Volumen 1. Número 2. Serie A

ISBN: 978-99939-0-055-9

ISSN: 2708-1141

CyberSecurity

Información & Privacidad

Converciencia Guatemala

Resumen de Conferencias

Call Centers de Guatemala

Una perspectiva de Ciberseguridad en tiempos de COVID-19

Alcanzando la idempotencia

de las tecnologías de información con Ansible

Ransomware en el Sector Salud

Estudio sobre el impacto de los ataques de Ransomware

Normativa JM 42-2020 en Guatemala

Su implementación en las PyMES

Ley de Protección de Datos

Elementos básicos para una propuesta

CyberSecurity
Información & Privacidad

CyberSecurity
Información & Privacidad

Proyecto de:

Asociación Universitaria en Ciencias de la Investigación
-AUCI Guatemala-

Con financiamiento de:

INCIBE GT
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ISBN: 978-99939-0-055-9
9 789993 900559

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:

Ing. Darwin Fuentes

Enero – Abril 2021

Nota del editor

La vida florecerá a pesar de las dificultades, hoy queremos agradecer a todas personas, profesionales y demás que apoyaron el proceso que llevó la adaptación en esta pandemia, desde los médicos, enfermeros, salubristas, bomberos y muchas más personas; y en temas de tecnología a todo el equipo de TI que optimizó los recursos en algunos casos y en otros apoyó la adquisición de nueva tecnología para proteger los servicios requeridos en las empresas.

Ha pasado ya 1 año desde que decidimos dar la oportunidad a las autoras y autores latinoamericanos para publicar artículos de actualidad que sirvieran de base para futuras investigaciones, hoy los logros se sobrepasaron y estamos muy complacidos por ello, no contamos con premios para cada uno de nuestros autores, pero queremos agradecer a todos ellos ya que sin sus investigaciones, artículos o estudios este espacio digital no tendría razón de ser, ustedes son los verdaderos agentes de cambio y ejercen una gran influencia en aspectos de tecnologías de la información y ciberseguridad en esta sociedad digital. Somos conscientes que la investigación en tecnologías y ciberseguridad en países de Latinoamérica es muy baja pero también sabemos de las oportunidades a futuro que ofrece esta ciencia en crecimiento.

Estamos convencidos que este nuevo año traerá oportunidades para todos nosotros y de parte de Cybersecurity Magazine les invitamos a participar en nuestras 3 ediciones planificadas, las convocatorias a partir de este año son Permanentes por ello queremos agradecer el apoyo recibido por parte de INCIBE Guatemala con lo necesario para la publicación de los números de la revista en los distintos canales digitales.

Además invitarles a nuestro I Congreso de Investigación y Desarrollo que se llevará a cabo el 29 de enero con profesionales reconocidos a nivel latinoamericano que expondrán sus investigaciones en el área de tecnologías y ciberseguridad.

Reciban nuestro saludo.

Maria

CyberSecurity
Información & Privacidad

INDICE

CyberSecurity
Información & Privacidad

Resumen de Conferencia

CONVERCIENCIA GUATEMALA

Secretaría Nacional de Ciencia y Tecnología

GOBIERNO de GUATEMALA
DR. ALEJANDRO GIAMMATTEI

SECRETARÍA NACIONAL DE CIENCIA Y TECNOLOGÍA

Converciencia Guatemala

Secretaría Nacional de Ciencia y Tecnología
sfdeleon@senacyt.gob.gt
Aprobado: 10/diciembre/2020.
Disponible en internet el 1 de enero de 2020

Resumen: El evento de Converciencia de la Secretaría Nacional de Ciencias y Tecnología de Guatemala se llevó a cabo del 21 de octubre al 27 de noviembre del 2020, este es el encuentro de la sociedad con científicos guatemaltecos que trabajan en investigación dentro y fuera de Guatemala, esto con el objetivo de impulsar efectivamente el desarrollo de la ciencia, tecnología y la innovación en Guatemala, las actividades consistieron en la convergencia de científicos guatemaltecos que trabajan en investigación y docencia dentro y fuera del país, desde el inicio de Converciencia en el año 2005 mas de 70 científicos han participado, dentro de los sectores participantes se encuentran niñez, adolescencia, estudiantes universitarios, profesores, investigadores , autoridades universitarias, funcionarios públicos, empresarios y público interesado en aumentar sus conocimientos en los distintos ejes como sociedad digital, salud, energía, educación, seguridad alimentaria, medio ambiente y cambio climático entre otros. El evento se desarrolló en las distintas plataformas virtuales del Senacyt teniendo como sedes oficiales a: La Universidad del Valle de Guatemala (Centro de Estudios Atitlán -CEA), Escuela de Estudios de Postgrado de la Facultad de Ingeniería de la Universidad San Carlos de Guatemala, Centro Universitario de Petén Universidad San Carlos de Guatemala, Instituto de Investigaciones Químicas y Biológicas de la Universidad San Carlos de Guatemala, UNESCO (United Nations Educactional, Scientific and Cultural Organization), Organization for Woman in Science for the Develping Word (OWSD), Universidad Galileo, University of Glassgow, Northumbria University Newcastle, Universidad Rafael Landívar de Guatemala, Facultad de Ciencias Químicas y Farmacia de la Universidad San Carlos de Guatemala, Universidad del Valle Central, Centro Universitaria de Zacapa Universidad San Carlos de Guatemala, Centro Universitario de Retalhuleu Universidad de San Carlos de Guatemala, CENAME, APEVIHS, Centro Universitario de Izabal CUNIZAB Universidad San Carlos de Guatemala.

Palabras Claves: ciencia, investigación, desarrollo, tecnología, innovación.

Abstract: The Converciencia event of the Secretaría Nacional de Ciencias y Tecnología de Guatemala was held from October 21 to November 27, 2020, this is the society's meeting with Guatemalan scientists who work in research inside and outside of Guatemala, this In order to effectively promote the development of science, technology and innovation in Guatemala, the activities consist of the convergence of Guatemalan scientists working in research and teaching within and outside the country, since the beginning of Converciencia in 2005 more of 70 scientists have participated, within the sectors that are found are children, adolescents, university students, professors, researchers, university authorities, public officials, businessmen and the public interested in increasing their knowledge in the different axes as a digital society, health, energy, education, food security, environment and climate change among others. The event was developed in the different virtual platforms of SENACYT having as official headquarters: La Universidad del Valle de Guatemala (Centro de Estudios

Atitlán -CEA), Escuela de Estudios de Postgrado de la Facultad de Ingeniería de la Universidad San Carlos de Guatemala, Centro Universitario de Petén Universidad San Carlos de Guatemala, Instituto de Investigaciones Químicas y Biológicas de la Universidad San Carlos de Guatemala, UNESCO (United Nations Educactional, Scientific and Cultural Organization), Organization for Woman in Science for the Develping Word (OWSD), Universidad Galileo, University of Glassgow, Northumbria University Newcastle, Universidad Rafael Landívar de Guatemala, Facultad de Ciencias Químicas y Farmacia de la Universidad San Carlos de Guatemala, Universidad del Valle Central, Centro Universitaria de Zacapa Universidad San Carlos de Guatemala, Centro Universitario de Retalhuleu Universidad de San Carlos de Guatemala, CENAME, APEVIHS, Centro Universitario de Izabal CUNIZAB Universidad San Carlos de Guatemala

Desarrollo:

La inauguración de Converciencia se llevó a cabo el 21 de octubre a las 9 de la mañana por parte de Magíster Ana Judith Chan Orantes, Secretaría Nacional de Ciencia y Tecnología, Dra. Susana Arrechea, Coordinadora Internacional de la Red Internacional de Ciencia, Tecnología e Innovación de Guatemala, Lic. Guillermo Castillo, Vicepresidente de la República y Presidente del Consejo Nacional de Ciencia y Tecnología, Lic. Marcos Antil, Emprendedor Tecnológico, Conferencia Inaugural e Ing. Alejandro Vidal, Presidente Comisión de Innovación y Emprendimiento del Sistema Nacional de Ciencia y Tecnología . Las actividades de Converciencia 2020 en esta edición se realizaron de forma virtual, con el objetivo de propiciar el intercambio entre científicos guatemaltecos que residen dentro y fuera del país, para compartir sus experiencias, así como dar a conocer los resultados de sus estudios y profundizar sobre el estado actual de la ciencia. Se busca promover la vinculación entre los diferentes sectores, dirigido a jóvenes universitarios, investigadores, científicos y púbico en general interesado en la ciencia y tecnología. Para esta edición, se han considerado 7 temáticas a abordar siendo: energía, medio ambiente, cambio climático, seguridad alimentaria, salud, educación y sociedad digital y se contará con la participación de 37 conferencistas.

La primera semana contó con la Conferencia Inaugural que fue impartida por Marcos Antil quien reside en Estados Unidos, en seguida las conferencias de Cristian Manuel Ovalle Rodas desde Francia, con Taller: Arte gráfico en la preparación de artículos científicos. Julio Gallegos Alvarado quien reside en España, compartio Astronomía en la Enseñanza de la Matemática. Pedro Morales-Almazan quien reside en Estados Unidos con Círculo Matemático. Kleinsy Yudrani Bonilla Landaverry, Liseth Carolina Pérez Alvarado, Bárbara Moguel Rodríguez quienes residen en Brasil, Alemania y México con Brechas de Género en la Ciencia Guatemalteca: Reflexiones sobre la realidad y propuesta de soluciones, Gabino Rafael Fernández Botrán quien reside en Estados Unidos con Avances en la lucha contra COVID-19 - Factores de riesgo, Patogénesis y Laboratorio. José María de la Roca quien reside en Chiapas México con Reunión de Coordinación entre interesados en investigaciones en Psicología. Rodrigo Castañeda Molina quien reside en Guatemala con Sinergia de compuestos para candidatos farmacológicos a complicaciones diabéticas. Pedro Morales-Almazan quien reside en Estados Unidos con como la matemática nos da una mejor perspectiva del mundo. Jeffrey Roberto Reina García Salas quien reside en Estados Unidos Explorando vías de señalización celular alteradas en el cáncer de mama para el desarrollo de nuevas formas de terapia.César Augusto Azurdia Meza quien reside en Chile con el Foro: Desarrollo y Aplicación de Redes 5G en América Latina.

La semana 2 incluyo actividades con Gabino Rafael Fernández Botrán quien reside en Estados UnidosAvances en la lucha contra COVID-19 - Inmunología, Inmunización pasiva y activa. Vacunas en desarrollo. José Ramiro Cruz López quien reside en Estados Unidos Mortalidad materna en Guatemala - ¿se puede reducir a corto plazo?, Mabel Taracena quien reside en Estados Unidos con la conferencia de Recursos Digitales en la Ciencia e Investigación. Rándol José Rodríguez Rosales quien reside en Estados Unidos con Cambios en el patrón alimentario y salud de América Latina con enfoque en ciencia y tecnología de carbohidratos. Sussanne Carola Reyes García quien reside en Chile ¿La deficiencia de hierro en la infancia puede tener consecuencias neurobiológicas a largo plazo?, César Augusto Azurdia Meza quien reside en Chile ¿Cómo abordar el desafío de preparar un manuscrito científico?. Héctor Roderico Amado Salvatierra Guatemala Vigilancia Tecnológica e Inteligencia Competitiva, herramientas útiles en la Sociedad Digital.

Claudia Suseth Romero Oliva quien reside en Alemania "Diagnóstico ambiental histórico de lagos en Guatemala y perspectivas transdisciplinarias para su manejo integral. Gumercindo Armando Monzón Escobar quien reside en Guatemala con El aseguramiento de la información en épocas del COVID- 19. César Augusto Azurdia Meza quien reside en Chile con la conferencia ¿Qué es Internet de las Cosas y cómo cambiará nuestras vidas?. Leonel Enrique Aguilar Melgar quien reside en Suiza con De modelos compartimentales a modelos basados en agentes, un tour práctico sobre modelado y simulación. Josué Rodolfo Obregón Velásquez quien reside en Corea del Sur con Interpretación de Modelos de Machine Learning. Juan Esteban Gramajo quien reside en Francia Introducción al diseño de plataformas satelitales. José Ramiro Montealegre quien reside en Estados Unidos ¿Cuál es el Rol de la Tecnología Digital en la Recuperación Pospandemia?. Kleinsy Yudrani Bonilla Landaverry quien reside en Brasil participo en el Panel: Formación de la fuerza científica y de investigación en Guatemala. Sergio Alejandro Minera Rebulla quien reside en Reino Unido con Materiales compuestos: La magia detrás de la ingeniería aeroespacial. Juan Esteban Gramajo quien reside en Francia con la conferencia El futuro de la industria aeroespacial y estudiar en el extranjero, José Ramiro Montealegre quien reside en Estados Unidos con La Necesidad de Business Intelligence Después de COVID-19.

La semana 3 se llevaron a cabo las conferencias de Julio Gallegos Alvarado quien reside en España con Enseñanza de la Astronomía. Marlene Susana Arrechea Alvarado quien reside en Estados Unidos con el Taller de STEAM para niñas y niños en Guatemala. Patricia Noemí Lucki Z. quien reside en Guatemala con el tema Ciencia o magia. La respuesta de la ciencia a las emergencias. El Caso de la COVID-19 y los aprendizajes ganados. Kleinsy Yudrani Bonilla Landaverry quien reside en Brasil en el Panel: Diplomacia Científica: Oportunidades y Desafíos para Guatemala y su participación internacional en Ciencia y Tecnología. Claudia Suseth Romero Oliva quien reside en Alemania con el Taller corto interactivo: Lecciones actuales y pasadas. El legado de los sedimentos del Lago de Amatitlán a través del lente de la Paleo-ecotoxicología. Cristina Domínguez Hernández quien reside en Suiza con el Acceso a energía limpia, asequible y sostenible para todos: Un reto posible para Guatemala. Edward Mario Augusto Guerrero Gutiérrez de Guatemala Membranas para aplicaciones de energía limpia y renovable. Marlene Susana Arrechea Alvarado, Cristina Domínguez Hernández y Edward Mario Guerrero quienes residen en Estados Unidos, Suiza y Guatemala con el Taller: Tecnologías para energía renovable y su aplicación en comunidades rurales de Guatemala. La clausura de Converciencia se llevo a cabo el 27 de noviembre con la participacion de Guillermo

Castillo Reyes, Pedro Morales, Susana Arrechea, Rafael Fernández Botrán, Patricia Noemí Lucki, Modera: Ana Chan, Secretaría Nacional de Ciencia y Tecnología con el Conversatorio de cierre: Horizonte Científico: áreas de oportunidad de la Ciencia, Tecnología e Innovación para Guatemala.

La Secretaría Nacional de Ciencia y Tecnologia como órgano de coordinación, es la responsable de apoyar y ejecutar las decisiones que emanen del CONCYT y dar seguimiento a sus respectivas acciones, por medio de la utilización eficiente de los recursos financieros FONACYT. Asimismo, constituye el vínculo entre las instituciones que integran el SINCYT. Su misión es Fortalecer y articular el sistema nacional de ciencia y tecnología, por medio de la formulación, coordinación y ejecución de políticas que contribuyan al desarrollo económico y social del país. Su visión es ser la organización clave en la promoción y articulación de la ciencia, la tecnología y la innovación como elemento estratégico para el desarrollo.

Artículos

Call Centers de Guatemala: Una perspectiva de Ciberseguridad en tiempos de COVID-19

Guatemala Call Centers: A Cybersecurity Perspective intimes of COVID-19.

Luis Liapán
email: lliapani@miumg.edu.gt

Recibido:6/octubre/2020. Revisado: 22/octubre/2020. Aprobado: 23/noviembre/2020.
Disponible en internet el 1 de enero de 2021

Resumen: El objetivo de este estudio es concientizar acerca de la importancia de la ciberseguridad en estos tiempos de pandemia COVID-19, lo cual fue algo que tomó por sorpresa a la industria de call centers de Guatemala y su plan de continuidad de negocio no tenía contemplado el work from home. El estudio se llevó a cabo recolectando información de otros artículos relacionados al tema de la pandemia y el teletrabajo, también se hizo uso de los estándares internacionales ISO 27001, ISO 27032 y PCI DSS, así como también, se realizó una encuesta digital, haciendo uso del servicio de anuncios de Instagram, y se obtuvo una muestra de 75 personas que actualmente laboran en la industria de call centers de Guatemala. La finalidad de la encuesta es conocer si la industria en cuestión tiene implementadas políticas y buenas prácticas de ciberseguridad. Los resultados indican que solo el 33% de los call centers tienen implementadas políticas y buenas prácticas de ciberseguridad, aunque se destaca su compromiso y responsabilidad con los estándares ISO 27001 y PCI DSS, también se puedo evidenciar que el número de ciberataques aumenta cada año a nivel mundial y durante la pandemia el phishing ocupa el primer lugar con un 59%, seguido del ransomware con un 36%. En conclusión, los call centers de Guatemala no está prestando atención al tema de ciberseguridad, lo cual es preocupante ya que, debido a su modelo de negocio este tema debería de estar en su lista de prioridades, no se debe de ver como un gasto innecesario sino como una de las mejores inversiones que pueden realizar.

Palabras Claves: pandemia, concientización, ciberataques, teletrabajo, phishing, ransomware, buenas prácticas de ciberseguridad, trabajo desde casa.

Abstract: The objective of this study is to raise awareness about the importance of cybersecurity in these times of the COVID-19 pandemic, which was something that took the Guatemalan call center industry by surprise and its business continuity plan didn't have the work from home contemplated. The study was carried out by collecting information from other articles related to the topic of the pandemic and telecommuting, the international standards ISO 27001, ISO 27032 and PCI DSS were also used, as well as a digital survey, making use of the Instagram's ad service, a sample of 75 people who currently work in the call center industry in Guatemala was obtained. The purpose of the survey is to find out if the industry in question has implemented cybersecurity policies and good practices. The results indicate that only 33% of call centers have implemented cybersecurity policies and good practices, although their commitment and responsibility with the ISO 27001 and PCI DSS standards stand out, it can also be evidenced that the number of cyber attacks increases

every year worldwide and during the pandemic, phishing ranks first with 59%, followed by ransomware with 36%. In conclusion, the call centers in Guatemala are not paying attention to the cybersecurity theme, which is worrying since due to their business model, this theme should be on their priority list, it should not be seen as an unnecessary expense but as one of the best investments they can make.

Desarrollo:

El presente tema de investigación concierne a las malas prácticas de ciberseguridad en tiempos de COVID-19, tomadas en el sector de Call Centers y BPO (Business Process Outsourcing) de Guatemala, el cual está formado por empresas que prestan sus servicios a los grandes mercados en Estados Unidos, Canadá, Centroamérica, España, etc. Ofreciendo los servicios de soporte técnico, ventas, finanzas, seguros, entretenimiento, hospedajes, telecomunicaciones, entre muchos otros.

"Actualmente la industria está compuesta por empresas internacionales y nacionales, y cuenta con alrededor de 42,000 agentes (2019). Los empleos generados se dividen en servicios de voz y no voz. El primero es alrededor de 90 por ciento, de los cuales se calcula que el 67 por ciento son empleos bilingües, que requieren de un conocimiento del idioma inglés; un 30 por ciento de los empleos son en español y un 3 por ciento en otros idiomas: francés, alemán, portugués" (AGEXPORT, 2019).

Esta industria, es una de las principales generadoras de empleo en Guatemala, a raíz del crecimiento exponencial de la tercerización de servicios a nivel mundial.

Para analizar esta problemática, cabe mencionar que, dicha industria maneja información sensible de las personas, y por lo tanto, las empresas que solicitan sus servicios exigen un alto nivel de seguridad de la información, con el fin de evitar el robo, alteración y acceso no autorizado a la misma. Adicionalmente, hay otro tipo de empresa que requiere el estándar PCI-DSS (Payment Card Industry Data Security Standard) debido a que se toman pagos por medio de tarjeta de crédito o débito.

Derivado de la Pandemia Covid-19, la cual es una enfermedad infecciosa y su principal fuente de propagación es el contacto con otra persona infectada por el virus, la Organización Mundial de la Salud (OMS) recomendó, como medida preventiva el distanciamiento físico, con un mínimo de distancia de un metro entre una persona y otra. Dicha medida tanto preventiva como necesaria, obligo a los call centers a realizar cambios en sus operaciones para mitigar el riesgo de contagio entre sus empleados, lo cual los llevo a la transición del trabajo en sitio al ahora famoso "work from home".

El work from home ha venido acompañado de malas prácticas de ciberseguridad, esto debido a que estas empresas se han enfocado más en la continuidad de sus operaciones, dejando su

ciberespacio, no solo vulnerable, sino también expuesto a todos aquellos vectores de ataque que pueden causar un daño de alto impacto e inseguridad en el mismo.

Por lo tanto, el presente artículo tiene como finalidad, concientizar acerca de la importancia de la ciberseguridad en estos tiempos difíciles de la pandemia COVID-19, en donde los call centers han tenido que reinventar sus operaciones, tomando medidas reactivas para evitar la suspensión de las mismas. Así como también, brindar buenas prácticas y/o recomendaciones de ciberseguridad para mitigar los riesgos derivados de la nueva modalidad laboral; trabajo desde casa.

Materiales y Métodos

Con el fin de abordar de una mejor manera la problemática del presente estudio, la metodología se dividió en tres partes; en la primera parte se recolecto información y datos obtenidos de artículos publicados por diferentes autores, en relación al tema de ciberseguridad, pero específicamente, se tomaron aquellos artículos enfocados a la ciberseguridad en tiempos de pandemia COVID-19 y todo lo relacionado a la nueva modalidad "trabajo desde casa". Dichos artículos fueron consultados en la plataforma Google académico.

La segunda parte de la metodología se llevó a cabo con base a los estándares internacionales: ISO 27001 para la seguridad de la información, ISO 27032 para todo lo relacionado a la ciberseguridad, y por último, pero no menos importante, PCI-DSS para toda la parte de seguridad que concierne a pagos con tarjeta de crédito y/o débito. Dichos estándares fueron utilizados para hacer una comparativa entre las buenas y malas prácticas que se están realizando por la industria en cuestión.

"Podemos decir que la Ciberseguridad es la capacidad de resistir, con un nivel determinado de fiabilidad, a toda acción que comprometa la disponibilidad, autenticidad, integridad, o confidencialidad de los datos almacenados o transmitidos, o de los servicios ofrecidos" (Ballestero, 2020).

La tercera parte de la misma, se llevó a efecto realizando una encuesta digital, para ello se utilizó el servicio de anuncios de Instagram. Cabe mencionar que, se recurrió a este tipo de servicios debido a la situación actual y a la nueva modalidad de trabajo. El público objetivo fueron todas aquellas personas que actualmente laboran en cualquiera de los diferentes call centers de Guatemala. El total de encuestas recibidas/contestadas fue de 75, lo cual representa un 0.018% del total de agentes contabilizados por AGEXPORT en el año 2019.

Resultados

Luego de analizar las encuestas recibidas y depurar la información obtenida, se pudo observar que, el 20% de los encuestados son de la generación X (entre 40 y 58 años), 65% de la generación Y (entre 24 y 39 años) y un 15% con una edad entre 18 y 23 años. Según (Gonzalez, 2017) "la generación X está comprendida por todas aquellas personas nacidas entre los años 1965 y 1979, la generación Y por aquellas personas nacidas entre los años 1980 y 1999, y la generación Z por aquellas personas nacidas a partir del año 2000". Ver tabla 1.

Del total de 6 call centers, se pudo identificar que, 2 de ellos (33%) cuentan con políticas de seguridad de la información, imparten cursos a sus empleados sobre concientización de ciberseguridad y cuentan con estrictos controles PCI, 3 (50%) cuentan con políticas de seguridad de la información y controles PCI, y 1 (17%) está en proceso de implementación de políticas de seguridad de la información. Cabe mencionar que por motivos de confidencialidad, el nombre de los mismos no será indicado, por lo tanto, se identificaran como: call center 1, 2, 3, 4, 5 y 6. Ver tabla 2.

De las 75 encuestas recibidas, 30 eran de empleados del call center 1, 5 eran del call center 2, 12 eran del call center 3, 9 eran el call center 4, 8 eran del call center 5 y 11 eran del call center 6. Cabe mencionar que se recibieron 12 encuestas adicionales, no obstante, las mismas estaban incompletas, por lo tanto, fueron descartadas para este estudio. Ver tabla 3.

"De acuerdo al reporte anual del Centro de Denuncias de Delito de Internet de 2019, los ataques cibernéticos incrementan gradualmente cada año" (Gamboa, 2020). Figura 1, y en la figura 2 se muestra una representación gráfica porcentual de los ciberataques más comunes durante la pandemia COVID-19.

Tabla 1: Perfil de los encuestados (hombres y mujeres) en base al tipo de generación
*Porcentaje por cada una de las generaciones.
Fuente: Elaboración propia

Tipo de generación	Porcentaje
X	20%
Y	65%
Z	15%

Tabla 2: Call centers que cuentan o no con políticas y controles, responde afirmativamente (si), negativamente (no) o en proceso, ante los enunciados mostrados (A). Porcentaje de call centers que tienen o no implementadas políticas, según las encuestas (B). Y porcentaje de call centers por cada enunciado (C)
Fuente: Elaboración propia

A

	Politicas de seguridad de la información	Politicas de Ciberseguridad	Controles PCI
Call center 1	Si	No	Si
Call center 2	En proceso	No	No
Call center 3	Si	Si	Si
Call center 4	Si	No	Si
Call center 5	Si	No	Si
Call center 6	Si	Si	Si

B

	Cantidad de call centers	Porcentaje
Cuentan con políticas de seguridad de la información, politicas de ciberseguridad, y controles PCI	2	33%
Cuentan con politicas de seguridad de la información y controles PCI	3	50%
Sus politicas están en proceso	1	17%

C

	Cantidad de call centers	Porcentaje
Cuentan con políticas de seguridad de la información	5	83%
Cuentan con politicas de ciberseguridad	2	33%
Cuentas con controles PCI	5	83%

Tabla 3: Porcentaje de encuestas recibidas por cada call center
Fuente: Elaboración propia

	Numero de encuestas	Porcentaje
Call center 1	30	40%
Call center 2	5	7%
Call center 3	12	16%
Call center 4	9	12%
Call center 5	8	11%
Call center 6	11	14%

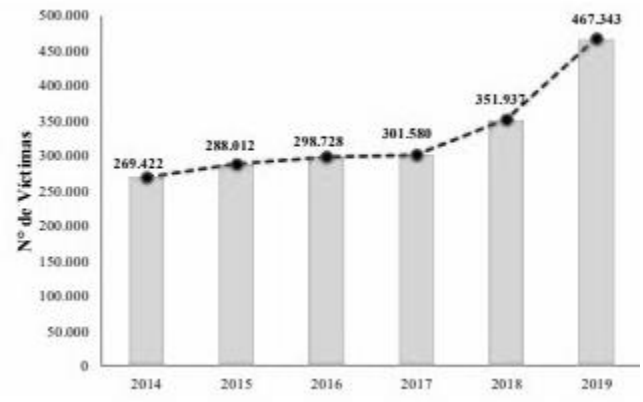

Figura 1: Número de víctimas de ciberataques en los últimos 6 años a nivel mundial.
Fuente: (Gamboa, 2020)

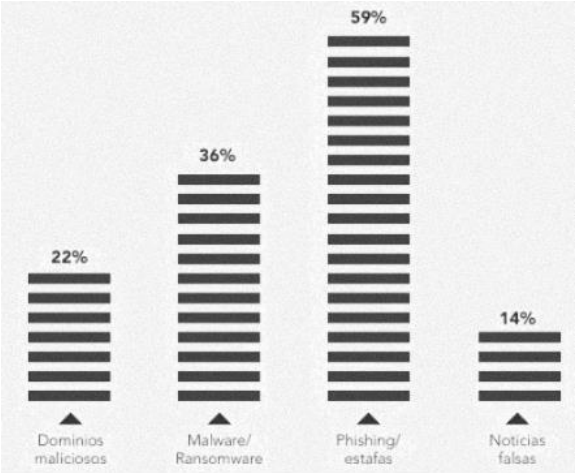

Figura 2: Ciberataques más comunes durante la pandemia COVID-19
Fuente: (INTERPOL, 2020)

Discusión

En el presente estudio se puede observar que, la taza de call centers que cuenta con políticas de seguridad de la información y controles PCI es alta, lo cual destaca el compromiso y responsabilidad de los mismos ante los estándares ISO 27001 y PCI DSS respectivamente. No obstante, el tema de ciberseguridad es preocupante, ya que, según el estudio solo 2 (33%) call centers cuentan con políticas de ciberseguridad.

Por otra parte, se pudo evidenciar que el número de ciberataques aumenta cada año, en el 2019 la cifra llego a 467,343 ataques cibernéticos, siendo esta la mayor cifra registrada en los últimos 6 años. Entre los ciberataques más comunes durante la pandemia COVID -19 se encuentran: Dominios maliciosos, Malware/Ransomware, Phishing. El Phishing ocupa la primer posición con un 59%, seguido de Malware/Ransomware con un 36%, según datos obtenidos de la página oficial de la INTERPOL.

Actualmente, toda empresa independientemente de su tamaño es candidata a ser víctima de un ciberataque, como el robo de información, la encriptación de datos, el bloqueo de accesos, el borrado de información, entre otros. Esto podría provocar que un call center quedará totalmente paralizado por un tiempo indefinido, y por consiguiente, causar grandes pérdidas económicas.

Por lo tanto, se recomienda a la industria de call centers que empiecen a implementar sus políticas y buenas prácticas de ciberseguridad, basándose en el estándar internacional ISO 27032, el cual les permitirá mitigar todos aquellos riesgos que podrían ocasionar daños de alto impacto en su ciberespacio.

Dentro de las recomendaciones y buenas prácticas de ciberseguridad que deben tomar en consideración, resalta el tema de concientización; el educar y/o capacitar a los empleados sobre las diferentes amenazas, la forma en que se presentan y cómo actuar ante una situación donde puedan estar siendo víctimas de un ciberataque, ayudara a mitigar en gran escala el riesgo de ser víctimas de phishing, ransomware, ingeniería social y muchos otros ciberataques, ya que los usuarios (empleados) son la primer y mejor línea de defensa, pero también, el eslabón más débil. Todo dispositivo (endpoint) con acceso a la red interna de la organización debe ser propiedad de la empresa, con el objeto de tener un control total sobre el mismo, evitar el BYOD (Bring Your Own Device) debido a que esto representa una brecha muy grande de seguridad. Todas las computadoras deben ser encriptadas antes de ser entregadas a los empleados remotos. Hacer uso de VPN para conectar a la red interna a cada colaborador de la empresa que está trabajando desde casa. Utilizar contraseñas robustas y que todos los trabajadores remotos tengan configurado la autenticación multifactor (MFA), lo cual brindara un acceso autenticado a todas las aplicaciones y sistemas de la organización. Instalar actualizaciones y parches para que los endpoints y sistemas estén lo más actualizado

posible y esto no represente una brecha más de seguridad. Contar con servicios que permitan monitorear los sistemas, la red, las aplicaciones y a los usuarios de manera periódica.

Estas empresas deberían de considerar la posibilidad de pagar un servicio de internet a cada empleado, evitando así que se conecten a una red familiar donde se desconoce la finalidad de la misma, esto permitiría que el empleado se conectara a una red estrictamente laboral, para ello el empleado deberá comprometerse a ser la única persona que estará conectada a esa red, firmando una carta de compromiso.

Conclusiones

El arribo del COVID-19 fue algo sorpresivo para la industria de los call centers, y debido a la naturaleza de sus operaciones, su plan de continuidad de negocio no contemplaba ni la mínima posibilidad de la modalidad "work from home". Independientemente de la pandemia, los call centers son empresas que no pueden operar sin una conexión a internet, el internet es uno de sus servicios críticos, por lo tanto, están más expuestos a ser víctimas de los diferentes vectores de ataque, los cuales buscan una vulnerabilidad para provocar daño, por consiguiente, la ciberseguridad debe ser un tema prioritario para esta industria. No obstante, es preocupante el hecho de que únicamente la tercer parte de los mismos tiene implementadas políticas de ciberseguridad, ya que su ecosistema siempre está expuesto debido a su modelo de negocio.

La concientización es de suma importancia en el tema de ciberseguridad, es un arma de defensa contra el cibercrimen. Los ataques de Phishing, como se pudo observar en este estudio, son los más comunes y han tenido éxito debido a la falta de programas de capacitación al usuario, lo cual le permita conocer e identificar este tipo de ataques y cómo actuar ante los mismos.

Por último, el regreso a "la nueva a la nueva normalidad" genera incertidumbre, es imposible saber con exactitud el fin de la pandemia. El COVID-19 no vino a cambiar la reglas del juego, sino el juego como tal, pero todo va a depender de la postura que tomen los call centers ante este nuevo mundo; mas conectado, sin fronteras, pero al mismo tiempo, más vulnerable y más expuesto al riesgo, cibernéticamente hablando. Ante esta incertidumbre, sería estupendo que la industria de call centers creará una estrategia de ciberseguridad, haciendo una convergencia de los tres estándares internacionales mencionados en este estudio, y porque no, incluir otros que pudieran ayudar al fortalecimiento de la misma.

Referencias bibliográficas

AGEXPORT, G. (2019). AGEXPORT Guatemala. Obtenido de https://export.com.gt/sector/contact-center-bpo

Ballestero, F. (28 de Abril de 2020). LA CIBERSEGURIDAD EN TIEMPOS DIFÍCILES¿Nos ocupamos de ella o nos preocupamos por ella? Obtenido de http://www.revistasice.com/index.php/BICE/article/view/6993/6993

Cano, J. J. (10 de Junio de 2020). Seguridad de la información y ciberseguridad empresarial. Obtenido de https://sistemas.acis.org.co/index.php/sistemas/issue/view/14/11

Gamboa, J. L. (Agosto de 2020). IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA Y CIBERSEGURIDAD EN EL MUNDO ACTUAL. Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/8668

Gonzalez, B. (26 de Abril de 2017). Diferencias entre Baby Boomers y las generaciones XYZ. Obtenido de http://begonagonzalez.com/generacionxyz/

Hern, A. (13 de Marzo de 2020). Covid19 could cause permanent shifttowards home. Obtenido de http://www.miamidadetpo.org/library/2020-03-13-uk-covid19-could-cause-permanent-shift-towards-home-working.pdf

INTERPOL. (4 de Agosto de 2020). Ciberdelincuencia: efectos de la COVID-19. Obtenido de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

Muñoz, C., Pérez, B., & Navarrete, M. d. (30 de Abril de 2020). LAS EMPRESAS ANTEL EL COVID-19. Obtenido de https://www.editorialeidec.com/revista/index.php/GISST/article/view/83/64

Oneto, A. (23 de Julio de 2020). COVID-19 El rol del Directorio: de los peligros a las oportunidades. Obtenido de https://scioteca.caf.com/handle/123456789/1616

Oneto, A. (24 de Junio de 2020). COVID-19: Continuidad del Negocio, Gestion de Crisis y Gobierno Coorporativo. Obtenido de https://scioteca.caf.com/handle/123456789/1596

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

Santillán, W. (20 de Mayo de 2020). EL TELETRABAJO EN ELCOVID-19. Obtenido de http://cienciamerica.uti.edu.ec/openjournal/index.php/uti/article/view/289/451

Wyplosz, C. (24 de Abril de 2020). COVID ECONOMICS VETTED AND REAL-TIME PAPERS. Obtenido de http://fadinger.vwl.uni-mannheim.de/Research_files/CovidEconomics9.pdf

Sobre el autor:

Ingeniero en Sistemas de Información egresado de la Universidad Mariano Gálvez de Guatemala. En los últimos ocho años ha laborado con 2 BPO de Guatemala; 5 años en el área de operaciones y 3 años en el área de informática. Actualmente laborando en Telus International como Analista de Soporte Técnico, brindando soluciones de impacto global para los diferentes sitios con los que cuenta la organización a nivel mundial. Recientemente finalizó la Maestría en Seguridad de la Información en la Universidad Mariano Gálvez de Guatemala. Apasionado por la seguridad informática.

Alcanzando la idempotencia de TI con Ansible

Achieving IT Idempotency with Ansible

Ceballos Paz, Karin Susana
email: Karin.ceballospaz@gmail.com

Recibido:10/octubre/2020. Revisado: 23/octubre/2020. Aprobado: 24/noviembre/2020.
Disponible en internet el 1 de enero de 2021

Resumen: Una de las razones más importantes por la que muchas organizaciones han adoptado a la automatización como una forma de realizar sus procesos informáticos y así alcanzar sus objetivos de forma más segura, rápida y eficaz, para lo cual se explica cómo funciona la automatización, que es la idempotencia y que es Ansible. El presente estudio se basa fundamentalmente en el estudio de Ansible, esta herramienta de automatización le permite extenderse hasta abarcar tecnologías específicas y áreas más amplias como la nube, la seguridad, etc. y se refiere al análisis de una empresa que se ha dedicado a utilizar Ansible para automatizar sus operaciones diarias de TI para su plataforma de servicios en la nube y locales; dicho análisis presenta como anteriormente el cliente trabajaba y los beneficios que la empresa a logrado obtener con el uso de Ansible, también se muestra la actualidad de la organización, que automatizó las tareas relacionadas con el suministro de recursos y servicios en la nube y redujo enormemente los tiempos de espera. La organización utilizó Ansible para automatizar la funcionalidad de sistemas de red y dicha automatización de tareas liberó a los empleados para trabajar en proyectos más interesantes, incluida la experimentación con Ansible y orientarse más al área de DevOps.

Palabras Claves: Reducción de Costos en TI, Automatización, Ansible, Automatización de Tareas TI, DevOps.

Abstract: One of the most important reasons why many organizations have adopted automation as a way to carry out their IT processes and thus achieve their objectives in a safer, faster and more efficient way, for which it is explained how automation works, which is idempotency and what is Ansible. This study is fundamentally based on the Ansible study, this automation tool allows it to be extended to cover specific technologies and broader areas such as cloud, security, etc. and refers to the analysis of a company that has dedicated itself to using Ansible to automate its daily IT operations for its cloud and local services platform; This analysis shows how the client previously worked and the benefits that the company has achieved with the use of Ansible, it also shows the current situation of the organization, which automated the tasks related to the provision of resources and services in the cloud and greatly reduced waiting times. The organization used Ansible to automate network systems functionality, and such task automation freed up employees to work on more interesting projects, including experimenting with Ansible and focusing more on DevOps.

Desarrollo:

Hace mucho tiempo atrás a finales de los años 40's se dio a conocer el termino de automatización; todo comenzó en la feria mundial en 1939 en la que se presentó un robot

creado por Westinghouse llamado Elektro, dicho robot podía hablar y contar con los dedos hasta 10, pero lamentablemente este era operado por humanos remotamente y se veía afectado en su funcionamiento. De allí surgió la idea de tener algo o alguien capaz de programar y gestionar tareas sin equivocarse, lidiar con eventos inesperados y resolver problemas de rendimiento y seguridad.

Las empresas hoy en día se enfrentan a la necesidad de poder competir contra otras empresas de su índole y en parte esta depende de su capacidad de poseer servicios de alta calidad y que brinden seguridad, integridad y disponibilidad en cada momento. Esto ha sido una de las razones más importantes por la que muchas organizaciones han adoptado a la automatización como una forma de realizar sus procesos informáticos y así alcanzar sus objetivos de forma más segura, rápida y eficaz.

La característica principal de la automatización de procesos informáticos se le conoce en la actualidad como una categorización o un conjunto de herramientas tecnológicas que nos ayudan a ser más eficientes con las actividades de TI en el día a día y aunque en la actualidad existen muchas herramientas para la automatización, la presente investigación se realiza bajo un ambiente de actualidad que permite incorporarse y aplicarse a cualquier elemento del entorno de TI tal y como lo es Ansible. Esta herramienta de automatización le permite extenderse hasta abarcar tecnologías específicas y áreas más amplias como la nube, la seguridad, etc. Y es una de las mejores herramientas de automatización existentes, ya que no necesita tener agentes instalados en los equipos y adicionalmente permite tener conexión con distintos tipos de sistemas operativos, versiones y categorizaciones de los equipos a trabajar.

En este caso en particular el objetivo principal de la presente investigación es impulsar el uso de la automatización y la optimización de los tiempos que toman las operaciones diarias de manejo de las actividades de TI referente a los equipos (servidores, equipos de usuarios, etc.). Muchas de las tareas que realiza el departamento de TI pueden mejorarse a través de la automatización de los procesos, entre algunas de estas tareas podemos mencionar: el manejo de inventarios, parcheo, actualizaciones de políticas, manejo de seguridad, etc.

La Idempotencia se le conoce a la propiedad para realizar una acción determinada varias veces y aun así conseguir el mismo resultado que se obtendría si se realizase una sola vez y esto se logra a través de la automatización de los procedimientos. También es importante conocer que es Ansible: A Network of Social Interactions for Bilateral Life Enhancement. Es un conjunto de herramientas de apoyo que permite interacciones multifacéticas entre humanos y agentes virtuales, diseñadas para adaptarse a ciertas limitaciones técnicas.

Debido a que Ansible es prácticamente una nueva herramienta de automatización y que está implementándose en las nuevas áreas de TI como los es Cloud Computing y las últimas tecnologías y ambientes de trabajo; para el presente artículo de revisión se tomó en

consideración del estudio realizado a Ansible Red Hat por la empresa Forrester en Junio 2018, el estudio se basa en la entrevista realizada a un cliente con más de cinco años de experiencia en el uso de Ansible, y la información del sitio de Red Hat, en la sección de Ansible. La empresa evaluada se ha dedicado a utilizar Ansible para automatizar sus operaciones diarias de TI para su plataforma de servicios en la nube, y de esta forma ha ahorrado costos.

Antes que el cliente utilizará Ansible, contaba con personal que provisionaba, actualizaba y mantenía manualmente la infraestructura del servicio en la nube; el completar las tareas manualmente requería muchísimo tiempo y estaba lleno de errores y frecuentemente se requería de costosos contratistas por hora.

Para cualquier organización es fundamentalmente importante que se garantice la Integridad, Disponibilidad y Confidencialidad de su información, que, a su vez, esto sea de forma rápida y efectiva. Actualmente, muchos administradores de sistemas gestionan y mantienen sus sistemas mediante una colección de secuencias de comandos por lotes o de actividades repetitivas a realizar para mantener a flote todas las actividades informáticas del día a día y de esta forma garantizar los tres pilares de la información. Algunos de los criterios a considerar para la selección de una buena herramienta de automatización efectiva son:

• **Aprendizaje Automático Maduro**: es importante que el aprendizaje automático juegue un papel importante en los términos de implementaciones reales. "Con los datos como parte integral de las nuevas tendencias en las áreas de Desarrollo, el software de automatización puede tomar decisiones que, de otro modo, podrían ser responsabilidad del desarrollador" (Mehul Amin, director de ingeniería de Advanced Systems Concepts, Inc.)

• **Crear oportunidades de Automatización usando la inteligencia artificial**: a corto plazo podemos definir que el aprendizaje automático tendrá un mayor impacto y es vital para el éxito empresarial en los siguientes años.

• **Obsolescencia**: aunque la automatización conlleva cambios en varios roles, esta también conlleva la creación de nuevos roles. Para los profesionales de TI, esto requerirá el desarrollo de nuevas habilidades para el manejo de automatización, programación, inteligencia artificial y ante todo una fuerte postura de seguridad.

• **Evolución continua de las herramientas de scripting y automatización**: existen muchos procesos en el entorno de TI y que muchos son repetitivos y están sujetos a errores humanos, muchas tecnologías ayudan a mejorar estos problemas, con estas herramientas los desarrolladores podrán construir y automatizar flujos de trabajo en menor tiempo y que a su vez reducirán la codificación propensa a errores.

• **Apertura de oportunidades**: Ya que la automatización no elimina la necesidad de medir el rendimiento, esta da la opción a que aumenten las actividades de desarrollo de control y medición, se puede utilizar esta información para el manejo de tendencias de alto nivel y afirmar observaciones cualitativas

A partir de la entrevista y el análisis de datos de este cliente, Forrester concluyó que Ansible Tower tiene el siguiente impacto financiero en un período de tres años: 1,7 millones de USD en beneficios frente a unos costes de 704 490 millones de USD, lo que da como resultado un valor actual neto (VAN) de 1,03 millones de USD y un ROI de un 146%.

Beneficios cuantificados: A continuación, los beneficios cuantificados proporcionales al riesgo obtenido por la compañía entrevistada:

• Mejora en la eficiencia de operación, reduciendo en un 66% los tiempos de espera para la entrega. Con Ansible, la organización automatizó las tareas relacionadas con el suministro de recursos y servicios en la nube y redujo notablemente los tiempos de espera.

• Funcionalidades de equipamiento automatizadas, ahorrándose 389,707 USD. La organización utilizó Ansible para automatizar la funcionalidad de sistemas de red clave, eliminando la necesidad de comprar equipamiento costoso.

• Reconfiguración automatizada, que permite reducir las horas de tiempo implementación del personal en un 94%. La organización automatizó el proceso de recuperación y reconfiguración, reduciendo los tiempos de respuesta y la necesidad de contratar servicios externos.

• Actualizaciones de seguridad automatizadas, que reducen las horas de tiempo de implementación del personal en un 80%. La organización simplificó y automatizó sus prácticas de actualización de seguridad, reduciendo el tiempo y los recursos necesarios.

Beneficios no cuantificados. La organización entrevistada obtuvo los siguientes beneficios, que no se cuantifican en este estudio:

• Se evitó contratar personal adicional. Simplificar y automatizar tareas de TI eliminó la necesidad de ampliar el departamento de TI.

• Reconocimiento de ingresos acelerado. Automatizando la entrega en el servidor, la organización pudo registrar más rápidamente los ingresos.

• Estándares de seguridad mejorados. La organización incorporó a sus protocolos estándares de seguridad establecidos, permitiendo que la organización mantuviese fácilmente sus requisitos actuales.

• Se evitaron errores costosos. Con la automatización de procesos, la organización evitó costosos errores asociados al trabajo manual.

• Mejora de la moral de los empleados. La automatización de tareas liberó a los empleados para trabajar en proyectos más interesantes, incluida la experimentación con Ansible, lo que mejoró la moral.

• Mayor grupo de contratación. Con Ansible Automation, la organización redujo su necesidad de habilidades de lenguaje de programación especializado

Por lo que la tendencia más grande es que la tecnología del mañana será un ecosistema de personas y máquinas. Las aplicaciones monolíticas y centralizadas se encuentran dando paso al desarrollo de soluciones ágiles y distribuidas. Esta innovación impulsada por la tecnología podrá provenir de cualquier persona, en cualquier lugar y no será solo para las organizaciones tecnológicas dedicadas.

Como cualquier empresa para poder brindar un buen control de calidad y un buen servicio de TI, es necesario poder dominar varias herramientas para el manejo del día a día de la empresa, y debido a que automatizar las tareas repetitivas de TI nos permite no solo ganar tiempo y maximizar la productividad de nuestra infraestructura, también el ahorro de costos, ya que se puede hacer más con menos. Y de esta forma podemos conseguir que el personal de TI de nuestra empresa pueda dedicar más tiempo a generar valor para la compañía evitando las tareas repetitivas que se pueden realizar de forma automática.

La automatización debe ser parte de la actualidad de las empresas y es necesaria para los procesos de negocio, lanzamiento y testing continuo, pero lo más importante es sacarles provecho a esos flujos de trabajo existentes, así como su estandarización e integración con toda la cadena de herramientas y procesos de DevOps en el área de TI.

Una verdadera idempotencia se logrará con el apoyo de todas las partes involucradas en los procesos de IT y será de mucha utilidad sacarle todo el provecho a Ansible, esta herramienta permitirá que sean más eficientes y eficaces las actividades diarias de TI, y además permitirá el beneficio de ser capaces de resolver casos fortuitos o bien mejorar en las distintas áreas o segmentos de trabajo y así brindar una mejor calidad y atención al usuario.

Referencias bibliográficas

Ansible For the Windows Admin. Creado: 15 de febrero 2019. Recuperado de: https://opensource.com/article/19/2/ansible-windows-admin

How Ansible Works Actualizado : Marzo 2020. https://www.ansible.com/overview/how-ansible-works?intcmp=701f2000000h4RcAAI

The Total Economic Impact TM OF Red Hat Ansible Tower. Creado en Junio 2018. https://www.ansible.com/hubfs/pdfs/cm-forrester-total-economic-impact-ansible-analyst-paper-f13019-201806-en.pdf

Overview Ansible. Actualizado: Sept.2020. https://www.ansible.com/

Getting started with Ansible security automation: Threat Hunting. Creado: Oct-15 2020 por: Roland Wolters. Recuperado de: https://www.ansible.com/blog/getting-started-with-ansible-security-automation-threat-hunting

What is Ansible?. Recuperado de: https://networklore.com/ansible/

Ansible for Devops. Jeff Geerling. ISBN-13: 978-0986393419. ISBN-10: 098639341X

Ansible: Up and Running: Automating Configuration Management and Deployment the Easy Way (Inglés) 2nd. Lorin Hochstein. "ISBN-13: 978-1491979808. ISBN-10: 1491979801". Segunda Edición. Editorial O'reilly

Ansible Playbook Essentials: Design automation blueprints using Ansible's playbooks to orchestrate and manage your multitier infrastructure. Gourav Shah. Primera Edición. https://ualmtorres.github.io/CursoAnsible/tutorial/

Sobre la autora:

Ingeniera en Sistemas por la Universidad Mariano Gálvez de Guatemala, cuenta con más de 20 años de experiencia en distintas áreas de IT. Actualmente se encuentra incursionando en el área de DevOps y Automatización de Procesos, debido a su alta experiencia en administración de sistemas operativos Windows y Linux y desarrollo y pruebas de software, también posee experiencia sobre administración de Bases de Datos, Análisis de Datos, Reportería, QA, etc. Culminó su maestría en Seguridad informática en el presente año y ha trabajado en compañías multinacionales de alto nivel y de distintas áreas, como Atos Information Technology, Xerox, Lankin Technologies, Grupo Hame, Serviplast, Ecoplast.

CyberSecurity
Información & Privacidad

Estudio sobre el impacto de los ataques de Ransomware en el Sector de la Salud

Study on the impact of Ransomware attacks in the Sector of the health

Noé Istacuy Carrillo
email: nistacuyc@miumg.edu.gt

Recibido:6/octubre/2020. Revisado: 14/noviembre/2020. Aprobado: 23/noviembre/2020.
Disponible en internet el 1 de enero de 2021

Resumen: El sector de la salud es uno de los objetivos principales de los ciberdelincuentes. Cada año hay un incremento en la cantidad de ataques de Ransomware que impactan a organizaciones que prestan servicios de salud. El objetivo de este estudio fue identificar y exponer el impacto que ha tenido el Ransomware en el sector de la salud, analizando ataques producidos durante los años 2019 y 2020. Para ello, se desarrollaron actividades de recolección, observación y análisis de contenido de fuentes que abordan la realidad actual del sector de la salud frente al Ransomware y se realizó un análisis del impacto operacional, económico, legal y en la vida de los pacientes de 15 ataques de Ransomware producidos en organizaciones dentro del sector de la salud. Los resultados fueron relevantes: respecto a lo operacional, 15 organizaciones vieron interrumpidas sus actividades y 2 de ellas cerraron operaciones. En lo económico, 4 organizaciones realizaron el pago exigido por los ciberdelincuentes y 3 reportaron pérdidas económicas por miles y millones de dólares. El impacto legal se reflejó en demandas legales impuestas a 4 organizaciones por pacientes infectados. El impacto en la vida de los pacientes se determinó por los miles de personas que vieron comprometida su información personal y clínica, 5 organizaciones reportaron que se divulgó esta información. En conclusión, el impacto de los ataques de Ransomware en el sector de la salud se vio determinado por aspectos como: interrupción parcial o total de las operaciones de las organizaciones, pérdidas económicas derivadas de pagos por rescate y de la interrupción de operaciones y, también por demandas legales que afectaron a la reputación de las organizaciones. La vida de los pacientes se vio afectada por la falta de atención médica y porque se comprometió y divulgó su información, la cual es un vínculo directo hacia ellos.

Palabras Claves: Incidentes de Ciberseguridad, COVID-19, demandas por falta de atención médica, pago de rescate a ciberdelincuentes, secuestro de información digital.

Abstract: The healthcare sector is one of the main targets for cybercriminals. Every year there is an increase in the number of Ransomware attacks that impact organizations that provide healthcare services. The purpose of this study was to identify and expose the impact that Ransomware has had on the healthcare sector, analyzing attacks produced during 2019 and 2020. To do this, activities to collect, observe and analyze content from sources that approach the current reality of the health sector against Ransomware were developed and an analysis of the operational, economic, legal and life impact of patients of 15 Ransomware

attacks produced in organizations within the healthcare sector was carried out. Results were relevant: in terms of operations, 15 organizations saw their activities interrupted and 2 of them shut down operations. Related to economic impact, 4 organizations made the payment demanded by cybercriminals and 3 reported financial losses of thousands and millions of dollars. The legal impact was reflected in legal claims imposed on 4 organizations by affected patients. The impact on patients' lives was determined by the thousands of people who had their personal and clinical information compromised, 5 organizations reported that this information was disclosed. In conclusion, the impact of Ransomware attacks in the health sector was determined by aspects such as: partial or total interruption of the operations, economic losses derived from ransom payments and the interruption of operations, and also from legal claims that affected the organizations' reputation. The patients' lives were affected by the lack of medical care and because their information, which is a direct link to them, was compromised and disclosed.

Desarrollo:

En la actualidad, son muchas las organizaciones que continuamente evolucionan dentro del marco de la transformación digital, en busca de desarrollar de forma eficiente y óptima sus procesos y actividades de negocio, así como de potenciar el intercambio de información a través de la implementación de nuevas tecnologías.

Las organizaciones que pertenecen al sector de la salud no son ajenas a esta transformación, ya que continuamente se integran a ella a través de la implementación de nuevas tecnologías que permitan mejorar la atención a los pacientes, la gestión de su información médica y personal, y la calidad de los procesos de investigación y diagnóstico clínicos, entre otros. Este hecho relevante implica también la exposición a potentes amenazas a la ciberseguridad que pueden comprometer sus activos tecnológicos y recursos más importantes, causando así un impacto negativo en sus procesos, operaciones y actividades más críticas.

Una de las principales amenazas que está presente dentro del ciberespacio, es el software malicioso identificado como Ransomware, el cual puede llegar a afectar de forma negativa los recursos de atención médica, los sistemas informáticos, la información propia del negocio, la información de los pacientes y en consecuencia, a la salud y la vida de los pacientes de las organizaciones del sector de la salud. De acuerdo con el informe titulado Data Breach Investigation Report 2020, elaborado por Verizon, una organización de tecnología y comunicación global, en el año 2020 se han reportado y registrado un total de 798 incidentes de seguridad dentro del sector de la salud a nivel mundial, de los cuales un total de 521 resultaron en la divulgación de información resguardada en las organizaciones.

Un dato relevante lo constituye el hecho que, dentro de los 798 incidentes de seguridad reportados, se encuentran un total de 192 los cuales fueron provocados por modalidades de

Crimeware, incluyendo ataques de Ransomware [1]. Tomando en cuenta que en la actualidad el sector de la salud es uno de los blancos principales para los ciberdelincuentes, resulta de gran importancia realizar este artículo, con el fin de analizar de qué forma impactan los ataques de Ransomware en las organizaciones del sector de la salud. Es importante también poder identificar aspectos importantes de incidentes relevantes de ciberseguridad de Ransomware que se han provocado en los años 2019 y 2020.

El Ransomware es un tipo de software malicioso utilizado por los ciberdelincuentes que infecta las computadoras y hace que los archivos o la computadora del usuario afectado, sean inutilizables hasta el momento en el que se pague un rescate por ellos. Básicamente, el Ransomware puede asumir el control del sistema o los recursos del usuario afectado y evitar el acceso. Los ciberdelincuentes aprovechan los vectores de ataque tales como ingeniería social, Phishing y protocolo de escritorio remoto para concretar ataques de Ransomware y lograr su cometido. (Keshavarzi & Ghaffary, 2020) [2]. Este tipo de malware es muy peligroso y, de infectar una computadora o cualquier otro equipo tecnológico, puede ocasionar interrupción en la funcionalidad y paralizar así las operaciones y procesos que soportan a los usuarios y las organizaciones.

Considerando todos estos aspectos se elabora este artículo, el cual tiene como objetivo identificar y exponer el impacto que ha tenido el Ransomware en las organizaciones del sector de la salud, a través del análisis de distintos ataques cibernéticos específicos que se han conocido en el espacio de tiempo de los años 2019 y 2020, examinando sus características y efectos provocados, además de su relación con la perspectiva de lo económico, operacional, legal y, principalmente, en lo relacionado a la vida de los pacientes.

Materiales y Métodos

La metodología empleada para el desarrollo del estudio en cuestión, relacionado con el Ransomware y su impacto en el sector de la salud, se llevó a cabo con base a tres métodos puntuales, cada uno determinado por el tipo de fuente consultada que sirvió como base para la sustentación teórica, descriptiva y analítica.

El primer método se orientó a la observación y análisis de información contenida en Informes de Seguridad Informática, elaborados por organizaciones expertas en soluciones de Ciberseguridad. El fin de este método fue obtener, con base a datos estadísticos puntuales contenidos en dichos informes, un marco de referencia que permita describir cómo se ha visto afectado el sector de la salud por ataques cibernéticos. Estos datos incluyen: cantidad, patrones y motivos, tipo de datos comprometidos en los incidentes de seguridad reportados y específicamente, el porcentaje de estos incidentes que fueron causados por acción del Ransomware.

El segundo método se orientó a la recolección y análisis de contenido, tanto teórico como descriptivo, de información incluida en artículos consultados en el sitio de Google Académico. El enfoque de este método fue identificar dentro de estos artículos, elementos que permitan explicar y describir, de forma cualitativa, cuál es la realidad actual del sector de la salud frente a la Ciberdelincuencia en lo relacionado a Ransomware.

El tercer método se orientó a la investigación, y análisis de contenido de artículos digitales de diversos sitios de la red de Internet, tales como: HealthITSecurity, SC Media, Modern Healthcare, BBC, DataBreachToday, entre otras. Estos sitios sirvieron de referencia en otros artículos de investigación que fueron consultados en Google Académico. El fin de este método fue de localizar casos puntuales de Ransomware, seleccionados de forma intencional, que permitieran identificar aspectos relevantes relacionados al tipo de impacto que han tenido estos ataques dentro del sector de la salud. Se analizaron un total de 15 ataques de Ransomware que tuvieron lugar en los años 2019 y 2020 en organizaciones del sector de la salud distribuidos en 3 países: Estados Unidos, Reino Unido y República Checa.

Tabla 1. Ataques de Ransomware analizados en organizaciones del sector de la salud en los años 2019 y 2020.

Fecha	**País**	**Organización**
Jun. 2020	Estados Unidos	University of California San Francisco (UCSF) [3] [4]
May. 2020	Estados Unidos	Assured Imaging [5] [6] [7]
Abr. 2020	Estados Unidos	Florida Orthopaedic Institute [8] [9] [10]
Abr. 2020	Estados Unidos	Arizona-based Magellan Health [11] [12]
Mar. 2020	República Checa	Brno University Hospital [13] [14]
Mar. 2020	Reino Unido	Hammersmith Medicines Research (HMR) [15] [16]
Dic. 2019	Estados Unidos	New Jersey's Medical Diagnostics Laboratories [17] [18]
Dic. 2019	Estados Unidos	Hackensack Meridian [19] [20] [21]
Oct. 2019	Estados Unidos	DCH Health System [22] [23]
Ag. 2019	Estados Unidos	Wood Ranch Medical [24] [25]
Jul. 2019	Estados Unidos	Premier Family Medical [26] [27]
Jun. 2019	Estados Unidos	N.E.O. Urology [28] [29]
Jun. 2019	Estados Unidos	Park DuValle Community Health Center [30] [31]

Jun. 2019	Estados Unidos	Grays Harbor Community Hospital and Harbor Medical Group [32] [33]
Abr. 2019	Estados Unidos	Brookside ENT and Hearing Center [34]

Fuente: Elaboración propia. Los índices hacen referencia a las fuentes consultadas de la información de cada ataque analizado.

El análisis del impacto se realizó desde 4 perspectivas principales: operacional, económico, legal y, principalmente, desde la perspectiva del impacto en la vida de los pacientes. Este análisis fue de tipo cualitativo, desarrollado a través de una matriz de datos que permitió identificar un conjunto de aspectos que se consideraron como parte de cada tipo de impacto analizado. Los aspectos analizados se observan en la Tabla 2.

Tabla 2. Elementos de cada tipo de impacto analizados por cada ataque de Ransomware.

Tipo de Impacto	**Aspecto analizado**
Operacional	¿Acceso restringido al sistema?
	¿Acceso restringido a la información?
	¿Interrupción de operaciones?
	¿Hubo recuperación en las operaciones?
Económico	Monto de pago de rescate solicitado
	Monto de pérdidas reportadas
	¿Se realizó el pago de rescate?
Legal	¿Hubo demanda legal?
	Motivo de la demanda
En los pacientes	Cantidad de pacientes afectados
	¿Se comprometió la información personal de los pacientes?
	¿Se comprometió la información clínica de los pacientes?
	¿Se divulgó la información comprometida?

Fuente: Elaboración propia

Resultados

Luego de haber analizado la información de los ataques de Ransomware relacionada al impacto en las organizaciones del sector de la salud, es posible describir los resultados observados.

En lo relacionado al impacto económico, se encontró que, de las 15 organizaciones, hubo 4 las cuales realizaron el pago por el rescate que los atacantes exigían para recuperar el acceso al sistema o la información comprometida. Los montos del pago del rescate que se efectuaron representan una suma monetaria considerable.

Además, se observó que 3 organizaciones reportaron pérdidas monetarias derivadas del ataque que sufrieron.

Tabla 4. Resultado de aspectos analizados relacionados al impacto económico en las organizaciones del sector de la salud.

Fecha	Organización	Monto de pago de rescate solicitado	Monto de pérdidas reportadas	¿Se realizó el pago de rescate?
Jun. 2020	University of California San Francisco (UCSF)	$1,140,895.00	$1,140,895.00	Sí
Dic. 2019	New Jersey's Medical Diagnostics Laboratories	$1,7000,000.00	No especifica	No
Dic. 2019	Hackensack Meridian	No especifica	No especifica	Sí
Jun. 2019	N.E.O. Urology	$75,000.00	$ 120,000.00	Sí
Jun. 2019	Park DuValle Community Health Center	$70,000.00	$1,000,000.00	Sí
Jun. 2019	Grays Harbor Community Hospital and Harbor Medical Group	$1,000,000.00	No especifica	No especifica
Abr. 2019	Brookside ENT and Hearing Center	$6,500.00	No especifica	No

Fuente: Elaboración propia

Adicional, también se observó que éstas 3 organizaciones reportaron pérdidas mayores o iguales al monto de rescate que los atacantes solicitaron. Estas organizaciones confirmaron que realizaron el pago por el rescate que exigieron los atacantes.

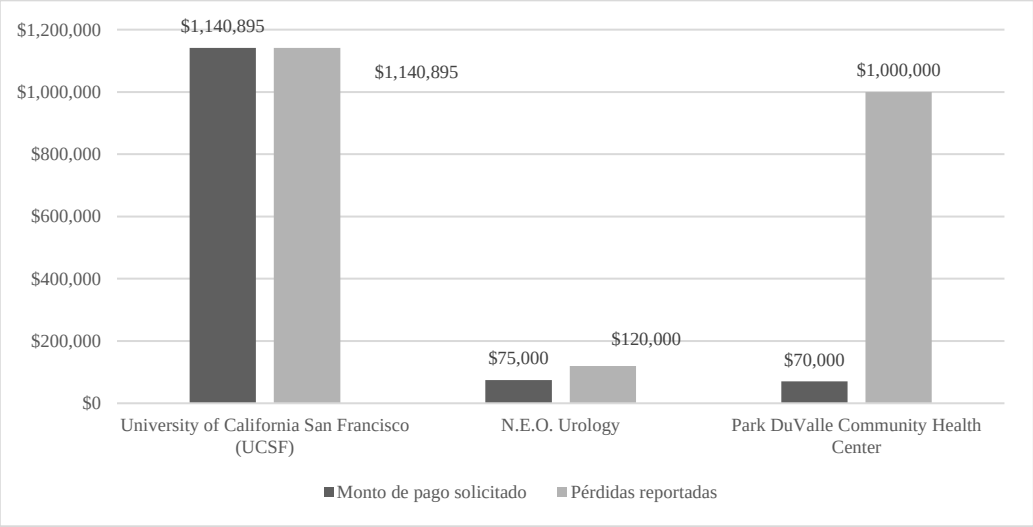

Figura 1. Impacto económico en las organizaciones que confirmaron el pago por el rescate. Fuente: Elaboración propia

Dentro del análisis del impacto operativo de los ataques de Ransomware, resulta relevante el hecho que reflejó que las 15 organizaciones se vieron afectadas en sus operaciones. De estas, hubo 2 que no pudieron recuperarse del impacto operativo derivado del ataque.

Tabla 3. Resultado de aspectos analizados relacionados al impacto operacional en las organizaciones del sector de la salud.

Fecha	**Organización**	**¿Acceso restringido al sistema?**	**¿Acceso restringido a la información?**	**¿Interrupción de operaciones?**	**¿Hubo recuperación en las operaciones?**
Jun. 2020	University of California San Francisco (UCSF)	Sí	Sí	Sí	Sí
May. 2020	Assured Imaging	Sí	Sí	Sí	Sí
Abr. 2020	Florida Orthopaedic Institute	Sí	Sí	Sí	Sí
Abr. 2020	Arizona-based Magellan Health	Sí	Sí	Sí	Sí
Mar. 2020	Brno University Hospital	Sí	Sí	Sí	Sí
Mar. 2020	Hammersmith Medicines Research (HMR)	Sí	Sí	Sí	Sí
Dic. 2019	New Jersey's Medical Diagnostics Laboratories	Sí	Sí	Sí	No especifica
Dic. 2019	Hackensack Meridian	Sí	Sí	Sí	Sí
Oct. 2019	DCH Health System	Sí	Sí	Sí	Sí
Ag. 2019	Wood Ranch Medical	Sí	Sí	Sí	No
Jul. 2019	Premier Family Medical	Sí	Sí	Sí	Sí
Jun. 2019	N.E.O. Urology	Sí	Sí	Sí	Sí
Jun. 2019	Park DuValle Community Health Center	Sí	Sí	Sí	Sí

Jun. 2019	Grays Harbor Community Hospital and Harbor Medical Group	Sí	Sí	Sí	Sí
Abr. 2019	Brookside ENT and Hearing Center	Sí	Sí	Sí	No

Fuente: Elaboración propia

Respecto al impacto legal se identificó que, de las 15 organizaciones, 4 enfrentaron demandas legales por parte de los pacientes afectados, siendo el principal motivo de acusación la negligencia en la gestión y protección de la información de los pacientes.

Tabla 5. Resultado de aspectos analizados relacionados al impacto legal en las organizaciones del sector de la salud

Fecha	**Organización**	**¿Hubo demanda legal?**	**Motivo de la demanda**
May. 2020	Assured Imaging	Sí	Negligencia en la protección de información de pacientes
Abr. 2020	Florida Orthopaedic Institute	Sí	Negligencia en la protección de información de pacientes
Dic. 2019	Hackensack Meridian	Sí	Negligencia en la protección de información de pacientes
Oct. 2019	DCH Health System	Sí	Falta de atención médica

Fuente: Elaboración propia

Por último, en lo relacionado al impacto que tuvieron los ataques de Ransomware en los pacientes de las organizaciones de salud, se pudo observar que los atacantes divulgaron la información tanto personal como clínica de los pacientes de 4 organizaciones, 3 de ellas con un número considerable de pacientes afectados.

Otro dato relevante es el hecho de poder observar la cantidad de pacientes que se vieron afectados en cada organización en las que se efectuó el ataque de Ransomware, se observan cifras de miles de pacientes que sufrieron las consecuencias de estos ciberataques.

Tabla 6. Resultado de aspectos analizados relacionados al impacto en los pacientes de las organizaciones del sector de la salud.

Fecha	Organización	Cantidad de pacientes afectados	¿Se comprometió la información personal de los pacientes?	¿Se comprometió la información clínica de los pacientes?	¿Se divulgó la información comprometida?
May. 2020	Assured Imaging	244,813	Sí	Sí	Sí
Abr. 2020	Florida Orthopaedic Institute	640,000	Sí	Sí	Sí
Abr. 2020	Arizona-based Magellan Health	365,000	Sí	Sí	Sí
Mar. 2020	Hammersmith Medicines Research (HMR)	2,300	Sí	Sí	Sí
Dic. 2019	New Jersey's Medical Diagnostics Laboratories	No especifica	No especifica	Sí	Sí
Oct. 2019	DCH Health System	No especifica	Sí	Sí	No especifica
Ag. 2019	Wood Ranch Medical	No especifica	Sí	Sí	No
Jul. 2019	Premier Family Medical	320,000	Sí	Sí	No
Jun. 2019	N.E.O. Urology	No especifica	Sí	Sí	No
Jun. 2019	Park DuValle Community Health Center	20,000	Sí	Sí	No
Jun. 2019	Grays Harbor Community Hospital and Harbor Medical Group	85,000	Sí	Sí	No
Abr. 2019	Brookside ENT and Hearing Center	No especifica	Sí	Sí	No especifica

Fuente: Elaboración propia

Discusión

El sector de la salud es uno de los principales objetivos de los ciberdelincuentes. Esto se ve reflejado en el hecho de que durante el año 2020 se produjeron 521 incidentes de seguridad, incluidos ataques de Ransomware, que comprometieron la información que se gestiona en estas organizaciones. El 88% de estos incidentes fueron llevados a la práctica por motivos financieros (Verizon, 2020) [1]. Sin duda alguna, los ataques de Ransomware persiguen el secuestro de la información personal, clínica y de negocio, la cual es vital para las organizaciones de salud y los pacientes que utilizan sus servicios.

En este estudio se ven reflejados los datos relevantes de los ataques de Ransomware analizados, los cuales han sido identificados en base a una serie de criterios expuestos anteriormente. Es importante mencionar que, según la información investigada de cada ataque, no todos incluyen datos relacionados a cada tipo de impacto analizado: económico, operacional, legal y el impacto en la vida de los pacientes. Esto se debe principalmente a que no todas las organizaciones divulgan la información completa sobre los ataques de los cuales han sido víctimas. Sin embargo, el hecho de que cada ataque tenga datos relevantes de por lo menos un tipo de impacto representa un elemento de gran utilidad para fundamentar, en base a datos reales, los argumentos que se exponen.

Impacto Operativo

El impacto operativo de los ataques de Ransomware en las organizaciones del sector salud es la primera manifestación de que se ha concretado una acción que compromete los activos tecnológicos y la información que se resguarda. Se trata de un impacto inmediato en las operaciones de los servicios de salud que se presenta a través de comportamientos no esperados, tales como el acceso restringido a los sistemas y a la información que se gestionar.

Se observa que todos los ataques de Ransomware concretados y analizados derivaron en interrupción de servicios de salud, esto permite afirmar que ninguna organización se ve librada del impacto operativo que resulta de estos hechos. Si bien hay organizaciones que pueden recuperarse de un ataque de este tipo, ya sea por tener capacidad tecnológica de recuperación o bien por la capacidad económica para realizar el pago, hay otras que no corren con la misma suerte y se ven obligadas a cancelar definitivamente sus operaciones. Esto se ve reflejado en 2 casos específicos de organizaciones que se vieron obligadas a cerrar sus operaciones.

El primer caso es el de la organización Wood Ranch Medical, la cual sufrió un ataque de Ransomware en el mes de agosto de 2019. El impacto fue de tal magnitud que no fue posible recuperar la información y reconstruir los registros médicos. La organización reporta que no accedió al pago del rescate exigido y se vio obligada a cerrar operaciones en diciembre de 2019 (Davis, 2019) [24] [25]. El segundo caso se trata de un ataque perpetuado en el mes de

abril de 2019 en la organización Brookside ENT and Hearing Center. Al negarse el pago por el rescate de la información secuestrada, los atacantes eliminaron toda la información de la organización y provocaron que los funcionarios tomaran la decisión de no continuar con la prestación de los servicios médicos que facilitaban a sus pacientes (Davis, 2019) [34].

En el análisis de estos casos se puede identificar una relación que se establece entre el impacto económico con el impacto operativo que se producen los ataques de Ransomware. El hecho de que las organizaciones no realicen el pago exigido por el rescate deriva en el hecho de no poder recuperar la información y los sistemas que han sido secuestrados y, en última instancia, ocasiona que no se pueda continuar con las operaciones de prestación de servicios de salud. Este efecto dominó, evidencia que se pueden establecer relaciones entre los factores que se analizan de cada tipo de impacto, los cuales no se presentan de forma aislada.

Impacto económico

Los ataques de Ransomware en el sector de la salud dejan consecuencias y pérdidas económicas significativas. Un estudio publicado por Emsisoft Malware Lab, indica que en el año 2019 se reportaron más de 950 ataques, con un costo total estimado de más de 7.5 billones de dólares (Karambelas, 2020) [19].

Dentro de lo relacionado al impacto económico, se pueden observar aspectos relevantes que permiten realizar deducciones interesantes. Primero, es importante mencionar que el impacto económico en toda organización que es víctima de ataques de Ransomware, se traduce en pérdidas que están integradas por el monto del pago se realizó por el rescate y/o por el monto reportado como pérdida de ingresos derivado de la interrupción de las operaciones. En esto se puede identificar también la relación de efecto que tiene el impacto operativo en el impacto económico para las organizaciones del sector salud: si no hay operaciones, no hay ingresos.

Algunos casos que ilustran esto, son los ataques confirmados por las organizaciones University of California San Francisco (UCSF) en junio de 2020 que en la actualidad enfoca sus esfuerzos en investigación y pruebas para dar respuesta a la pandemia del COVID-19 (Davis, 2020) [3] y por la organización Park DuValle Community Health Center en junio de 2019 (Davis, 2019) [4]. Ambas, reportan pérdidas que alcanzan los montos del millón de dólares y confirman que realizaron el pago exigido por los atacantes.

Segundo, se observa que algunas organizaciones tienen la capacidad económica de poder realizar el pago por el rescate. Este aspecto permite deducir que, en ocasiones, es preferible acceder a realizar el pago que a optar por recuperarse operativamente a través de medidas tecnológicas de continuidad y recuperación del negocio. Los motivos que pueden llevar a las organizaciones a tomar esta decisión pueden ser varios, pero se considera que el más importante es la criticidad de las operaciones que desarrollan en torno a los servicios que

prestan; la salud y la vida de los pacientes es prioridad ante cualquier situación que se pueda presentar.

Al mitigar el ataque de esta forma las organizaciones deben considerar que, al ser potenciales víctimas de futuras amenazas, se debe invertir también en desarrollar e implementar medidas tecnológicas para garantizar la seguridad, la respuesta y la recuperación inmediata ante cualquier amenaza de este tipo. Se debe prestar especial atención a la formación de los colaboradores de las organizaciones del sector de la salud en temas de ciberseguridad, ya que representan el eslabón más débil dentro de los sistemas de seguridad informática (Pranggono & Arabo, 2020) [14].

Impacto legal

Desde la perspectiva de lo legal, el impacto de los ataques de Ransomware también resulta relevante. Diferentes demandas legales resultan como consecuencia de las acciones concretadas de los ciberdelincuentes que llegan a comprometer las operaciones y la información de las organizaciones que prestan servicios de salud.

Al observar que para las organizaciones Assured Imaging, Florida Orthopaedic Institute, Hackensack Meridian y DCH Health System las consecuencias legales se han traducido en demandas por negligencia en la protección de la información que gestionan y por falta de atención médica de los pacientes, se hace relevante el hecho de la importancia que tiene la responsabilidad de toda organización de garantizar la Seguridad Informática, sobre todo considerando el tipo de información que gestionan, la cual está ligada directamente a los pacientes y a su integridad.

Otro aspecto relevante que deriva del impacto legal es el efecto negativo que tiene sobre la reputación de cualquier organización del sector de la salud. Enfrentar un proceso legal por los motivos indicados, daña de forma significativa la imagen de la organización ante las personas, presentándola como no confiable, irresponsable o incapaz de brindar sus servicios de salud críticos ante cualquier situación adversa.

Impacto en la vida de los pacientes

El año 2020 tiene un hecho que marca un punto de inflexión en la realidad del sector de la salud: la aparición del COVID-19. Los ciberdelincuentes han aprovechado esta situación para atacar con Ransomware a organizaciones cuyas actividades van encaminadas a la investigación y respuesta ante este virus. Esta realidad actual permite exponer argumentos importantes en lo relacionado al impacto que tienen estos ataques en la vida de los pacientes.

Ejemplo de lo anterior es el ataque que se concretó a la organización Brno University Hospital ubicada en República Checa en el mes de marzo de 2020, la cual se dedica a realizar pruebas de COVID-19 (Cimpanu, 2020) [13]. Las consecuencias de este hecho repercuten directamente en las operaciones de la organización, las cuales son fundamentales en la lucha

continua contra la pandemia, y especialmente en los pacientes que requieren este servicio, que en la actualidad se ha tornado crítico. El hecho de no tener la posibilidad de acceder a las pruebas de detección del virus que realiza esta organización impacta de forma drástica en los pacientes, atentando incluso contra su propia vida.

Otro hecho que se identifica en este tiempo de la pandemia es el ataque provocado por el grupo de Ransomware llamado Maze en la organización Hammersmith Medicines Research, ubicada en el Reino Unido, en el mes de marzo de 2020. Esta organización se dedica, entre otras cosas, a realizar investigaciones sobre una posible vacuna contra el COVID-19. (Goodwin, 2020) [15]. Este ataque tiene un impacto relevante que se debe considerar: en la actualidad es de vital importancia que las organizaciones de investigación del sector salud puedan desarrollar estudios que permitan determinar una posible cura ante el virus. Interrumpir estas actividades trae consecuencias considerables a nivel mundial: la posible vacuna se atrasa y día con día el virus se expande por todo el mundo, poniendo en riesgo la vida de las personas.

Se observa que la cantidad de pacientes afectados por consecuencia de los ataques de Ransomware en las organizaciones del sector salud, es considerable y supera los miles de personas que vieron comprometida tanto su información personal, como su información clínica. Un factor aún más crítico es el hecho de que se ha producido una divulgación de esta información la cual puede comprometer directamente la integridad de la persona.

Conclusiones

Los ataques de Ransomware aumentan año con año a medida que las organizaciones del sector de la salud adoptan nuevas tecnologías para la gestión de sus procesos y actividades de negocio. Las formas en que estas acciones impactan a las organizaciones y a los pacientes que hacen uso de los servicios de salud, están determinadas por la naturaleza y características propias del ataque producido. Se han identificado distintos factores que permiten evaluar los tipos de impacto que se producen cuando se concreta un ataque de Ransomware en una organización que presta servicios de salud.

Desde la perspectiva operativa se encuentran 2 factores relevantes que determinan si se produjo un impacto significativo de este tipo, el primero es el que establece si se produce una interrupción en las operaciones y el segundo es el que establece si una organización tiene la capacidad de reanudar las operaciones después que se produce el ataque. La consecuencia de este impacto se ve reflejada en el tiempo en el que una organización no puede prestar los servicios de salud o en última instancia, en el cierre definitivo de sus operaciones.

En lo relacionado a lo económico, un factor fundamental que determina este impacto es el monto de las pérdidas en términos monetarios que una organización reporta como consecuencia de haber sufrido un ataque de Ransomware. En este sentido también existe un

efecto negativo en la economía de una organización que presta servicios de salud, el cual viene determinado por la interrupción inmediata de sus operaciones. Como consecuencia de lo anterior, se observan pérdidas económicas por montos que sobrepasan el pago solicitado por el rescate del ataque perpetuado.

Hablando del impacto legal, los factores relevantes de los ataques de Ransomware se traducen en demandas y procesos legales no deseados. Esto también repercute en la imagen de la organización y conduce a pérdidas económicas derivadas de los gastos que todo proceso legal implica.

Por último, el impacto más importante es el que se relaciona directamente con la vida de los pacientes de las organizaciones dedicadas a prestar servicios de salud. Factores determinantes de este tipo de impacto son la cantidad de pacientes afectados, el tipo de información de los pacientes que se comprometió y si los atacantes divulgaron sin consentimiento esta información. La información personal y clínica de un paciente es un vínculo directo hacia la misma persona y su mala utilización puede llegar a comprometer su integridad e incluso su propia vida.

Además, existe una relación entre los distintos tipos de impacto que tienen los ataques de Ransomware en las organizaciones del sector de la salud. El impacto inmediato es el operativo del cual se derivan otros efectos en lo relacionado a lo económico, legal y en la vida de los pacientes. Si se interrumpen las operaciones de las organizaciones por causa de un ataque, se generan pérdidas económicas, se produce una carencia en la atención médica a los pacientes quienes ven comprometida su salud y su vida.

Referencias bibliográficas

[1] Verizon. (2020). 2020 Data Breach Investigations Report. Recuperado de: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/healthcare-data-breaches-security/

[2] Al Qartah, A. (2020). EVOLVING RANSOMWARE ATTACKS ON HEALTHCARE PROVIDERS. Recuperado de: https://www.researchgate.net/profile/Ayed_Al_Qartah/publication/344450646_EVOLVING_RANSOMWARE_ATTACKS_ON_HEALTHCARE_PROVIDERS/links/5f76e97e92851c14bca7b58a/EVOLVING-RANSOMWARE-ATTACKS-ON-HEALTHCARE-PROVIDERS.pdf

[3] Tidy, J. (2020). How hackers extorted $1.14m from University of California, San Francisco. Recuperado de: https://www.bbc.com/news/technology-53214783

[4] Davis, J. (2020). UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack. Recuperado de: https://healthitsecurity.com/news/ucsf-pays-1.14m-to-netwalker-hackers-after-ransomware-attack

[5] Davis, J. (2020). Assured Imaging Ransomware Causes Data Theft Affecting 245K Patients. Recuperado de: https://healthitsecurity.com/news/assured-imaging-ransomware-causes-data-theft-affecting-245k-patients

[6] Shaak, E. (2020). Assured Imaging Hit with Lawsuit Over May 2020 Ransomware Attack Affecting 244,000+ Patients. Recuperado de: https://www.classaction.org/news/assured-imaging-hit-with-lawsuit-over-may-2020-ransomware-attack-affecting-244000-patients

[7] Davis, J. (2020). Patient Breach Victims File Lawsuits Against Assured Imaging, BJC Health. Recuperado de: https://healthitsecurity.com/news/patient-breach-victims-file-lawsuits-against-assured-imaging-bjc-health

[8] McGee, M. (2020). Lawsuits After Ransomware Incidents: The Trend Continues. Recuperado de: https://www.databreachtoday.com/lawsuits-after-ransomwareincidents-trend-continues-a-14567

[9] Patterson, C. (2020). Notification of Data Security Incident. Recuperado de: https://oag.ca.gov/system/files/Florida%20Orthopaedic%20Institute%20-%20Ca.pdf

[10] U.S. Department of Health and Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Recuperado de: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[11] Davis, J. (2020). Magellan Health Data Breach Victim Tally Reaches 365K Patients. Recuperado de: https://healthitsecurity.com/news/magellan-health-data-breach-victim-tally-reaches-365k-patients

[12] Davis, J. (2020). UPDATE: The 10 Biggest Healthcare Data Breaches of 2020, So Far. Recuperado de: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far

[13] Cimpanu, C. (2020). Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak. Recuperado de: https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[14] Pranggono, B., Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. Recuperado de: https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247

[15] Goodwin, B. (2020). Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack. Recuperado de: https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

[16] Pranggono, B., Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. Recuperado de: https://onlinelibrary.wiley.com/doi/full/10.1002/itl2.247

[17] Iao, K. (2020). Maze Ransomware Group Publicly Releases Stolen Data. Recuperado de: https://www.paubox.com/blog/maze-ransomware-group-publicly-releases-stolen-data/

[18] Davis, J. (2020). Maze Ransomware Hackers Extorting Providers, Posting Stolen Health Data. Recuperado de: https://healthitsecurity.com/news/maze-ransomware-hackers-extorting-providers-posting-stolen-health-data

[19] Karambelas, C. (2020). Health Care Technology: Ransomware Risk and Protection. Recuperado de: https://search.proquest.com/openview/76e23931200b59a1e1afa2974b8ecd03/1?pq-origsite=gscholar&cbl=33486

[20] Davis, J. (2019). Ransomware Attacks Disrupt Patient Care at Hawaii, NJ Hospitals. Recuperado de: https://healthitsecurity.com/news/ransomware-attacks-disrupt-patient-care-at-hawaii-nj-hospitals

[21] Davis, J. (2020). Hackensack Meridian Faces Breach Lawsuit After Ransomware Attack. Recuperado de: https://healthitsecurity.com/news/hackensack-meridian-faces-breach-lawsuit-after-ransomware-attack

[22] Davis, J. (2020). DCH Health Faces Federal Lawsuit After 10-Day Ransomware Attack. Recuperado de: https://healthitsecurity.com/news/dch-health-faces-federal-lawsuit-after-10-day-ransomware-attack

[23] Davis, J. (2019). Ransomware Forces 3 Hospitals into Downtime, as 'Disruptionware' Emerges. Recuperado de: https://healthitsecurity.com/news/ransomware-forces-3-hospitals-into-downtime-as-disruptionware-increases

[24] Wood Ranch Medical. (2019). Wood Ranch Medical Notifies Patients of Ransomware Attack. Recuperado de: https://www.woodranchmedical.com/

[25] Davis, J. (2019). California Provider to Close After Ransomware Attack Damages System. Recuperado de: https://healthitsecurity.com/news/california-provider-to-close-after-ransomware-attack-damages-system

[26] Barth, B. (2019). Ransomware attack on Premier Family Medical reportedly impacts records of 320K patients. Recuperado de: https://www.scmagazine.com/home/security-news/cybercrime/ransomware-attack-on-premier-family-medical-reportedly-impacts-records-of-320k-patients/

[27] Cohen, J. (2019). Utah practice says 320,000 patient records hit in ransomware attack. Recuperado de: https://www.modernhealthcare.com/cybersecurity/utah-practice-says-320000-patient-records-hit-ransomware-attack

[28] Davis, J. (2019). Ohio Provider Pays $75K Ransom After Serious Hack on IT System. Recuperado de: https://healthitsecurity.com/news/ohio-provider-pays-75k-ransom-after-serious-hack-on-it-system

[29] Vallas, C. (2019). Boardman medical practice hacked, told to pay $75,000 in bitcoin to unlock system. Recuperado de: https://www.wfmj.com/story/40646778/boardman-medical-practice-hacked-told-to-pay-75000-in-bitcoin-to-unlock-system

[30] Davis, J. (2019). 3 Alabama Hospitals Pay Hackers Ransom to Restore System. Recuperado de: https://healthitsecurity.com/news/3-alabama-hospitals-pay-hackers-ransom-to-restore-system

[31] Davis, J. (2019). Kentucky Provider Pays $70,000 Ransom to Unlock Patient Data. Recuperado de: https://healthitsecurity.com/news/kentucky-provider-pays-70000-ransom-to-unlock-patient-data

[32] Davis, J. (2019). Hackers Demand $1M in Grays Harbor Ransomware Attack. Recuperado de: https://healthitsecurity.com/news/hackers-demand-1m-in-grays-harbor-ransomware-attack

[33] Monica, K. (2019). Grays Harbor Community Hospital Initiates EHR Downtime Protocol. Recuperado de: https://ehrintelligence.com/news/grays-harbor-community-hospital-initiates-ehr-downtime-protocol

[34] Davis, J. (2019). Michigan Practice to Shutter after Hackers Delete Patient Files. Recuperado de: https://healthitsecurity.com/news/michigan-practice-to-shutter-after-hackers-delete-patient-files

Sobre el autor:

Ingeniero en Sistemas de Información y Máster en Seguridad Informática en la Universidad Mariano Gálvez de Guatemala, con 10 años de experiencia en proyectos que incluyen los procesos de análisis, desarrollo e implementación de Sistemas de Información para las áreas de Telefonía, Banca y Recursos Humanos, a través de metodologías tales como Personal Software Process (PSP), Team Software Process (TSP), XP y SCRUM.

Conocimientos de desarrollo e implementación de Sistemas de Información en lenguaje RPG y herramientas como como SEU, RLU, SDA y PDM de IBM AS/400, así como de integración de estos sistemas con otros sistemas y aplicaciones.

Actualmente, desempeñando funciones de consultoría y administración en SAP SuccessFactors dentro de la organización que incluye actividades como Implementación de SAP SuccessFactors y su modelo de Recursos Humanos en diversas organizaciones. Consultoría Interna para SAP SuccessFactors 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 SuccessFactors frente a actualizaciones de versiones, incidentes y nuevas funcionalidades y Administración principal de accesos y configuraciones dentro de SAP SuccessFactors.

Análisis de la normativa JM 42-2020 de la Junta Monetaria para implementarla en PyMes de Guatemala

Analysis of the JM 42-2020 regulation of the Monetary Board to implement it in SMEs in Guatemala

Joshua Joel Arrivillaga Velasco
email: josharrivillaga@gmail.com

Levi Estib Gálvez Pérez
email: levigalvez4bib@gmail.com

Recibido:12/septiembre/2020. Revisado: 3/octubre/2020. Aprobado: 10/noviembre/2020.
Disponible en internet el 1 de enero de 2021

Resumen: La resolución JM-42-2020 modifica el Reglamento para la Administración del Riesgo Tecnológico emitido en la Resolución JM-102-2011, el cual establece los lineamientos mínimos que los bancos, las asociaciones financieras, las entidades fuera de plaza o entidades off shore y las empresas especializadas en servicios financieros, deben de observar y cumplir para administrar el riesgo tecnológico, por lo que esta normativa incorpora la gestión de la ciberseguridad. Esta norma fue aprobada por la Junta Monetaria del Banco de Guatemala, a raíz del crecimiento y desarrollo tecnológico que las entidades financieras han tenido que experimentar para poder competir y sobre todo mantenerse dentro del mercado en el que se desenvuelven, ya que esto ha hecho que sus transacciones y comunicaciones, sean más agiles y accesibles para sus colaboradores y clientes o cuentahabientes.

El crecimiento tecnológico no solo ha traído ventajas, también se han desarrollado nuevas amenazas cibernéticas, lo cual pone en riesgo la disponibilidad, confidencialidad e integridad de su información, así como la continuidad del negocio. Es por eso que esta Normativa trata sobre la Ciberseguridad dentro de estas instituciones.

En este documento se presentan las oportunidades y retos que las Pequeñas y Medianas Empresas –PYMES- tendrían o afrontarían, si les fuera aplicada esta normativa. Algunas empresas podrían cumplir con lo que la normativa establece, dependiendo del tipo de operaciones o tamaño de la empresa, ya que siempre es necesario invertir en ciberseguridad para evitarse perdidas, mala reputación o la no continuidad del negocio.

Palabras Claves: Riesgos tecnológico, ciberseguridad, reglamento, ley, políticas, procedimientos.

Abstract: Resolution JM-42-2020 modifies the Regulation for the Administration of Technological Risk issued in Resolution JM-102-2011, which establishes the minimum guidelines that banks, financial associations, off-market entities or off shore entities and

companies specialized in financial services must observe and comply to manage technological risk, so this regulation incorporates cybersecurity management. This standard was approved by the Monetary Board of the Bank of Guatemala, as a result of the growth and technological development that financial institutions have had to experience in order to compete and above all stay within the market in which they operate, since this has made your transactions and communications are more agile and accessible for your collaborators and clients or account holders.

Technological growth has not only brought advantages, new cyber threats have also developed, which puts the availability, confidentiality and integrity of your information, as well as business continuity at risk. That is why this Regulation deals with Cybersecurity within these institutions.

This document presents the opportunities and challenges that Small and Medium-sized Enterprises –PYMES- would have or would face, if this regulation were applied to them. Some companies could comply with what the regulations establish, depending on the type of operations or size of the company, since it is always necessary to invest in cybersecurity to avoid losses, bad reputation or non-continuity of the business.

Desarrollo:

En este documento analizaremos la Resolución JM-42-2020 donde la Junta Monetaria de la Superintendencia de Bancos en Guatemala, propone, realizar algunos cambios a su forma de abordar la administración del riesgo tecnológico; pero antes de entrar en materia comencemos por definir una norma, ¿Qué es?, ¿Para qué sirve? Y ¿Dónde se utiliza?, bueno pues, “se conoce como normativa a un conjunto de normas que dirigen y adaptan el comportamiento de un individuo, organización y/o actividad” (Significados, 2016).

Una normativa es utilizada comúnmente dentro de organizaciones y su cumplimiento es bastante importante, ya que al regir el comportamiento y funciones de cada uno de los colaboradores crea una convivencia más agradable y con esto alcanzar los objetivos trazados es más accesible.

Establecer una normativa dentro de una organización conlleva el establecimiento de reglas y políticas que regulan los procedimientos dentro de la organización, dejando constancia no solo de que hacer y cómo hacerlo, si no también, de las consecuencias que conlleva el no cumplir a cabalidad los lineamientos.

Otro punto interesante es conocer quien propone la normativa, en este caso la Junta Monetaria del Banco de Guatemala, ¿Quiénes son?, ¿Cuál es su función?, pues la Junta Monetaria, según la Constitución Política de la República de Guatemala (1985) es el ente que dirige el Banco de Guatemala, y su función principal, según el artículo 133, establece que “tendrá a

su cargo la determinación de la política monetaria, cambiaria y crediticia del país y velará por la liquidez y solvencia del sistema bancario nacional, asegurando la estabilidad y fortalecimiento del ahorro nacional" (1985, art. 133).

La Junta Monetaria o JM tiene como finalidad garantizar la estabilidad monetaria del país y en caso de catástrofes o desastres públicos, puede financiar a entidades del estado, siempre y cuando sea aprobado por el organismo legislativo de nuestra Nación. Una vez fundamentada la parte inicial de nuestro análisis, entremos en materia y analicemos en que consiste la normativa 42-2020 de la Junta Monetaria publicada en los medios oficiales.

Esta normativa, dada a conocer en marzo 2020, da a conocer la propuesta donde la junta monetaria busca realizar cambios al reglamento para la administración de riesgos tecnológicos, pero ¿Por qué?, ¿De qué cambios hablamos?, ¿Qué conlleva? Veamos más a fondo.

En su momento, cuando se emitió el reglamento, se pensó en únicamente en los requisitos mínimos, que las entidades que conforman el sistema financiero del país (bancos, sociedades financieras, off shore y empresas especializadas en servicios financieros) debían observar para administrar el riesgo tecnológico; ahora ante un notorio crecimiento y desarrollo tecnológico, la fluidez con la que se intercambia información y se generan comunicaciones, conlleva también un incremento en la existencia de amenazas cibernéticas, poniendo en riesgo la disponibilidad, integridad y confidencialidad de los activos digitales, aunado a esto también pone en riesgo la prestación de servicios por partes de las entidades mencionadas.

Hoy en día es indispensable, para las entidades del sector financiero del país gestionar de manera eficiente la ciberseguridad, gestión que les permita: detectar (riesgos, amenazas, vulnerabilidades, ataques, etc.), resistir, responder y en cualquier caso recuperarse de forma rápida ante incidentes cibernéticos.

Dentro de las modificaciones propuestas al reglamento lo más notorio es la implementación de un nuevo rol, como lo es el Oficial de Seguridad de la información, también conocido como Chief Information Security Officer – CISO por sus siglas en inglés, la creación e implementación de un Centro de Operaciones de Seguridad Cibernética, un equipo capacitado para respuestas a Incidentes Cibernéticos y aspectos de ciberseguridad para contratar proveedores.

Para comprender un poco mejor veamos cada una, comencemos por el Oficial de Seguridad de la información, ¿cuál es la definición?, ¿Qué perfil debe tener un Oficial de Seguridad?, ¿Qué responsabilidades tiene?

Arranquemos por definir el rol, pues un CISO, es el director de seguridad de la información, desempeñándose más a nivel ejecutivo y la principal función es de alinear la seguridad con

los objetivos del negocio, viéndolo así garantiza que todo el tiempo la información está correctamente custodiada.

En cuanto al perfil que debe tener un CISO, este debe ser un profesional del área de la informática, amplia experiencia en nuevas tecnologías y demostrar amplia experiencia en seguridad de la información, aunado a esto deberá poseer conocimientos legales, acompañando esto con certificaciones internacionales (Certificación de Auditor de Sistemas de Información, Certificación en Riesgos y Control de Sistemas de información, Gestión de la Seguridad de la información, por mencionar algunas).

¿Qué responsabilidades tiene un CISO?, pueden ser varias, pero mencionaremos algunas, por ejemplo: Generar e implementar políticas de seguridad, garantizar la seguridad y privacidad de los datos, supervisar el control de acceso a la información, supervisar el cumplimiento normativo de la organización, liderar el equipo de respuesta ante incidentes de seguridad y supervisar la arquitectura de seguridad.

Y ya que estamos en el tema, veamos algunas funciones que pudimos consultar en el libro blanco del CISO: Alinear la estrategia de ciberseguridad con los objetivos de la empresa, prevenir, detectar y analizar vulnerabilidades, informar y reportar a la alta dirección, dar respuesta rápida ante cualquier incidente cibernético y educar, concientizar y sensibilizar a la organización en materia de seguridad de la información.

Otro de los puntos a mejorar planteados dentro de la normativa es la creación e implementación de un Centro de Operaciones de Seguridad Cibernética o SOC por sus siglas en inglés, ¿a qué se refiere con esto?, pues a creación un centro donde se encargarán de dar seguimiento y análisis a la actividad que se lleva a cabo en redes informáticas, servidores, puntos de trabajo, bases de datos, aplicaciones, sitios web, entre otros, monitoreando constantemente en búsqueda de actividades anómalas y así tener indicios de incidentes cibernéticos o de la seguridad de la información comprometida.

Un centro de operaciones de Seguridad Cibernética es el total responsable de que todos los posibles incidentes se identifiquen, se analicen, se defiendan, investiguen y se documenten e informen adecuadamente.

A su vez un Centro de Operaciones tiene como objetivo principal:

· Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias, Analizar los ataques o posibles amenazas. Recuperar información perdida o dañada a consecuencia de ataques o incidentes. Mejorar la capacidad de respuesta ante cualquier ataque.

¿Qué actividades realiza un Centro de Operaciones de Ciberseguridad?

Establece conciencia de activos, el monitoreo continuo y proactivo, la clasificación de alertas, el ajuste de las defensas (gestión de vulnerabilidades) y la comprobación de cumplimiento

Aunado a esto la JM propone definiciones básicas de términos tecnológicos que no profundizaremos en este análisis, pero que pueden ser leídos en los anexos. Lo que si analizaremos es el "Articulo No. 3" que hace especial referencia a políticas y procedimientos, ¿De qué habla este articulo? Pues básicamente habla de que se deben implementar políticas que dicten el camino a seguir para una correcta administración del riesgo tecnológico, políticas que, acompañadas de los procedimientos adecuados, comprenderán las metodologías, herramientas y/o modelos de medición de riesgos.

Debemos tener presente que una política son declaraciones formales de las reglas que se deben cumplir dentro de la organización e involucran a toda persona que tenga acceso a la información y activos tecnológicos.

Una política tiene tres características básicas, deben ser concretas, contar con procedimientos, reglas y pautas claras; deben ser claras, definir de forma clara las responsabilidades y obligaciones de los distintos usuarios y deben ser obligatorias, respetar siempre su cumplimiento, dejando constancia de las sanciones de no seguirla al pie de la letra.

Beneficios para implementarla en PYMES de Guatemala

Las PYMES son pequeñas y medianas empresas, las cuales poseen un límite en cuanto su cantidad de puestos de trabajo y capital. Una empresa es considerada PYME cuando posee entre 1 y 200 empleados, aunque esto puede variar también según su nivel de facturación (PYMES, 2018).

Comúnmente este tipo de empresas están alineadas al mercado o comercio por el tipo de capital que estas manejan, donde el costo de inversión no es tan elevado a comparación del mercado industrial, donde rara vez se pueden situar.

Las pequeñas y medianas empresas (PYMES) de la República de Guatemala pueden ir abriendo brecha hacia la nueva era digital, la cual avanza a pasos agigantados, en este año 2020 el crecimiento es eminente, con el brote de la pandemia causada por el nuevo coronavirus Covid-19, ha ayudado al crecimiento digital. Muchas pequeñas y medianas empresas empezaron a modernizar sus procesos, por ejemplo, implementando servidores web, implementación de páginas web, uso de las nubes informáticas, con la finalidad de agilizar los procesos y poder vender los productos de una manera más productiva y generando más satisfacción y comodidad a los clientes.

Ahora bien, sabiendo que, en las tecnologías de información, no hay un 100 por ciento de seguridad, el cual es aprovechado por los ciberdelincuentes, que siempre andan buscando vulnerabilidades en los sistemas y las redes de telecomunicaciones con la finalidad de infiltrarse y poder robar, infectar o secuestrar información confidencial organizacional. Entonces siempre se trata de hacer uso de algunas herramientas que nos ayude a mitigar el riesgo para que dicha vulnerabilidad no sea explotada y cause un impacto muy severo a la organización.

¿Se puede implementar la Normativa JM-42-2020 para la Administración del Riesgo Tecnológico en las Pymes?

Este tipo de empresas para poder operar, crecer y lanzar nuevos productos, buscan fondos, sin embargo, en Guatemala hay poco acceso a financiamiento. Considerando todo lo que dicta la normativa como tal, y que las Pymes como tal no cuentan con un presupuesto tan elevado para implementar.

Sabiendo que las pymes no tienen la robustez financiera necesaria para costear la implementación de esta normativa como tal, pero considerando que ya cuentan con una gestión de procesos y que los datos están expuestos, porque ya cuentan con plataforma digital. Entonces se pueden administrar algunos lineamientos que rige esta normativa para llevar un control que ayude a Administrar de una manera esencial el Riesgo Tecnológico.

Funcionamiento de Políticas y Procedimientos

Según el artículo 3 de esta normativa el cual hace mención a las “políticas y procedimientos” estas políticas deben de ser tomadas en cuenta en las siguientes áreas y procesos:

Area de infraestructura de TI, incluyendo sistemas de información, base de datos, y servicios de TI, Seguridad de tecnologías de información y Ciberseguridad.

Las políticas ayudaran de una manera más proactiva a la Administración del Riesgo tecnológico según sea el tipo de negocio, estas políticas también pueden ser tomadas en cuenta o implementarla a los empleados que manejan los sistemas de información con la finalidad de que estos tomen las medidas necesarias a la hora de realizar las operaciones y tener una base para actuar ante algún tipo de incidente.

Otro aspecto que se debe de tomar en cuenta en las pymes en relación con la normativa 42-2020 es el caso de la ciberseguridad, la pregunta es ¿Por qué un ciberdelincuente se fijaría en una entidad pequeña y no en una grande? El motivo más grande es porque los ciberdelincuentes saben que las grandes instituciones invierten en herramientas tecnológicas tanto en hardware como en software para mantener un mejor control sobre la gestión de todo tipo de riesgos incluyendo los tecnológicos, entonces ellos sabiendo que la presa más fácil y que saben que carecen de una buena seguridad, por tal motivo tratan de vulnerar empresas

más pequeñas lo cual le tomaría menos tiempo para lograr infiltrarse. Por lo tanto, se puede decir que "La poca inversión de las pequeñas y medianas empresas en ciberseguridad es el principal riesgo de que estas sufran ataques a sus sistemas informáticos" (TUYU, 2017).

Mejores Prácticas en la seguridad cibernética

Uno de los puntos claves para llevar una buena gestión del riesgo tecnológico y que no genera un coste elevado para la implementación, es la implementación de las buenas prácticas.

Ya que las Pymes no cuentan con un presupuesto alto para invertirlo en ciberseguridad, se pueden implementar algunas mejoras, tratando de sectorizar las áreas más críticas y que pueden causar un impacto severo si llegara a sufrir algún tipo de ataque cibernético. Las áreas que deben de contar con un grado de ciberseguridad aceptable son:

Seguridad en las páginas web

Muchas de las pymes cuentan con servicios online por eso es de mucha importancia cuidar que el contenido de esta sea veraz y que no se introduzca diferentes malware en los equipos de sus clientes es indispensable. Un sencillo hackeo puede modificar el contenido de la web, introducir SPAM, robarnos datos de los formularios entre otro tipo de hackeos posibles.

Proteger el email de los empleados que tengan acceso al sistema de información

Sabiendo que el eslabón más débil con la que cuenta toda entidad ya sea, financiera, industrial, empresas públicas entre otras son los empleados, si se sabe que ellos son la presa más fácil a la cual puede manipular los ciberdelincuentes ¿Por qué no protegerlos o tomarlos muy en cuenta en la gestión de ciberseguridad? El correo electrónico es la principal vía de entrada de software malicioso. Por tal motivo se deben implementar políticas de seguridad de la información, capacitar constantemente a los empleados etc.

Protección en las redes de telecomunicaciones y wifi abiertos

Muchas veces no se sectorizan las redes en las empresas pequeñas quizá porque no hay necesidad, ya sea porque no se cuentan con un numero de host en funcionamiento o porque no se lleva un control de esta. Y otro de los puntos muy importantes son que las empresas crean la zona de red wifi abiertas para que los visitantes tengan acceso gratis, sin embargo, no saben los peligros a los que se enfrentan si llegara algún tipo de persona con conocimientos avanzados en informática.

Ventajas u oportunidades al implementar la Norma JM-42-2020 en las PYMES.

Aunque la normativa va dirigida a aquellas empresas que se dedican a servicios financieros, las cuales están obligadas a cumplir lo que en ella se establece, las Pequeñas y Medianas Empresas –PYMES- dependiendo del giro de comercio u actividad económica a la cual se

dediquen, pueden implementar varias acciones que lo norma estipula, ya que está, ha sido promovida y aprobada para mejorar la información de una institución, en relación a ciberdefensa, para gestionar y tratar el riesgo tecnológico.

Dentro de las ventajas que se obtendrían dentro de las PYMES e pueden mencionar algunos, tales como:

1. Crear una cultura de seguridad de la información, por medio del programa continuo de capacitación del recurso humano y concientización a los usuarios de la institución.

2. Contar con el Equipo de Respuesta de incidentes Cibernéticos, un Comité de Gestión de Riesgos y una unidad de Administración de Riesgos, los cuales deben de estar formados por personal multidisciplinario de las distintas áreas de la institución.

3. Contar con el Plan Estratégico de TI alineado a la estrategia del negocio.

4. Roles y responsabilidades para la gestión de la seguridad de la información bien definidos.

5. Incorporar aspectos de ciberseguridad en la contratación de proveedores.

6. Administrar y gestionar el riesgo tecnológico de la institución, tomando en cuenta o considerando la naturaleza, complejidad y volumen de sus operaciones.

7. Contar con el Plan de Recuperación de Desastres, el cual deberá estar alineado al Plan de Continuidad del Negocio.

8. Crear un nivel de confianza en los clientes o stakeholders con relación al manejo y seguridad de su información.

Desventajas o limitantes para la implementación de la Norma.

Uno de los aspectos más críticos para la implementación de la Normativa JM-42-2020 es el tema financiero, ya que muchas de las PYMES en Guatemala, no cuenta con el capital suficiente para poder implementar lo que la normativa establece, en relación a personal, procesos y tecnología necesaria para cumplir a cabalidad dicha normativa. En la figura 1, se puede observar el rango de ventas anuales en las que se ubican las Pequeñas y Medianas Empresas.

Dentro de las desventajas o limitantes que este tipo de empresas podrían tener para poder implementar esta Normativa, podemos listar algunas:

1. Bajos ingresos y altos cotos para la contratación de personal profesional en materia de ciberseguridad, tal es, el caso de un CISO dentro de la organización.

2. Resistencia al cambio por parte del personal existente dentro de la institución.

3. Poca y/o infraestructura de TI inadecuada, la cual no cuenta con capacidad o rendimiento necesario para administrar y gestionar el riesgo.

4. Necesidad de inversión en equipo tecnológico o contratación de proveedores para involucrar a terceros en las infraestructuras para el almacenamiento y seguridad de la información.

Conclusión

Aunque falta mucho por hacer para normar todo lo relacionado a la ciberseguridad en Guatemala, la Normativa JM-42-2020 de la Junta Monetaria, es un paso importante dentro del grupo financiero del país, para que quienes forman parte de él, como los bancos, las sociedades financieras, las entidades fuera de plaza o entidades off shore y las empresas de servicios financieros, puedan administrar el riesgo tecnológico, por medio del reglamento, el cual por medio de esta normativa, incorpora la gestión de la ciberseguridad, para la disponibilidad, confidencialidad e integridad de la información y continuidad del negocio. En relación a la implementación en las Pequeñas y Medianas Empresas, consideramos que, por el tamaño económico de estas, es bastante difícil y complicado que estas tengan la capacidad para poder cumplir con todo lo que la Normativa establece, por lo que deberá existir una normativa específica para este tipo de empresas, pero según su crecimiento deberán invertir Tecnologías de Información, sin dejar por un lado la inversión en ciberseguridad e implementar políticas, estrategias y planes de respuesta y recuperación de desastres, los cuales deben de estar alineados al Plan de Continuidad del negocio. Así mismo, deberán crear equipos, comités y unidades para la Gestión de la ciberseguridad, tomando en cuenta los perfiles y pericias del personal existente.

Se puede decir que las pequeñas y medianas empresas (PYMES)son presa fácil para los ciberdelincuentes ya que estas no cuentan con una infraestructura sólida y con una buena administración del riesgo tecnológico debido al bajo presupuesto que estas manejan y por lo difícil que es en Guatemala buscan fondos para operar, crecer o lanzar nuevos productos, mucho menos lo hay para dedicarle un presupuesto a la ciberseguridad. Exponiendo de esta forma toda la información organizacional.

Referencias bibliográficas

Al, J. (16 de Abril de 2015). portaley. Obtenido de Qué es y cómo combatir el cibercrimen: https://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/

guiaspracticas. (06 de Mayo de 2017). guiaspracticas. Obtenido de Información sensible: http://www.guiaspracticas.com/recuperacion-de-datos/informacion-sensible

INCIBE . (30 de Noviembre de 2016). INCIBE . Obtenido de CEO, CISO, CIO… ¿Roles en ciberseguridad?: https://www.incibe.es/protege-tu-empresa/blog/ceo-ciso-cio-roles-ciberseguridad

Perez Porto, J., & Gardey, A. (2016). Definicion.de. Obtenido de base de datos: https://definicion.de/base-de-datos/

PYMES. (2018). enciclopediaeconomica. Obtenido de ¿Qué son las PYMES?: https://enciclopediaeconomica.com/pymes/

riesgotecnologico. (22 de Mayo de 2013). riesgotecnologico. Obtenido de Riesgo tecnológico: riesgotecnologico.blogspot.com

Significados. (07 de Septiembre de 2016). significados.com. Obtenido de Significado de Normativa: https://www.significados.com/normativa/

sistemius. (24 de Abril de 2020). sistemius. Obtenido de Ciberdelincuencia: Los 4 delitos informáticos más comunes: https://www.sistemius.com/ciberdelincuencia-4-tipos-de-delitos-informaticos/

TUYU. (03 de Julio de 2017). tuyu.es. Obtenido de La importancia de la ciberseguridad en las PYMES: https://www.tuyu.es/ciberseguridad-pymes/

welivesecurity. (16 de Junio de 2015). welivesecurity. Obtenido de ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia: https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Resolución JM-42-2020 (2020). Diario de Centro América, Ciudad de Guatemala, Guatemala, 24 de abril de 2020.

Constitución Política de la Republica (1985). Ciudad de Guatemala, Guatemala, 31 de mayo de 1985.

Ley Orgánica del Banco de Guatemala, Decreto No. 16-2002 (2002). Diario de Centro América, Ciudad de Guatemala, Guatemala, 1 de junio del año 2002.

Ministerio de Economía (2020). Fondo de Garantía MIPYME. Recuperado el 09 de septiembre de 2020, extraído de MINECO: URL: https://www.mineco.gob.gt/sites/default/files/Fondo%20de%20Garantia%20MIPYME.pdf

Asociacion de la Pequeña y Mediana Empresa de Guatemala (2020). Politica económica 2016-2021. Recuperado el 09 de septiembre de 2020, extraido de ASOPYME: https://asopyme.org/sector-mipyme/

Resolución JM-102-2011 (2011). Diario de Centro América, Ciudad de Guatemala, Guatemala, 26 de agosto del año 2011.

Superintendencia de Bancos (2018). Directorio de Grupos Financieros y entidades Supervisadas. Recuperado el 09 de septiembre de 2020, extraído de SIB: URL: https://www.sib.gob.gt/web/sib/entisup?__cf_chl_jschl_tk__=d68a398a9f0a81b831b676600243fb627acca7ac-1599799171-0-AdeIQZmxNQJqZDmvJTpVAKCIIK0vQNN5atJao-BGNM__Ti-S_XrWaJAHK5caRyYvfNISchVzFeygc-qbZEKJQ7E4bdFEVGYreVe6pH1VRr2a0aj0xAI07cpov4xAjSSW538grPls4i7eHY953ocjJRgOAhMwBIc2L4U4d5Yg43VKlkFKBFpNyGZbhP65nmPD5l_Fb46rxi8k-SEtaASFoQalLf5iSnswFJQ7ZGMAynNQX09BzBZndl_8KhNWlHoBy82IhvAVyLifGyl7MDPelDjKd88BeVHUJSdba4L-Gvia

Ministerio de Economía (2020). Servicios Financieros. Recuperado el 09 de septiembre de 2020, extraído de MINECO: URL: https://www.mineco.gob.gt/servicios-financieros

Inter-American Development Bank(2015). Directorio de Servicios financieros para PYMES en Guatemala. Recuperado el 09 de septiembre de 2020, extraído de Connect Americas: URL: https://connectamericas.com/es/service/directorio-de-servicios-financieros-para-pymes-en-guatemala

Sobre de los autores:

Joshua Joel Arrivillaga Velasco, Ingeniero en Sistemas, estudiante de Maestría de Seguridad Informática. Instructor de formación profesional actualmente desempeño la función de jefe de IT en una empresa de la agroindustria, con experiencia en formación profesional impartida en INTECAP y desarrollo de software y soporte en el comercio local. Certificaciones: MTA Introduction to Java, MTA Introduction to Python, MTA Data Base Fundamentals, Microsoft Certified Educator.

Levi Estib Gálvez Pérez, Sistemas de Información y Ciencias de la Computación cuenta con una Maestría en Seguridad Informática. Laborando actualmente en el área de electrónica y microprocesadores.

Elementos básicos para una Ley de Protección de Datos Personales

Basic elements for a Personal Data Protection Law

Ciro Edgardo Camey Valdez
email: ciro_ev@tuta.io

Anthony Azurdia de León
email: tony7_azurdia@hotmail.com

Ricardo Valentín Fuentes Pérez
email: rfuentesp1@miumg.edu.gt

Juan Antonio Rivera Mérida
email: antoniorivm1394@gmail.com

José Adolfo Pineda Guerra
email: adopin10@gmail.com

Recibido:6/octubre/2020. Revisado: 12/octubre/2020. Aprobado: 23/noviembre/2020.
Disponible en internet el 1 de enero de 2021

Resumen: En la actualidad se manejan millones de datos personales, para poder gestionar a distintos servicios o acceder a determinados contenidos, los cuales deben proporcionar previamente ciertos datos de carácter personal, y que deberían de ser utilizados para el propósito que fueron recopilados, con ello se dan muchas anomalías por los diferentes tipos de datos, estableciendo con ello la responsabilidad de su tratamiento, la transparencia, la cesiones de datos, el uso establecido a la intimidad, dando para ello muchos parámetros para su utilización, aunque la información que se recaba necesita de cierta protección y confidencialidad para salvaguardar a la persona, ya que gracias a la tecnología se puede facilitar este proceso pero se necesita una protección a nivel jurídico para establecer reglas que instruyan su aplicabilidad para su uso correcto.

Por lo tanto, se necesitan elementos o puntos básicos para una ley de protección de datos personales, ya que la legislación en Guatemala carece y necesitan leyes que ayuden a establecer elementos que constituyan una falta o delito (se puede definir al delito como una "acción u omisión típica, antijurídica, culpable y punible.) sobre su mal uso sobre la protección de nuestros datos personales.

Dichos elementos deben darles protección a los datos personales en materia de principios sobre su uso, uso posterior, ámbito territorial, responsabilidades hacia la persona, privacidad, derecho al olvido de información, así como la desconexión digital del mismo y una neutralidad de los datos en la red.

Con la asistencia de los elementos, se podría establecer una ley que obligaría a todas las personas, empresas y organismos, tanto privados como públicos que dispongan de datos de carácter personal a cumplir una serie de requisitos y aplicar determinadas medidas de seguridad en función del tipo de datos que posean, cómo principio general, no compartir ni revelar información obtenida, excepto cuando haya sido autorizada por usted, o en ciertos casos cuando sean necesarios para salvaguardar la integridad de las personas.

Abstract: Millions of personal data are currently handled, in order to manage different services or access certain content, which must previously provide certain personal data, and which should be used for the purpose they were collected, thus providing many anomalies for the different types of data, thus establishing responsibility for their processing , transparency, data transfer, the use established to privacy, giving for this purpose many parameters for its use, although the information that is collected needs some protection and confidentiality to safeguard the person, since thanks to technology this process can be facilitated but protection is needed at the legal level to establish rules that instruct its applicability for its correct use.

Therefore, basic elements or points are needed for a personal data protection law, as legislation in Guatemala lacks and needs laws that help establish elements that constitute a misdemeanor (crime can be defined as a "typical, anti-legal, guilty and punishable action or omission.) misuse over the protection of our personal data.

Such elements should protect personal data in terms of principles about its use, subsequent use, territorial scope, responsibilities towards the person, privacy, the right to forget information, as well as the digital disconnection of the same and a neutrality of the data on the network.

With the assistance of the elements, a law could be established that would oblige all individuals, companies and bodies, both private and public, that have personal data to meet a number of requirements and apply certain security measures depending on the type of data they hold, how general principle, not to share or disclose information obtained, except where authorized by you , or in certain cases where necessary to safeguard the integrity of persons.

Palabras Claves: datos informáticos, robo de información, aseguramiento, protección de información.

Desarrollo:

En el presente documento se muestra un listado de los elementos y puntos básicos para la creación de una ley de protección de datos personales. Guatemala carece de reglamentos definidos para poder sancionar la violación de privacidad de toda información personal de las personas. Dentro del listado de elementos, también se redactará los niveles de accesos

que las instituciones tanto públicas como privadas pueden obtener a la misma información y el tratamiento adecuado que se le debe de dar a la misma.

Aplicación de la ley: Las reglas deben de aplicarse sobre todos los datos personales sensibles de las persona física o jurídica, independientemente de su nacionalidad, residencia o domicilio.

Definición de palabras claves: Está categoría tiene como objetivo definir todas aquellas palabras a efecto de la ley. Datos informáticos, Protección de datos y Robo de información

Calidad de Datos: En esta parte se debe de definir las dimensiones de calidad, que son aspectos cualitativos que pueden representar una faceta de alto nivel de la calidad de datos. Por ejemplo se debe de conocer ¿Cómo se están actualizando los datos?, ¿Se tienen los datos completos?, ¿Todos los datos con los que se cuentan son totalmente íntegros y correctos? dentro de la ley se deben de contestar las preguntas planteadas con anterioridad, para un tratamiento correcto de los datos, para conocer cuáles son las vías con las que se están actualizando, si todos los datos están completos y no existen huecos dentro de nuestros registros de información y de último, conocer si los datos son correctos. para una correcta calidad de datos se debe de evaluar los factores de calidad sobre la exactitud de estos. En esta se muestran los aspectos sintácticos y semánticos de los datos.

Ámbito territorial: Existe una Iniciativa de Ley en el Congreso de la República de Guatemala identificada con el número 4054 y titulada "Ley Contra el Cibercrimen". con la finalidad de darle al Estado y a la sociedad las herramientas que le permitan prevenir y reprimir estas nuevas manifestaciones criminales, en donde conceptualiza un punto importante, el avance de la tecnología en la actualidad es constante y que se debe emitir una ley sobre delitos informáticos lo más amplio posible, eso sí, sin caer en el problema que cualquier actividad que realicemos a través de una herramienta informática pueda encuadrarse dentro de la actividad tipificada como delito. Lo que conlleva a un problema que es el ámbito territorial refiriendo a cómo aplicarse al momento de aplicar la persecución penal en el territorio y fuera del territorio

Aunque el Comité de Ministros del Concilio de Europa aprobó la solicitud de Guatemala de acceder a la Convención de Budapest, dicho convenio ayudará a los legisladores al momento de tipificar conductas delictivas, ya que el Estado de Guatemala enfrenta el mayor de los problemas, el cual es poder aplicar la ley a un caso práctico. Y en la práctica el Convenio de Budapest es el único instrumento internacional vinculante sobre este tema ya que el objetivo principal de este instrumento es establecer una política penal común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia, esto se alcanza tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales y a través de una cooperación internacional armónica.

Considerando con ello un mejor tratamiento enfocado a los datos personales en el contexto de actividades de un establecimiento del responsable así como independientemente del tratamiento que tenga el lugar.

Licitud del tratamiento: La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento de protección de datos, será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas, las cuales solo así obtendrán la licitud:

El interesado dio su consentimiento expreso para el tratamiento de sus datos. El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para a la aplicación a petición de éste de medidas precontractuales. Siempre tienen que informar previamente mediante una cláusula informativa. El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento. El tratamiento es necesario para proteger los intereses vitales del interesado o de otra persona física. El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. El tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre esos intereses no prevalezcan los intereses o derechos y libertades del interesado que requieran la protección de datos personales, en particular cuando sea de un niño.

Seguridad de los datos: En este punto nos enfocaremos en la iniciativa de ley 4055 Ley de Delitos Informáticos que se propuso dentro del Congreso de la República de Guatemala en donde se busca sancionar de forma penal los delitos de hacking, cracking, phishing, smishing y vishing, es por eso por lo que se creó esta iniciativa con el fin de proponer una protección para los datos personales mediante la creación de una unidad de investigación especial para este tipo de delitos. Es por eso, que en el artículo 4 se cita: “Acceso sin autorización: El que sin plena autorización, acceda, intercepte, interfiera o utilice un sistema o dato informático, de naturaleza privada o público y de acceso restringido, será penado con prisión de dos a seis años”.

Cesión de datos: Toda cesión o comunicación de los datos o base de datos ya bien sea públicos o privados debe ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello, en todo caso será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando tenga un interés legítimo para su tratamiento o

conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado, en todo caso se deberá de tomar en cuenta lo mencionado anteriormente en seguridad de los datos donde se sancione de forma penal los delitos de hacking, cracking, phishing, smishing y vishing, relacionado a la iniciativa de ley 4055.

Derechos y garantías: Tener el derecho de acceder a cualquier registro o banco de datos a la propia información, debe tenerse en cuenta que cualquier tipo de cesión de datos personales debe venir precedida de la información adecuada y pertinente al titular de los datos personales.

La información debe de presentarse de forma clara y exenta de encriptaciones en todo caso una explicación de los términos técnicos que se utilicen, a opciones del titular la información puede solicitarse por medios físicos o electrónicos u medio seguro a fin de asegurar que la información no fue alterada o modificada en ningún momento por terceros.

El propietario de la información puede solicitar el borrar cualquier información que esté vinculada al mismo no obstante se encuentre en cualquier registro o banco de datos se deberá notificar el cese de toda información del propietario como tal.

Transferencia de datos: Las personas públicas y privadas encargadas del manejo de base de datos estarán exentas de transferir información que hayan recibido directamente del titular a terceros.

Si dado caso por algún motivo se deba de hacer transferencia la información de tercero que sea solicitada por una entidad pública o privada se debe de notificar al propietario de la información, a ese consentimiento se le llama aviso de privacidad, y a la persona que los pretende utilizar, responsable. El aviso de privacidad es un documento (físico o electrónico) que contiene información básica sobre quién es el responsable de los datos y las finalidades para las que pueden utilizarse, de modo que el titular pueda consentir o no dicho uso y así confirmar que no se vulneren los derechos y libertades fundamentales del interesado.

Si hubiera transferencia de datos de un tercero sin su debido consentimiento se deberá de tomar en cuenta lo mencionado en el punto de seguridad de los datos donde se sancione de forma penal los delitos de hacking, cracking, phishing, smishing y vishing, relacionado a la iniciativa de ley 4055.

Portabilidad de los datos: En este punto se busca como derecho del interesado, la física cuyos datos personales son objeto de tratamiento, a recibir del responsable del tratamiento si es que los datos se llegaran a transmitir mediante el consentimiento o el cumplimiento de un contrato ya preestablecido. Esto quiere decir que la ley ampara el compartir datos por parte de un interesado cuando el sujeto estuvo de acuerdo en compartir sus datos. Las empresas

emplean ciertas políticas para poder compartir cierta información de sus clientes, basándose en los contratos.

Notificación de una violación de la seguridad de los datos personales a la autoridad de control: Se toma como referencia la Reglamento General de Protección de Datos (UE RGPD), el cual es un reglamento europeo y como tal lo menciona en el artículo 33, en Guatemala también se debe de poseer un ente encargado de llevar el control del tipo de violación para poder imponer una sanción según el tipo de delito cometido. Estas sanciones se deberán dar a conocer en un lapso de 72 horas una vez presentadas las pruebas que den veracidad al delito.

Delegados de dirección de protección de datos, el tratamiento deberá delegarse a un ente que regule la responsabilidad de la protección de datos en función judicial sobre las sanciones o infracciones que conlleva el delito sobre condenas debido a su naturaleza, alcance y/o fines, requiriendo una observación habitual y sistemática de los interesados.

Sanciones: En esta sección se debe de incluir cuáles serán las multas establecidas, para toda aquellas:

a. *Faltas leves*, se considerará falta leve alguna de los siguientes:

   No proporcionando información a la Asociación Gubernamental de Protección de Datos - AGPD. No inscribir un fichero. Proceder a la recogida de datos de carácter personal sin proporcionar la información que señala la ley y otras que se consideren necesarias.

b. *Faltas graves*, se considerará falta grave alguna de las siguientes:

   Vulnerar el deber de secreto. No remitir a la Asociación Gubernamental de Protección de Datos la información requerida. Impedir u obstaculizar el ejercicio de derechos de acceso, oposición. Crear ficheros o iniciar la recogida de datos con fines distintos a los definidos e Incumplir el deber de información.

c. *Faltas muy graves,* Se considerará falta muy grave alguna de las siguientes: Recoger datos de forma engañosa o fraudulenta. No atender u obstaculizar el ejercicio de derechos de acceso. No atender el deber de la inclusión de datos en un fichero y comunicar o ceder datos personales fuera de los casos permitidos.

Certificación: Dentro de la ley se pueden definir mecanismos de certificación en materia de protección de los datos y la creación de sellos físicos o virtuales que demuestren el cumplimiento de todo lo definido en el reglamento a crear.

Vigencia: Se debe de establecer un periodo de tiempo donde la ley será vigente después de la publicación en el diario oficial, por ejemplo 5 días hábiles.

Conclusiones

Toda persona tiene derechos y garantías cuando de datos personales se habla en todo caso la cesión y la transferencia de datos, la persona, entidad privada o pública debe dar aviso de privacidad en un documento (físico o electrónico) que contiene información básica sobre quién es el responsable de los datos y la finalidades para las que pueden utilizarse, en caso contrario el propietario no esté informado, y no del consentimiento del manejo de la información propia a tercero se tomarán las acciones penales correspondientes.

En Guatemala se debe establecer leyes en vigencia que puedan respaldar la protección de los datos ya que únicamente se han creado iniciativas de ley más no se han concretado.

Las empresas tienen como obligación brindarles a los clientes la forma en que sus datos personales son tratados.

Los legisladores del congreso deben contemplar la opción de un consultor para temas informáticos y así puedan ser capaces de identificar el tipo de violaciones que se están cometiendo e imponer las sanciones respectivas dependiendo de la falta cometida, siendo esta leves, graves o muy graves.

Toda empresa dentro de Guatemala que manipula información sensible de personas debe de contar con una certificación en materia de protección de datos, donde se demuestra que cuentan con procedimientos adecuados para el almacenamiento y tratado de la misma.

Es prioridad agilizar el proceso de implantación del convenio de Budapest en Guatemala, para poder regular todo delito en materia informática y que sea un precedente para su tipificación, ya que actualmente el país carece totalmente de este tipo de leyes y sanciones respectivas.

Referencias bibliográficas

Ley N° 57-2008. Palacio de organismo legislativo, ciudad de Guatemala, Guatemala, 23 de septiembre de 2008.

Iniciativa de ley N° 4090. Palacio de organismo legislativo, ciudad de Guatemala, Guatemala, septiembre de 2008.

Iniciativa de ley contra el cibercrimen. Palacio de organismo legislativo, ciudad de Guatemala, Guatemala.

Iniciativa de ley de delitos informáticos 4055. Palacio de organismo legislativo, ciudad de Guatemala, Guatemala. Recuperado de: https://transdoc.com/assets/images/users/dani/file/Resumen_ejecutivo_ DELITOS_INFORMATICOS.pdf

Iniciativa de ley de protección de datos personales 4090. Palacio de organismo legislativo, ciudad de Guatemala, Guatemala, 2009. Recuperado de: http://www.oas.org/es/sla/ddi/docs/G7%20Iniciativa%204090-2009.pdf

GDPR made searchable by Algolia. Chapters, articles and recitals easily readable. (n.d.). Recuperado de https://gdpr.algolia.com/es/

Licitud del tratamiento. Curso DPO y Experto en el RGPD. (2019, August 28). Recuperado de https://iscibersegurídad.es/licitud-del-tratamiento-curso-dpo-y-experto-en-el-rgpd/

Oea. (2009, August 01). OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo. Recuperado de http://www.oas.org/es/sla/ddi/proteccion_datos_personales_dn_guatemala.asp

Portabilidad de datos: ¿Cómo puede asegurar este derecho una empresa? (2020, March 16). Recuperado de https://www.ticportal.es/glosario-tic/portabilidad-datos

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (n.d.). Recuperado de http://noticias.juridicas.com/base_datos/Privado/574082-regl-2016-679-ue-de-27-abr-proteccion-de-las-personas-fisicas-en-lo-que.html#a3

Sobre de los autores:

Anthony Azurdia, Asesor en enlaces punto a punto Wireless con más de 6 años en experiencia, Ingeniero en Sistemas de Información y Ciencias de la Computación, MA con especialidad en Seguridad Informática ambas por Universidad Mariano Gálvez de Guatemala, Conocimientos en infraestructura, equipos de redes LAN y Soporte técnico.

Jose Adolfo Pineda, Ingeniero en Sistemas de la Información y Ciencias de la Computación, así también, un postgrado en Seguridad Informática, ambos cursados dentro de la

Universidad Mariano Gálvez de Guatemala. Certificado en Técnico en Redes de Datos. Experiencia en atención al cliente y negociaciones. Emprendedor y Empresario.

Juan Rivera, Ingeniero en sistemas, culminando un postgrado en seguridad de la información ambos en la universidad Mariano Gálvez de Guatemala. 7 años de experiencia en programación, especialmente web, tanto frontEnd Javascript, como backEnd PHP (Laravel). Conocimientos en base de datos como Oracle, SQL Server y base de datos noSQL como MongoDB. Ha laborado en empresas tanto industriales como logísticas en el área de la costa sur en Guatemala. Analítico e implementador de proyectos.

Ciro Edgar Camey, Ingeniero en sistemas, con estudios en maestría en seguridad informática, ambos por Universidad Mariano Gálvez. Experiencia en implementación y evaluación de procesos, consultor para la reingeniería de procesos con enfoque de automatización y seguridad, así también en análisis de datos financieros en y propuesta de nuevas estrategias e implementación de estas.

Ricardo Fuentes, Ingeniero en sistemas de información y ciencias de la computación, y un postgrado en seguridad informática, de la Universidad Mariano Gálvez de Guatemala, con 6 años de experiencia en distintas áreas de TI incluyendo infraestructura y administración de redes, base de datos, programación, servicios de CCTV, analista de sistemas, Pentester y manejo de edición de imagen y video.

Donaciones

Mas Información

paypal.me/incibegt

info@csecmagazine.com

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.

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 2,021.

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