffer Mazariegos
Recibido:15/enero/2020. Revisado: 22/febrero/2020. Aprobado: 10/Marzo/2020.
Disponible en internet el 10 de Abril de 2020

Resumen: En este caso exploraremos brevemente algunos de los sesgos que podrían afectar a un auditor de tecnologías de información en la validación de cumplimiento. Los entrenamientos en auditoría tienden a hacer mucho énfasis en poder mantener la objetividad, la independencia y la racionalidad al realizar una auditoría, y se centran mucho en metodologías, pero pocas veces entramos en detalle en los aspectos humanos que pueden interferir con las validaciones.

Palabras Claves: auditoria, sistemas, sesgos, cognitivo, cumplimiento.

Abstract: We will briefly explore some of the biases that could affect an information technology auditor in compliance validation. Audit training tends to put a lot of emphasis on being able to maintain objectivity, independence and rationality when conducting an audit, and focus a lot on methodologies, but we rarely go into detail on the human aspects that can interfere with validations .

Desarrollo:

El 2002, el psicólogo Daniel Kahneman fue galardonado con el premio Nobel de Economía, gracias a una investigación que dio origen al campo de "behavioral economics" (economía conductual). Kahneman, en conjunto con Amos Tversky inició una investigación en 1969, que acuñó término: sesgos cognitivos. A través de múltiples experimentos, y un estudio del funcionamiento del cerebro humano, Daniel Kahneman logró identificar patrones en los errores que las personas cometen. Dichos errores, son ilusiones del pensamiento, o ilusiones cognitivas, que nos engañan de la misma forma que lo hace una ilusión visual. Lo interesante y trascendente, de este estudio psicológico, es que prácticamente descubre y tipifica los "bugs" del cerebro humano. Y, ojo, esto no tiene nada que ver con nuestra inteligencia, ya que todos estamos sujetos a los mismos "bugs", por el simple hecho de ser humanos.

En su momento Kahneman logró aplicar los resultados de su estudio a la economía, ya que toda la teoría económica hasta el momento se basaba en el supuesto de que los seres humanos somos seres racionales, que tomamos decisiones racionales. El análisis de Kahneman, comprobó que nuestra capacidad de tomar decisiones racionales está seriamente afectada por nuestros bugs humanos. Ahora bien, siendo este un estudio que analiza nuestros fallos cognitivos toma relevancia en todos los aspectos de la vida que involucren decisiones, tanto en nuestra vida laboral como en la vida profesional.

Framing (Marcos), este sesgo, nos indica que presentar la misma información de distintas formas, puede evocar distintas emociones. Abajo vemos la imagen de una carta de renuncia que fue escrita por un juez argentino, con tipo de letra Comic Sans. Este detalle,

aparentemente absurdo, cambió totalmente la forma en la que el mensaje fue recibido por el receptor, ya que dicho tipo de letra está asociado a comunicaciones informales (o Comics).

Imagen 1 – Carta de Renuncia Ejemplo

Juez de la Corte argentina renuncia con carta escrita en Comic Sans

La misiva enviada por Eugenio Zaffaroni atrae la atención de usuarios de redes sociales que critican su formato

Por: EL INFORMADOR
31 de Octubre de 2014 - 11:36 hs

Eugenio Raúl Zaffaroni

Buenos Aires, octubre 31 de 2014

A la Señora Presidenta de la Nación Argentina
Dra. Dª Cristina Fernández de Kirchner
Su Despacho.

Distinguida Señora Presidenta:

Tengo el alto honor de dirigirle las presentes líneas para elevar a su fina consideración mi renuncia al cargo de Ministro de la Corte Suprema de Justicia de la Nación, para el que fui designado por el Presidente Néstor Kirchner mediante decreto 932 de 2003, y que asumí hace hoy exactamente once años.

Fragmento de la carta enviada por Zaffaroni a la presidenta de Argentina. ESPECIAL /

Fuente: Informador.mx

Este ejemplo nos hace cuestionar, si la formalidad, la presentación y la forma en que se nos presenta la evidencia al momento de una auditoría tiene un impacto sobre la valoración que le daremos. Es posible que tengamos una tendencia a aceptar evidencia que sea entregada en un formato que sea agradable a nosotros. O lo contrario, que rechacemos evidencia que tiene una mala presentación o un formato poco amigable.

Motivated reasoning bias, estudios han indicado que, en la ausencia de evidencia de soporte, los auditores son más propensos a convencerse a sí mismos de que una explicación dada por el cliente es razonable, aunque no tenga una evidencia de soporte. Esto, con tal de lograr un objetivo deseado por el auditor, como agradar al cliente o cumplir con un presupuesto de horas. Por ejemplo, en una situación en la que el objetivo es finalizar la auditoría y emitir el informe en tiempo record, si el auditor se encuentra con que no ha recolectado suficiente información para validar un punto, existirá la tentación de colocar un control en cumplimiento, basado solamente en una conversación o en evidencia no concluyente.

Confirmation Bias (Sesgo de confirmación), el sesgo de confirmación se ejemplifica mejor con el siguiente caso: Si alguien pregunta "¿Juan es amigable?", la pregunta nos hará traer a la mente características de Juan que no hubieran venido a la mente si la pregunta hubiera sido "¿Juan es hostil?". De la misma forma, si tenemos una idea preconcebida, tendemos a buscar en el entorno, datos que nos permitan validar la misma, y obviar información que pueda botar nuestra idea. Si el auditor ya cuenta con la idea preconcebida de que algo está mal o bien, buscará evidencia de soporte para poder respaldar su punto. En algunos casos, la experiencia

nos da ciertas pistas sobre lo que podría estar mal, lo importante es saber recolectar toda la evidencia, y estar dispuestos a aceptar evidencia que contradiga nuestra hipótesis inicial.

Anchoring Bias (Sesgo de ancla), tendemos a ser presas de este sesgo cognitivo en nuestro día a día, por ejemplo: Es más probable que compremos un sándwich de 7 quetzales si previamente vimos un sandwhich que costaba 20 quetzales. ¿Qué podría sucederle a un auditor que valida cumplimiento para distintas empresas de forma consecutiva? Podríamos plantear el caso en que sea necesario validar el cumplimiento de una empresa A (en muy mal estado de cumplimiento) y la empresa B (en un estado de cumplimiento más aceptable). Si se valida cumplimiento para B inmediatamente después de finalizar la validación de A, pueda que exista una tendencia a calificarla de mejor forma que si hubiera validado primero A y luego B.

¿Qué podemos hacer al respecto?

Como fue expuesto en un inicio, los sesgos cognitivos tienen que ver mucho con el cerebro, pero no con nuestra inteligencia. Una persona muy inteligente puede tomar las peores decisiones si se basa solo en su intuición.

Lo más importante que podemos hacer para evitar caer en este tipo de errores, es conocer los distintos sesgos y saber reconocerlos cuando se presentan en el día a día. Al reconocerlos, sabremos esquivar de mejor forma estas trampas cognitivas y poder realizar así un trabajo más profesional.

Referencias bibliográficas

Kahneman, D. (2011). Thinking, fast and slow.

https://www.journalofaccountancy.com/issues/2019/aug/biases-jeopardize-audit-quality.html

https://www.journalofaccountancy.com/issues/2019/aug/biases-jeopardize-audit-quality.html

https://medium.com/the-mission/nobel-prize-winning-psychologist-explains-the-cognitive-biases-that-lead-to-bad-decisions-74a729e98cc9

https://search.proquest.com/openview/54c5c5ba63b751445d533d93f168660f/1?pq-origsite=gscholar&cbl=41798

Sobre el autor:

Ingeniera en Sistemas, con estudios en MBA con especialidad en Finanzas. Con 9 años de experiencia en auditoría y consultoría de TI, cuenta con las certificaciones ISO 27001, ISO 27005, CISM, y CISSP.

Seguridad de Bases de Datos

Database security

Jonathan Mancilla
Email: kevinmancilla@gmail.com
Linkedin: Jonathan Mancilla
Recibido:8/marzo/2020. Revisado: 20/marzo/2020. Aprobado: 25/marzo/2020.
Disponible en internet el 10 de Abril de 2020

Resumen: Nos encontramos en una época donde la seguridad e integridad de las bases de datos es de suma importancia debido a que las vulnerabilidades incrementan con forme la evolución tecnológica sigue avanzando a grandes pasos, vemos que cada día son más las organizaciones e industrias que apoyan sus procesos en bases de datos, esto conlleva a que dichas organizaciones tengan información sensible en sus equipos informáticos y que la misma sea objeto de ataques, por lo cual, los ciber criminales buscan como poder obtener acceso a dicha información. A raíz de esto, las organizaciones buscan incrementar sus niveles de seguridad apoyándose en tecnologías, metodologías, configuraciones y una buena administración de los recursos, asegurando así la Confidencialidad, Integridad y Disponibilidad de la información. Derivado de lo anterior, en esta sección veremos de forma introductoria estos fundamentos en cuanto a la implementación de seguridad para las bases de datos a partir de los pilares de seguridad de la información, mejores prácticas extraídas de diversas metodologías y los requisitos mínimos requeridos, con el propósito de garantizar el aseguramiento de los datos en reposo, en tránsito y en procesamiento.

Palabras Claves: base de datos, seguridad, integridad, protección, diseño.

Abstract: We are at a time when the security and integrity of databases is of utmost importance because vulnerabilities increase as technological evolution continues to advance in strides, we see that more and more organizations and industries support their processes. In databases, this means that these organizations have sensitive information on their computer equipment and that it is the object of attacks, so that as well as cyber criminals looking for ways to obtain such sensitive information, organizations also seek to increase their security levels. relying on technologies, configurations and good administration to ensure the Confidentiality, Integrity and Availability of the information. In this work we will address the security for databases, the minimum measures required, the necessary configurations and as the best practices to ensure data at rest, in transit and in processing.

Desarrollo:

Cuando hablamos de integridad en base de datos nos estamos refiriendo a la completitud, exactitud y la coherencia de un conjunto de datos. Podemos tener una percepción de esta integridad cuando vemos que entre dos instancias o entre dos actualizaciones de un registro de datos, no hay ninguna alteración, lo que significa que los datos están intactos y sin cambios. El concepto de integridad garantiza que todos los datos pueden ser rastreados mediante técnicas de trazabilidad, así como conectarse a/entre otros datos. De esta forma se asegura que todo se puede buscar y recuperar.

La seguridad de la información se encarga de proteger la confidencialidad, disponibilidad e integridad en las bases de datos de todos los activos de conocimiento de la organización. La forma de lograrlo tiene que ver con:

Confidencialidad: se trata del aspecto más importante de la seguridad de base de datos. Este objetivo se alcanza mediante la encriptación, que ha de aplicarse a datos en reposo, pero también a los datos que, por un motivo u otro, se encuentren en tránsito.

Integridad en base de datos: busca garantizar que sólo las personas autorizadas podrán acceder a información privilegiada de la empresa. La integridad de una base de datos se aplica a través de protocolos de autenticación, políticas internas (como las que impulsan la seguridad de las contraseñas) y un sistema de control de acceso de usuario que define los permisos que determinan quién puede acceder a qué datos. Sin embargo, no debe obviarse el tomar medidas que ayuden a conseguir que las cuentas no utilizadas queden bloqueadas o sean eliminadas.

Disponibilidad: hace referencia a la necesidad de que las bases de datos y toda la información que contienen estén listas para su uso. Por una parte, se debe garantizar su funcionalidad y confiabilidad mientras que, por otra, es recomendable planificar los tiempos de inactividad fuera del horario laboral.

Garantizar la integridad en base de datos, así como su disponibilidad y confiabilidad es determinante para obtener un buen funcionamiento y alcanzar de manera ágil y eficiente los objetivos de negocio. Sin embargo, la amenaza no da tregua, hoy, los ataques se multiplican, tanto en frecuencia, como en objetivo. Los ciber delincuente ya no codician sólo los activos de información de las grandes corporaciones multinacionales, sino que tienen en su punto de mira a todo tipo de empresas, independientemente de su tamaño, propósito o industria.

Una de las formas más efectivas de garantizar la integridad en base de datos es implementando algunas de las mejores prácticas de seguridad. Entre ellas se encuentran las siguientes:

Recurrir al enmascaramiento de datos o permitir a los usuarios acceder a cierta información sin poder verla, ayuda a mantener la confidencialidad incluso en entornos de pruebas. Minimizar los extras y limitarse a los servicios, aplicaciones y funcionalidades que realmente son necesarios para asegurar el adecuado funcionamiento de las operaciones del negocio, de esta manera se reduce el riesgo.

Asegurarse de que los administradores de la base de datos entiendan la importancia de garantizar su protección. Mantener actualizadas las bases de datos y eliminar los componentes desconocidos. Recurrir a herramientas como el análisis de código estático, que ayudan a reducir los problemas de inyección de SQL, desbordamiento de búfer y problemas a nivel de configuración.

Hacer copias de seguridad frecuentes, hacer pruebas de funcionamiento a esas copias, almacenarlas y emplear un Sistema de Alimentación Ininterrumpida o SAI que garantice que un corte de energía no causa la pérdida de datos.

La base de datos debe ser protegida contra el fuego, el robo y otras formas de destrucción. Los datos deben ser reconstruibles, ya que siempre pueden ocurrir accidentes. Los datos deben poder ser sometidos a **procesos de auditoria,** el sistema debe diseñarse a prueba de intromisiones, no deben poder pasar por alto los controles. Ningún sistema puede evitar las

intromisiones malintencionadas, pero es posible hacer que resulte muy difícil eludir los controles. El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.

La seguridad se logra si se cuenta con un mecanismo que limite a los usuarios a su vista o vistas personales. La norma indica que toda base de datos relacional cuente con dos niveles de seguridad: Relación: Puede permitírsele o impedírsele que el usuario tenga acceso directo a una relación. Vista: Puede permitírsele o impedírsele que el usuario tenga acceso a la información que aparece en una vista.

Audite: Una vez que haya creado una configuración y/o bien haya madurado sus controles, realice auto evaluaciones y de seguimiento a las recomendaciones de auditoría para asegurar que no se desvíe de su objetivo (la seguridad). Automatice el control de las configuraciones de tal forma que se registre cualquier cambio en la misma. Implemente alertas sobre cambios en la configuración. Cada vez que un cambio se realice, este podría afectar a la seguridad de la base de datos.

Monitoree en tiempo real la actividad de las bases de datos, esto es clave para limitar su exposición, aplique o adquiera agentes inteligentes de monitoreo (apóyese en herramientas de ser necesario), detección de intrusiones y uso indebido. Recuerde que el monitoreo de usuarios privilegiados es requisito para la gobernabilidad de los datos y cumplimiento de regulaciones como la Ley SOX y regulaciones de privacidad. Esto también, ayuda a detectar intrusiones, ya que muchos de los ataques más comunes se hacen con privilegios de usuario de alto nivel. El monitoreo dinámico es también un elemento esencial para la evaluación de vulnerabilidades, le permite ir más allá de evaluaciones estáticas o forenses. Un ejemplo clásico lo vemos cuando múltiples usuarios comparten credenciales (a lo que se le conoce como préstamo de usuarios) con privilegios o un número excesivo de inicios de sesión en las bases de datos.

Aplique pistas de auditoría y genere trazabilidad de las actividades que afectan la integridad de los datos, o la visualización los datos sensibles. Recuerde que es un requisito de auditoría, y también es importante para las investigaciones forenses. La mayoría de las organizaciones en la actualidad hacen uso de manuales de auditoría de transacciones o aplicaciones nativas de los sistemas gestores de bases de datos. Sin embargo, estas aplicaciones son a menudo desactivadas, debido a: su complejidad, altos costos operativos, problemas de rendimiento, la falta de segregación de funciones y la necesidad mayor de capacidad de almacenamiento.

Afortunadamente, se han desarrollado soluciones con un mínimo de impacto en el rendimiento y poco costo operativo, basado en tecnologías de agente inteligentes. No todos los datos y no todos los usuarios son creados iguales. Usted debe autenticar a los usuarios, garantizar la rendición de cuentas por usuario, y administrar los privilegios para delimitar el acceso.

Implemente y revise periódicamente los informes sobre los accesos otorgados e ingresos registrados de los usuarios, como parte de un proceso formal de auditoría.

Utilice el cifrado para hacer ilegibles los datos confidenciales, complique el trabajo a los atacantes, esto incluye el cifrado de los datos en tránsito, de modo que, un atacante no pueda escuchar en la capa de red y tener acceso a los datos cuando estos son enviados al cliente de base de datos.

Referencias bibliográficas

ISO/IEC 27001:2005 – Information technology – Security techniques
http://www.iso.org/iso/catalogue_detail?Csnumber=42103

ISO/IEC 17799:2005 - Information technology -- Security techniques http://www.iso.org/iso/catalogue_detail

Malware - Ataque a la Base de Datos http://ataquebd.blogspot.mx/

Sobre el autor:

Jonathan Mancilla, Ingeniero en Sistemas por universidad Mariano Gálvez de Guatemala, con 9 años de experiencia en Tecnologías de la Información y 3 años dedicado al control de seguridad informática, así como a la elaboración y dirección de auditorías en ambientes tecnológicos, operativos y financieros, con alto enfoque en gestión de riesgos, continuidad de negocio y servicio, aseguramiento de sistemas, administración de proyectos, servidores, redes, bases de datos, infraestructura, desarrollo, soporte técnico y comunicaciones móviles. A laborado en empresas multinacionales como Samsung y Codisa. Actualmente se desempeña como Supervisor de Auditoria para Bac Credomatic de Guatemala. Sus principales bases Dios y su familia.

Educación para usuarios sobre seguridad de la información

Information Security Awareness

Lourdes Molina
email: lu.molina10@gmail.com
Linkedin: Lourdes Molina
Recibido:19/noviembre/2019. Revisado: 20/febrero2020. Aprobado: 10/marzo/2020.
Disponible en internet el 10 de Abril de 2020

Resumen: Es responsabilidad de las empresas el realizar una correcta capacitación y/o concientización sobre las amenazas de seguridad de la información que apliquen a su entorno así como las políticas y procedimientos para administrarlas. Las políticas de seguridad de la información están contempladas en distintas normas y estándares de seguridad de la información y se incluye adicional como control de cumplimiento la correcta divulgación y capacitación sobre las mismas. Los medios de divulgación de estas políticas y mejores prácticas dependen de las metodologías de enseñanza adoptadas por cada empresa y de los recursos disponibles. El constante avance de las tecnologías de información nos ha brindado herramientas con las que podemos capacitar y educar a las personas de forma remota. Plataformas de E-Learning cuentan con distintas funcionalidades que permiten generar cursos y capacitaciones a la medida de las empresas.

Palabras Claves: E-Learning, Seguridad de la información, Concientización, LMS.

Abstract: The human element is one of the most critical factors of an information security program and it is often the most neglected. A large proportion of the incidents are caused by uninformed employees who have no real awareness of the scope of their actions. This also applies as individuals, if you don't want your checkbook to be stolen you don't leave it in a public space, right? Then how do you explain this to your employees in an understandable yet affordable and effective way? The main objective is to protect your company information but how do you do it? In this article you can find answers to that kind of question.

Desarrollo:

La información que se administra es ahora el activo más importante de las empresas, el flujo de información permite que los datos sean vulnerables de captura y por lo tanto de manipulación. Existen distintas prácticas, herramientas y métodos para la prevención de cualquier tipo de delito informático, estas incluyen hardware y software que ayudan a proteger la información y el flujo de esta. El trabajo metódico de los analistas de seguridad informática debe considerar todos los puntos débiles y realizar mejoras sobre los mismos con el fin de evitar cualquier robo, fraude, manipulación, mal uso y destrucción de los datos que permiten el funcionamiento óptimo de las empresas.

Este es un proceso constante de mejora que debe ser llevado por los ingenieros en seguridad de la información; recordemos que si bien hablamos de información digital la seguridad no se limita solo a la información intangible; hablamos también de la información que encontramos en medios físicos como papelería, oficinas en donde se almacene información, instalaciones de centros de cómputo, videovigilancia, seguridad perimetral, entre otros.

Las evaluaciones constantes nos permiten tener control sobre las medidas a tomar para la protección de la información; sin embargo encontramos que los vectores de ataque también se mantienen en constante evolución, este es el caso de ataques como Ransomware el cual luego de infectar al equipo, secuestra la información cifrándola para que no pueda ser utilizada. El atacante luego de esto extorsiona a sus víctimas para que realicen un pago con cierta cantidad de dinero en dinero electrónico para recuperar sus datos. Los atacantes que utilizan el Ransomware por lo general perjudican a los archivos de ofimática, estos archivos son los que contienen información sensible y son los que generan más pérdida cuando no pueden ser recuperados.

La administración de la seguridad de la información es uno de los grandes problemas de las organizaciones. Se depende de administradores y analistas de seguridad para mantener las distintas capas de información aseguradas. Los especialistas de Seguridad Informática deben administrar los valores de las empresas manteniendo la confidencialidad, integridad y disponibilidad de la información.

En un estudio realizado por IBM se demostró que la inmensa mayoría de los ataques perpetrados por ciberdelincuentes alcanzaban el éxito debido a algún tipo de error humano. En el informe elaborado por investigadores en seguridad de IBM, conocido por IBM X-Force Threat Intelligence Index 2018, se puso de manifiesto este hecho analizando las causas de diversos incidentes de seguridad revelados públicamente a lo largo de 2015, 2016, 2017 y 2018. (OSI, 2018). Esta información se refiere únicamente a los incidentes de seguridad de las empresas, ¿nos podemos imaginar entonces que sucede en nuestros hogares o en pequeñas empresas con cero o poco soporte técnico?

Como usuarios finales hacemos de lado la importancia de nuestra propia información; consideramos que nuestras cuentas bancarias, números de tarjetas, correos electrónicos y contraseñas no son un botín apetitoso para los ciberdelincuentes y que no somos un objetivo para ellos. Sin embargo no consideramos que para un atacante no siempre es un objetivo el tamaño del botín si no la facilidad de alcanzarlo. La poca seguridad con la que utilizamos y damos nuestros datos personales en línea nos convierte en un objetivo fácil de alcanzar para los atacantes.

Si analizamos la información brindada por Index Global Web (MediaClick, 2019) podemos ver que es posible identificar las edades de los usuarios dependiendo del uso de las redes sociales. Si tomamos esta información podemos ver que Facebook y LinkedIn son las redes sociales utilizadas por las personas mayores a 50 años. Según las edades el uso de internet y redes sociales tiene una variación; las personas de menor edad han sido expuestos desde temprano a la tecnología por lo que el uso es más fácil mientras que las personas de mayor edad tienen una adaptabilidad distinta lo cual puede generar una brecha de seguridad.

El desconocimiento de las estafas electrónicas, la generación de claves de forma segura, los distintos tipos de gusanos y virus existentes en la red son temas que representan una constante amenaza para los usuarios de mayor edad. De esa misma forma nos tiene que preocupar nuestra información digital, en que sitio la almacenamos, a quien le compartimos nuestros datos de identificación y correo electrónico y como la utilizamos.

En el caso de las empresas la responsabilidad podemos decir que es “compartida” diciendo esto nos referimos a que el usuario se hace responsable según las políticas de seguridad de la información establecidas por la empresa y la empresa se hace responsable de establecer y monitorear estas políticas. En muchas empresas es posible ver que existen acuerdos de confidencialidad que limitan a los usuarios sobre qué información compartir y bajo que reglamentos. El incumplimiento de estos acuerdos puede tener como consecuencia penalizaciones, despidos y hasta denuncias legales dependiendo la legislación del país en donde fue firmado. A pesar de que los usuarios son responsables del manejo de la información las empresas son las que establecen y divulgan estas políticas.

Cuando los usuarios se encuentran familiarizados con las técnicas de prevención de incidentes de seguridad, bajo una metodología de aprendizaje constante y con herramientas interactivas; se reduce el riesgo de que sucedan ataques contra la integridad, confidencialidad y disponibilidad de la información de forma significativa. Estamos preparando a los usuarios para posibles escenarios dentro de sus funciones. El uso de herramientas como las plataformas E-Learning nos permiten distribuir cursos y capacitaciones asegurando que el eslabón más débil de la empresa ha sido reforzado. El reto para las organizaciones consiste en asegurar siempre la información, quienes la usan, como se distribuye y almacena y la constante revisión de este ciclo de forma que los usuarios no sean una brecha de seguridad y se conviertan en una herramienta para la prevención de incidentes de seguridad que afecten la estabilidad económica y reputacional de las empresas.

Referencias bibliográficas

(19 de 11 de 2019). Obtenido de Gepeese: http://www.finanzasparatodos.es/gepeese/es/inicio/laEconomiaEn/laHistoria/revolucion_industrial.html

27001, I. (29 de 10 de 2015). SGSI. Obtenido de SGSI: https://www.pmg-ssi.com/2015/10/clasificar-incidentes-norma-iso-27001/

Coveware. (19 de 12 de 2018). Squarespace. Obtenido de https://static1.squarespace.com/static/5ab16578e2ccd10898976178/t/5c4675dbaa4a995fe6badb80/1548121568515/Coveware+Global+Ransomware+Marketplace+Report+-+2018+Q4.pdf

El Periodico. (05 de 07 de 2019). Obtenido de https://elperiodico.com.gt/inversion/2019/07/05/tigo-fortalece-seguridad-de-datos/

Institute, S. (11 de 12 de 2018). Obtenido de https://www.sans.org/reading-room/whitepapers/awareness/paper/34385

MediaClick. (19 de 06 de 2019). MediaClick. Obtenido de MediaClick: https://www.mediaclick.es/blog/cual-es-la-edad-de-los-usuarios-de-las-redes-sociales/

Merriam Webster. (03 de 26 de 2016). Obtenido de "Simple Definition of profess": merriam-webster.com

OSI. (05 de 12 de 2018). Obtenido de OSI: https://www.osi.es/es/actualidad/blog/2018/12/05/sabias-que-el-95-de-las-incidencias-en-ciberseguridad-se-deben-errores

Techradar. (22 de 10 de 2019). Obtenido de https://www.techradar.com/best/best-online-learning-platforms

Zimmermann, K. A. (2019). Obtenido de https://www.livescience.com/20718-computer-history.html

Sobre el autor:

Ingeniera en sistemas por la Universidad Mariano Gálvez con 15 años de experiencia en distintas áreas de TI incluyendo telecomunicaciones e infraestructura. Analista de Seguridad de la información en entidades bancarias y actualmente en empresas de alimentos y bebidas. Estudiante de maestría en seguridad de la información y certificada como auditor líder de seguridad de la información ISO 27001:2013 (IS, AU y TL)

CyberSecurity
Información & Privacidad

Implementación de buenas prácticas en los proyectos de tecnología: un reto más allá de las metodologías

Implementation of good practices in technology projects

Melvin Daniel García
email: melvingar@gmail.com
Linkedin: melvin-garcia-79113971
Recibido:19/enero/2019. Revisado: 23/febrero2020. Aprobado: 14/marzo/2020.
Disponible en internet el 10 de Abril de 2020

Resumen: Hoy en día, las organizaciones requieren de estrategias que permitan establecer mecanismos de transición de un modelo tradicional, a un esquema denominado "transformación digital". Su principal objetivo es integrar tecnologías que apoyen a los procesos y a las áreas de la organización, generando valor en los clientes tanto internos como externos. Por ello, no es extraño que las organizaciones planteen una serie de preguntas en las que se cuestionan y reflexionan respecto a dos concepciones ¿Por qué es importante que la organización desarrolle cambios digitales? y ¿Cuál es el impacto a nivel de las Tecnologías de la Información?

Palabras Claves: Transformación Digital, objetivos, alcances, proyectos.

Abstract: Today, organizations affected by strategies that establish transition mechanisms from a traditional model, a scheme, called "digital transformation". Its main objective is to integrate technologies that support the processes and areas of the organization, generating value for both internal and external customers. Therefore, it is not strange that organizations pose a series of questions in which they question and reflect on two concepts. Why is it important for the organization to develop digital changes? And what is the impact at the Information Technology level?

Desarrollo:

Los proyectos de transformación digital requieren del esfuerzo de toda la organización para establecer estrategias que deben estar enmarcadas desde la alta gerencia hasta los niveles operativos de la institución. Según el Pulse of the Profession® indica que "las organizaciones desperdiciaron casi el 12% del gasto de inversión en proyectos, debido a un desempeño deficiente" (PMI, 2019), por lo tanto, las organizaciones deben establecer proyectos que se alineen a la estrategia organizacional, sin perder el vínculo con la tecnología. Según (Forbes, 2018), indica que "el 80% de las organizaciones se ha sometido a una trasformación significativa con tecnología disruptiva, y solo el 25% de esas iniciativas ha producido beneficios tangibles con respecto a sus objetivos originales".

¿Por qué fallan los proyectos? Principalmente fallan por tres aspectos. El primero, falta del establecimiento del alcance, el cual debe alinearse a la estrategia de la organización. Todo proyecto que no esté alineado no representará valor para la institución. El segundo elemento por el cual fallan los proyectos se debe a la mala planificación del tiempo, esto repercute en los recursos asignados teniendo sobrecarga de trabajo, personal no capacitado, entregas fuera de los horarios laborales, entre otros. El tercer componente del por qué fallan los proyectos,

se debe a una estimación sobre dimensionada o por debajo de lo que se requiere en el presupuesto, lo que termina afectando la calidad de los entregables, cierre de proyectos o de fases por falta de fondos en su ejecución.

Otros componentes que son importantes destacar para el éxito de un proyecto, es la capacidad de dirección y buenas prácticas de proyectos, esto involucra la capacitación en gestión de proyectos, implementación de nuevas tecnologías, análisis de procesos, desarrollo de habilidades para el director de proyectos y el equipo, tales como: liderazgo, trabajo en equipo, negociación, relajación, inteligencia emocional, entre otros. La implementación de proyectos de tecnología implicará el establecimiento de mecanismos que evidencien los niveles de madurez en la organización, tanto a nivel de TI como a nivel de proyectos, permitiendo así que la organización establezca mecanismos de innovación, fortaleciendo la incorporación de buenas prácticas de dirección de proyectos, marcos de trabajo, estándares, tales como los enfoques ágiles, predictivos o bien el resultado de modelos híbridos.

La guía del Project Management Body of Knowledge (PMBoK®, del Project Management Institute PMI®), establece las buenas prácticas en la dirección de proyectos, recomendando incorporar herramientas y técnicas para completar 49 procesos de dirección de proyectos, los cuales se clasifican en 10 áreas de conocimiento y 5 grupos de procesos.

Según el (PMBoK, 6th ed.) un proyecto “es un esfuerzo temporal destinado para crear un único producto, servicio o resultado”, dicho de esta manera la implementación de proyectos de transformación digital nos llevará a razonar no solamente en proyectos sino en la incorporación de programas y portafolios de proyectos. En este caso, PMI define un programa como “un grupo de proyectos relacionados, subprogramas y actividades de programas cuya gestión se realiza de manera coordinada para obtener beneficios que no se obtendrían si se gestionarán de forma individual”, dicho de esta manera, el programa centrará sus esfuerzos en generar dependencias entre proyectos, implementará mecanismos para reducir costos, evaluará el riesgo de manera integral para mitigarlo y en la manera de lo posible eliminarlo.

En este sentido, un programa de transformación digital involucrará proyectos tales como: Dispositivos interconectados, Inteligencia Artificial, Big Data, Blockchain, impresión 3D, aprendizaje autónomo, tecnologías emergentes, redes, seguridad a nivel de hardware, software, de base de datos, entre otros. Una de las cosas que este tipo de proyectos determina es la capacidad de adaptarnos al cambio y es aquí donde surge el concepto de proyectos híbridos, donde se adaptan procesos de proyectos predictivos con ceremoniales de proyectos ágiles como el marco de trabajo de SCRUM®.

Según la guía de SCRUM es “un marco de trabajo simple que promueve la colaboración en los equipos para lograr desarrollar productos complejos” (Ken Schwaber, Jeff Sutherland, 2019), el principal propósito es incorporar la adaptabilidad y la respuesta al cambio, se basa en el principio de la hipótesis y el establecimiento de modelos empíricos, los equipos son autogestionados. Involucra 5 eventos importantes, 3 artefactos y 3 roles, permitiendo así al líder del proyecto, intervenir en cualquier etapa, tomar decisiones en conjunto con el equipo de trabajo, involucrar al cliente y a los demás interesados.

La implementación de cualquier proyecto de tecnología, requiere del establecimiento de buenas prácticas en dirección de proyectos, el departamento de TI debe involucrar prácticas como gestión del alcance de proyectos, o bien, gestión de programas a través de mecanismos como SCRUM escalado, sin olvidar que es necesaria la incorporación de habilidades de la era digital como: la ciencia de datos, mentalidad innovadora, conocimientos de seguridad y privacidad, conocimientos de cumplimiento de normas y regulaciones, capacidad para tomar decisiones basadas en datos y liderazgo colaborativo.

Referencias bibliográficas

Guía de los Fundamentos para la Dirección de Proyectos (PMBoK® Guide) 6ª. Edición . ISBN-13: 978-1628251845

ICB4 – IPMA Individual Competence Baseline for Project Management ISBN-13: 978-8888198392

Transformación digital para empezar la disrupción corporativa: contexto, etapas y agentes de cambio de la transformación digital. Autor: Andrés Vrant. The INK Publishing; Edición: 1 (25 de febrero de 2019). ASIN: B07P9T7MZQ

Lidera la Transformación Digital con éxito: Guía práctica y operativa sobre cómo abordar la Transformación desde IT. Autor: Mario Cortés Flores. ASIN: B08241Z33T

Project Management: An Essential Guide for Beginners Who Want to Understand Agile, Scrum, Lean Six Sigma, Kanban and Kaizen When Applied to Managing Projects. Autor: Wade Golden. ISBN: 978-1-64748-219-0

Sobre el autor:

Melvin García es especialista en el área de análisis, diseño, programación e implementación de soluciones informáticas, e-learning, comercio electrónico, diseño web, proyectos de tecnología y empresarial. Posee varias certificaciones a nivel internacional como IPMA Nivel D; Scrum Master; Legos Serious Play; es par evaluador certificado por la Agencia Centroamericana de Acreditación de Arquitectura y de Ingeniría – ACAAI, así como, par evaluador del Consejo de Acreditación de la Enseñanza de la Ingeniería A. C. (CACEI).

Ha brindado servicios en instituciones educativas, pequeñas y medianas empresas, organizaciones gubernamentales, ha dirigido proyectos tanto en empresas nacionales como internacionales, catedrático de varias universidades y director de la Maestría en Gestión y Dirección de Proyectos.

Ha participado como miembro de la Junta Directiva del PMI Capítulo Guatemala y es miembro activo de la Comisión de Informática e Información de la SENACYT. Es conferencista internacional y ha hecho publicaciones en varios congresos con temas relacionado a proyectos predictibles y ágiles, tecnología educativa entre otros.

CyberSecurity
Información & Privacidad

Donaciones

Contraportada
$500.00

Portada Interior
$450.00

Pagina Interior (Especifica)
$400.00

Pagina Interior
$350.00

Media Página
$200.00

Mas Información

info@csecmagazine.com

CyberSecurity
Información & Privacidad

LINEAMIENTOS PARA LA PUBLICACIÓN DE ARTÍCULOS

I. Lineamientos Generales

Los artículos 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.

Las cuales deberán atender los siguientes lineamientos:

1. Deben 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, formato Word, letra tamaño 12, tipo Arial, interlineado 1.5, márgenes de 3 centímetros, hoja tamaño carta.

4. Los artículos deberán ser entregados en formato digital al correo de la asistente de editores cfa@csecmagazine.com

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 (Opcional): 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.

Resultados de discusión (Opcional). 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.

CyberSecurity
Información & Privacidad

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 2,020.

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 de tu autoría, envíanos tu resumen para poder analizarlo y posteriormente publicarlo.

cfa@csecmagazine.com

Magazine

CyberSecurity

Información & Privacidad