REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

CIBERSEGURIDAD, UN RETO PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD.

Tutor: José De Los Reyes Rivera Castro

Autores: Zuyitza Yesagelis Rivas Julio

Carlos Mata Parra

Panamá, 17 de diciembre de 2021

REPÚBLICA DE PANAMÁ

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA

FACULTAD CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

CIBERSEGURIDAD, UN RETO PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

PROYECTO DE TRABAJO PARA OPTAR AL GRADO DE LICENCIADO EN INGENIERÍA EN REDES DE COMUNICACIONES CON ÉNFASIS EN SEGURIDAD

Autores: Zuyitza Yesagelis Rivas Julio

Carlos Mata Parra

Panamá, 17 de diciembre de 2021

Ciudad de Panamá, 17 de diciembre de 2021

Profesor (a)
Nagib Yassir
Coordinador Comité de Titulación de Estudios de Licenciatura.
Presente.

En mi carácter de Tutor del Trabajo de Grado presentado por los estudiantes Zuyitza Yesagelis Rivas Julio y Carlos Mata Parra; documento de identidad (cédula o pasaporte) , para optar al grado de, Licenciatura En Ingeniería En Redes De Comunicaciones Con Énfasis En Seguridad considero que el trabajo: reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Jurado examinador que se designe.

Atentamente,

(firma)
_____
(Nombre y Apellidos del tutor

Documento de identidad_____, No. _____

Línea de Investigación:
_____

UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

INFORME DE ACTIVIDADES DE TUTORÍA OPCIÓN DE TITULACIÓN II

Estudiantes: Zuyitza Yesagelis Rivas Julio.
Carlos Mata Parra.

Tutor: Prof. José Rivera Cédula de identidad o pasaporte

Correo electrónico de los participantes:

Título tentativo del trabajo de grado (TG) y de pasantía profesional (PEOP). CIBERSEGURIDAD, UN RETO PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

SESIÓN	FECHA	HORA REUNIÓN.	ASPECTO TRATADO	OBSERVACIÓN
1.	30/07/2021	5:30 pm.	Selección del Tutor para el proyecto de grado	
2.	06/08/2021	5:30 pm	Selección del tema a investigar	
3.	13/08/2021	5:30 pm	Mejorar planteamiento del problema, formulación del problema y objetivos	
4.	27/08/2021	5:30 pm	Mejora del Título del trabajo	Se analizó escoger un título adecuado al tema planteado
5.	17/09/2021		Mejora de recolección de datos	
6.	01/10/2021	5:30 pm	Mejora de análisis y conclusión	
7.	06/10/2021	5:30 pm	Revisión de los avances	se corrigió justificación, y marco teórico.
8.	18/11/2021	5:30 pm	Detalles de técnica e instrumento	Se corrigió en base al tipo de investigación documental.
9.	10/12/2021	5:30 pm	Revisión de Trabajo Final	Revisar que el trabajo mantenga las normas.

Titulo definitivo: <u>CIBERSEGURIDAD, UN RETO PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.</u>

Comentarios finales acerca de la investigación: Declaramos que las especificaciones anteriores representan el proceso de dirección del trabajo de grado arriba mencionado.

Firma	Firma
_____	_____

ÍNDICE GENERAL

Páginas

ÍNDICE DE TABLAS Y FIGURAS

Tablas

Figuras

REPÚBLICA DE PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTAD CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍA

CIBERSEGURIDAD, UN RETO PARA LAS PEQUEÑAS Y MEDIANAS EMPRESAS.

Autores: Zuyitza Yesagelis Rivas Julio
Carlos Mata Parra
Tutor: José De Los Reyes Rivera Castro
Año: 2021

RESUMEN

El propósito de esta investigación fue conocer cuáles son los retos que se enfrentan las pequeñas y medianas empresas con un enfoque en el campo de la ciberseguridad, utilizando el método de **investigación de tipo documental** según González, Gabriela. (3 de abril de 2020) es un método de estudio e interpretación basado en la revisión de libros, artículos, vídeos y documentales. Permitiendo así la definición de la población a estudiar, un **grupo de todos los documentos existentes que abarcan desde 2016 hasta 2021**, que contengan información relevante en cuanto a temas de ciberseguridad en las pequeñas y medianas empresas, siendo estos los protagonistas principales. Como siguiente paso se procedió a la selección de la muestra a analizar, la cual es un subgrupo de la población. Como estos documentos son de fuentes secundarias externas podemos decir que esta técnica es de **observación documental indirecta** una vez definidos y ordenados todos los conceptos dentro de aquellos documentos abordados, se identifican los tipos de ataques cibernéticos que más se han detectado, que sectores empresariales están siendo foco de los ciberdelincuentes, el resultado del ataque y cuáles son las razones por la cual están teniendo fallas al mitigar las vulnerabilidades, con esto se pudo obtener un enfoque centrado y concluir acerca de la problemática que sucede en las PyMes en cuanto a ciberseguridad se trata y como deberían enfrentar estos retos.

Palabras claves: ciberseguridad, documentos, investigación, PyMes.

REPUBLIC OF PANAMÁ
UNIVERSIDAD INTERNACIONAL DE CIENCIA Y TECNOLOGÍA
FACULTY OF ENGINEERING AND TECHNOLOGY

CYBERSECURITY, A CHALLENGE FOR SMALL AND MEDIUM-SIZED ENTERPRISES.

Author: Zuyitza Yesagelis Rivas Julio,
Carlos Mata Parra
Tutor: José De Los Reyes Rivera Castro

ABSTRACT

The purpose of this research was to know what are the challenges faced by small and medium enterprises with a focus on the field of cybersecurity, using the documentary type research method according to Gonzalez, Gabriela. (April 3, 2020) is a method of study and interpretation based on the review of books, articles, videos and documentaries. Thus, allowing the definition of the population to be studied, a group of existing documents spanning from 2016 to 2021, containing relevant information regarding cybersecurity issues in small and medium-sized enterprises, these being the main protagonists. As a next step, we proceeded to the selection of the sample to be analyzed, which is a subset of the population. As these documents are from external secondary sources we can say that this technique is of indirect documentary observation once defined and ordered all the concepts within those documents addressed, the types of cyber-attacks that have been detected the most, which business sectors are being the focus of cybercriminals are identified, the result of the attack and the reasons why they are having failures to mitigate vulnerabilities, with this it was possible to obtain a focused approach and conclude about the problems that occur in SMEs in terms of cybersecurity and how they should face these challenges.

Keywords: cybersecurity, documents, research, SMEs.

INTRODUCCIÓN

Antes de la pandemia se observaba un incremento en los ataques cibernéticos, por lo cual grandes empresas comenzaron a tener demandas millonarias entre otros problemas, por no mantener un plan de riesgo adecuado, por lo que no solo estas eran el foco de atención para los ciberdelincuentes, y es donde se comenzaba también a observar que las pequeñas y medianas empresas ya tenían indicios de un incremento en las estadísticas, y boletines de ciberseguridad.

Al dar paso al 2020 la ciberseguridad se vio afectada, además de los tantos problemas causados por la pandemia, las empresas tuvieron que prescindir de su personal, hasta colocarlos en teletrabajo, empresas con muy poco conocimiento implementaron infraestructuras muy poco robustas, con tal de que la productividad no se detuviera, es donde los ciberdelincuentes se beneficiaron aún más de las vulnerabilidades que mantenían, y explotó el incremento de ciberataques, ya sea de Phishing, Ransomware, entre otros tipos. Es por la cual en esta investigación se enfoca en brindar un panorama de qué se debe reforzar en las infraestructuras, analizar donde se han visto más vulnerables, desde la creación de contraseñas, reducir el impacto de pérdidas millonarias, y preservar la confianza con sus clientes.

En esta investigación el planteamiento del problema se desarrolla en el capítulo I, detallando la problemática de las PyMes, específicamente, se presentan los objetivos generales y especifico. Justificando por qué la necesidad de la misma.

El marco teórico se presenta a lo largo del capítulo II, mostrando los antecedentes, llegando también a las bases teóricas y describiendo los términos más relevantes para el entendiendo correcto de esta investigación.

Siguiendo en esta línea en el capítulo III, se describe el marco metodológico, que va desde el tipo de investigación hasta la población, muestra, técnica e instrumento de investigación.

Los resultados de la investigación se describen en el capítulo IV, donde posteriormente seguirá un análisis de los mismo en el capítulo V para obtener las conclusiones en el capítulo VI.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Problema De Investigación

En los últimos años se ha visto un gran aumento de los ciberdelitos, afectando la integridad y privacidad de muchas personas civiles hasta personas con puestos públicos de gran importancia para una región. En algunos casos se ha podido dar con los responsables de dichos delitos, encontrando en su mayoría delincuentes en busca de dinero o recompensas importantes, formando organizaciones a nivel mundial.

En 2020 con la pandemia esto ha empeorado, aún más llevando hasta a las pequeñas organizaciones a pensar o replantear su estructura para implementar e invertir en equipo y personal para evitar ser víctima de ciberataques y proteger su información. Otro punto importante es que la hora de que las empresas, desafortunadamente sean víctimas de ciberataque no solo son afectadas ella, sino que también sus clientes, algo que es muy importante ya que existen normas y leyes a nivel internacionales y nacional. Como es la Ley No. 81 de protección de datos personales de la República de Panamá. Esta ley tiene como objetivo establecer los principios y derechos de cada ciudadano en cuanto a protección de datos personales se habla.

Con la llegada apresurada del teletrabajo aumentaron aún más los riesgos de la fuga de datos personales de las organizaciones, pues como todos sabemos se han realizado prácticas de seguridad que no fueron las adecuadas, pero los responsables de esto deben prevenir los riesgos a terceros.

1.2 Objetivos de la Investigación

1.2.1 Objetivo general

Analizar la importancia de la ciberseguridad en las PyMes, de manera que puedan estar al tanto de cómo protegerse de ciberdelincuentes, sabiendo que son muchas las maneras en las que pueden ser vulnerables, y perder información de suma importancia.

1.2.1 Objetivos específicos:

- Identificar cuáles son los tipos de ataques de ciberseguridad que más se han detectado.
- Identificar qué obstáculos están teniendo las PyMes en ciberseguridad, para disminuir los riesgos.
- Analizar los documentos encontrados, con referencia tanto a las pymes, como a los ciberataques.

1.3 Formulación del Problema

¿Cuáles son los retos que enfrentan las pequeñas y medianas empresas en el campo de la ciberseguridad?

1.4 Justificación del estudio

Ciudad del Saber (2019) “Con el avance de la conectividad de las personas y de las cosas (IoT) y el uso creciente de los datos se incrementan los ataques y vulnerabilidades, por lo que las organizaciones deben de seguir los pasos correctos para gestionar un camino seguro a su digitalización y que no cause riesgos para su información”, expresó Eli Faskha, CEO de Soluciones Seguras.

A través de este proyecto observaremos algunos documentos de ciberseguridad, donde queda constancia que en medio de la pandemia se han visto involucradas una gran cantidad de pequeñas y medianas empresas afectadas con daños a pequeña o gran escala, provocando hasta el cierre de estas o afectaciones colaterales que no les dejan un pronóstico.

Además, se detalla la importancia de las medidas de ciberseguridad en las empresas, principalmente las pequeñas y medianas dentro del mercado. Pues si bien es cierto, tiempos atrás las grandes empresas tenían problemas o afectaciones en sus infraestructuras en materias de ciberseguridad, lo que los llevó a realizar inversiones para remediar este aspecto importante. Lo cual nos lleva a las PyMes que no pudieron por temas económicos, o no vieron

viable invertir en infraestructuras de ciberseguridad, no midiendo los riegos que pasarían de no hacerlo, a partir de ello muchas PyMes fueron blancos fáciles para los ciberdelincuentes, quienes, de múltiples formas lograron explotar sus vulnerabilidades dentro de sus infraestructuras, con ello poniendo en alerta y preocupación a este grupo de empresas tan numeroso.

La ciberseguridad está tomando una gran importancia dentro de las empresas, y las PyMes tienen un reto en disminuir los riesgos que puedan ocurrir a futuro, teniendo especial cuidado en las afectaciones que podría tener estas organizaciones de no contar con las herramientas, equipos y personal adecuado especializado en temas de ciberseguridad, lo que justifica la inversión para prevenir ser víctimas de ciberdelincuentes. Con esta investigación se observará cuáles son las fallas de seguridad que más afectan a las PyMes, para así reducir los riesgos y cumplir con las normativas.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes del Estudio

2.1.1Antecedente 1

En una investigación realizada por Alberto Urueña y Antonio Hidalgo estudiantes de la Universidad Politécnica de Madrid en el año 2016 titulada "ciberseguridad en la sociedad digital" en donde se puede observar que tras varios años de estudio la ABI Research público en el 2017 su más reciente artículo con respecto al índice mundial de ciberseguridad (IMC) mostrando que estos índices fueron basados en cinco puntos principales para demostrar que la ciberseguridad si existe a nivel de los países, como lo es: las medidas técnicas, las medidas jurídicas, creación de capacidades, medidas organizativas y corporativas.

Arrojando como resultados que en Alemania era uno de los países con mayor IMC obteniendo un promedio de 0.71, mientras que países como España estaban un poco más abajo con un IMC de 0.59. sin embargo, no todos tenían las mismas medidas como lo es Eslovenia que tenía un IMC de 0.18 teniendo consigo 0.00 en las medidas organizativas lo que nos lleva a concluir que incluso desde estos tiempos aún se veía que no todos los países cuentan con los mismos mecanismos para mitigar el impacto del ciberdelito.

Otro aspecto importante a destacar dentro de este trabajo fue que los phishing según investigaciones comprobadas que son los que se utilizan con mayor frecuencia para obtener la contraseña de sus usuarios pudiendo así acceder a las cuentas y así a grandes sumas de fondos e información valiosa para los implicados, ya que los malware se instalan en las computadoras de las víctimas. Por tal razón, se considera que cada uno de los usuarios dentro de una organización son responsables, o más bien deberían tener mayor cuidado con lo que aceptan con cada click en los equipos ya que es una tarea de todos implementar estas medidas de ciberseguridad, ayudando así a aumentar el IMC dentro de la organización y que incluso la buena práctica estas medias conlleva a cambiar hasta

la manera en la que manejamos nuestro dispositivos personales para evitar que nuestra información personal y sensitiva sea robada.

2.1.2 Antecedente 2

El estudiante Juan José Hurtado Quijada de la Universidad Internacional de Ciencia y Tecnología, realizó la investigación titulada: Estudio comparativo de las tecnologías alternativas: Computación en la nube, computación en el borde y computación en la niebla, para las PYME en panamá, en el año 2021.

De este trabajo se puede resaltar que las PyMes están migrando a la nube en respuesta a los problemas de costos de inversión, velocidad de despliegue, costo de mantenimiento, costo de actualización de tecnología, y los altos costos de personal calificado para implementar los sistemas tecnológicos. Esto ve claramente como empresas ante la problemática de inversión, deciden migrar a la nube, hacer un análisis de presupuesto y con ello mejorar la seguridad en la nube.

2.1.3 Antecedente 3

El siguiente antecedente es una investigación realizada Martínez Cortes, John Fredy estudiantes de la Universidad Piloto de Colombia en el año 2015 titulada “Seguridad de la Información en pequeñas y medianas empresas (pymes)” en donde aborda la seguridad de la información en las pymes, sus principales errores al implementar un sistema de gestión de la seguridad de información (SGSI).

Se detalla que la implementación de SGSI en las grandes empresas toman de referencias normas ISO 27001, COBIT e ITIL, estás teniendo un grado alto de dificultad de implementar y entender, ya que muchos de estos modelos solo fueron desarrollados pensando en las grandes empresas, y no tanto en las PyMes.

Se observa que los principales incidentes de seguridad en las pymes son la descarga de códigos maliciosos, seguido por el phishing, y explotación de vulnerabilidades. Se

establece que existen muchas metodologías para implementar un SGSI en una pyme, en donde todas tienen el mismo objetivo que es el de calcular el riesgo asociado a los activos de la organización y establecer medidas para reducirlo.

2.2 Bases Teóricas.

Según estudios realizados dieron como resultados que los días de la semana de lunes a viernes son días en los que se debe tener un mayor cuidado con las amenazas recibidas ya que si bien es cierto, si un lunes hay 1000 usuarios conectados se detectan 100 amenazas. Sin embargo, los días sábados, viernes y domingo sucesivamente son los días que se generara menor detección de amenazas. Daniel Kundro, We Live Security (17 de febrero de 2020) – "¿Qué día de la semana es más probable infectarse?".

2.1 Definición de Términos

Ciberataques: Ataques cibernéticos o ciberataques, afectan tanto software, dispositivos, como infraestructuras, aprovechando vulnerabilidades.

Ciberseguridad: La ciberseguridad se enfoca en la protección, métodos, para proteger la información, software, redes y dispositivos.

Amenazas: Son aquellas acciones que afectan la seguridad informática, pueden ser pro vulnerabilidades, o errores por parte de personas.

Malware: Códigos maliciosos que se encargan de causar daño dentro de un software, red, infraestructura, o dispositivos.

Ransomware: Ataques que cifran los archivos, o el dispositivo de la víctima, luego exigen un pago por brindarte la llave de descifrado, en muchas ocasiones por medio de bitcoins, de no pagar, tus datos serán divulgados en la red.

Cripto Ransomware: cifrar los documentos de la víctima, y para descifrarlos se necesita una clave.

Locker Ransomware: cifra el dispositivo de la víctima, la misma es incapaz de acceder, se le muestra un mensaje en pantalla donde, le indican que necesita realizar el pago, y en que monedero digital para así obtener el rescate.

Bitcoins: Moneda digital para hacer distintos tipos de transacciones de una forma anónima.

Ciberdelincuentes: Aquellos quienes cometen delitos informáticos, que incumplen con la ley, y afectan a terceros utilizando medios de telecomunicaciones.

Mitigar: Reducir los riesgos que puedan causar las vulnerabilidades, implementando métodos de seguridad para que tengan un impacto menor.

Exploit: Un programa capaz de aprovechar las vulnerabilidades dentro de un sistema.

Phishing: método de estafa, suplantando una identidad con ingeniería social aprovechando la manipulación con las victimas para robar información confidencial.

BYOD: Bring your own device, tendencia de organizaciones a permitir que sus colaboradores traigan sus propios dispositivos.

HTTPS: Protocolo Seguro de transferencia de hipertexto (Hyper Text Transfer Protocol Secure) estable una comunicación segura entre cliente y servidor para el envío de información una página web.

CAPÍTULO III
MARCO METODOLÓGICO.

3.1 Tipos de investigación.

Se toma como referencia o punto de partida la investigación documental, ya que con este tipo de investigación se describe características o rasgos de la situación, eventos o casos que hayan ocurrido. Con esta investigación se recolectará información para determinar frecuencias de ataques cibernéticos, tipos de ataques, funciones de la ciberseguridad en la empresa, llevando consigo la disminución del impacto de los ataques cibernéticos, por esta razón se tomará investigaciones anteriores para recolectar datos de importancia en contextos de protección y prevención para mantener los datos de una organización a salvo.

La investigación documental es un método de estudio e interpretación basado en la revisión de libros, artículos, vídeos y documentales. También se puede definir como un proceso de recolección, organización y análisis de una serie de datos que tratan sobre un tema en particular. González, Gabriela. Lifeder (3 de abril de 2020).

3.2 Población y muestra

Para Paella, Santa (2006) “la población de una investigación es el conjunto de unidades de las que desea obtener información y sobre las que se va a generar conclusiones”. De manera que para este trabajo de grado la población a investigar es transeccional ya que abarca todos los documentos existentes entre el 2016 hasta el 2021 referente en temas de ciberseguridad para las pequeñas y medianas empresas, destacando los ciberataques ocurridos dentro del periodo de pandemia que dio inicio a mediados del 2020.

Para la muestra de esta investigación se utilizó un subgrupo de dicha población, seleccionando 6 informes los cuales se observan en la Tabla 1, para posteriormente ser analizados.

Tabla 1.

Características de la población, documental.

CARACTERÍSTICAS DE LA POBLACIÓN, ARTICULOS, REVISTAS, E INFORMES.				
POBLACIÓN	CONTENIDO	TIPO	FUENTE	FECHA
6	Información sobre ciberataques	Informes	https://ibm.ent.box.com	2021
	Información sobre ciberataques	Informes	https://www.bakerlaw.com	2021
	Información sobre ciberataques	Informes	https://content.fireeye.com	2021
	Información sobre ciberataques	Informes	https://f.hubspotusercontent40.net	2021
	Información sobre ciberataques	Informes	https://assets.ey.com	2019-2020
	Información sobre ciberataques	Informes	https://www.ospi.es/	2019

3.3 Técnicas e instrumentos para la recolección de datos o información.

En este proyecto se utilizó la técnica de observación documental indirecta, ya que es una de las técnicas que nos permite la obtención de datos o información de fuentes secundarias, con ello se logró obtener una mejor visualización de los tipos de ciberataques y su impacto en las PyMes.

"Un instrumento de recolección de datos es, en principio, cualquier recurso del cual pueda valerse el investigador para acercarse a los fenómenos y extraer de ellos información." Palella, Santa (2006), por lo que para investigación se utilizó el instrumento de matriz de análisis documental la cual nos permite ordenar y clasificar los documentos consultados, Sierra Bravo (1992) también menciona que el análisis de contenido es "La técnica, sin duda más elaborada y que goza de mayor prestigio científico en el campo de la observación documental".

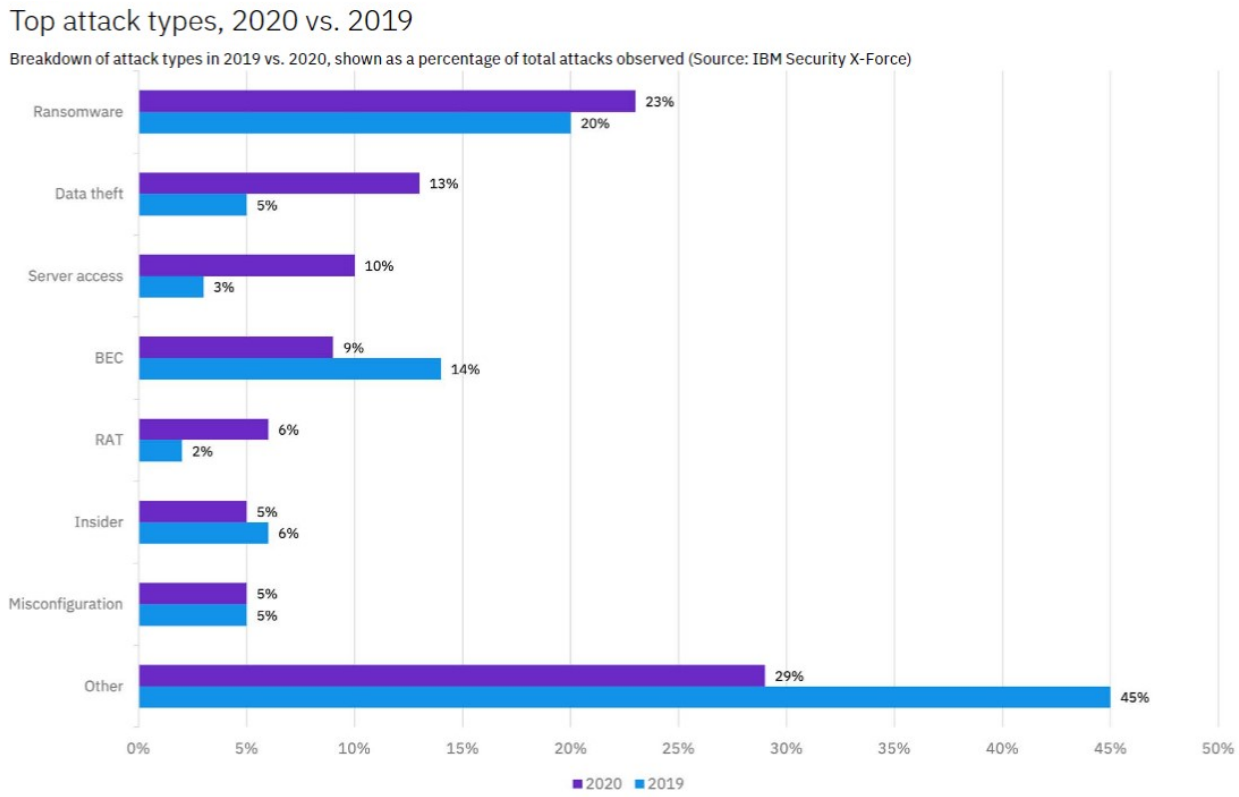
Tabla 2.

Matriz para el análisis de los informes.

N°1	Tipo documento	Titulo	Fecha	Autor	Aporte	Área de conocimiento
1	Informe	XForce-Threat-Intelligence-Index-2021	2021	IBM	Reporte de ataques cibernéticos	Ciberseguridad
2	Informe	Digital Assets and Data Management - Disruption and Transformation	2021	BakerHostetler	Reporte de ataques cibernéticos	Ciberseguridad
3	Informe	M-Trends 2021 Report	2021	FireEye	Reporte de ataques cibernéticos	Ciberseguridad
4	Informe	Sectigo State of Website Security and Threat Report	2021	Sectigo	Encuestas a PyMes	Ciberseguridad
5	Informe	Encuesta Global de Seguridad de la Información de EY	2019-2020	EY	Encuestas a PyMes	Ciberseguridad
6	Informe	La ciberseguridad en España, Una perspectiva desde las Pymes, sociedad civil y administración pública	2019	Google	Encuestas a PyMes	Ciberseguridad

CAPITULO IV
RESULTADOS DE LA INVESTIGACIÓN

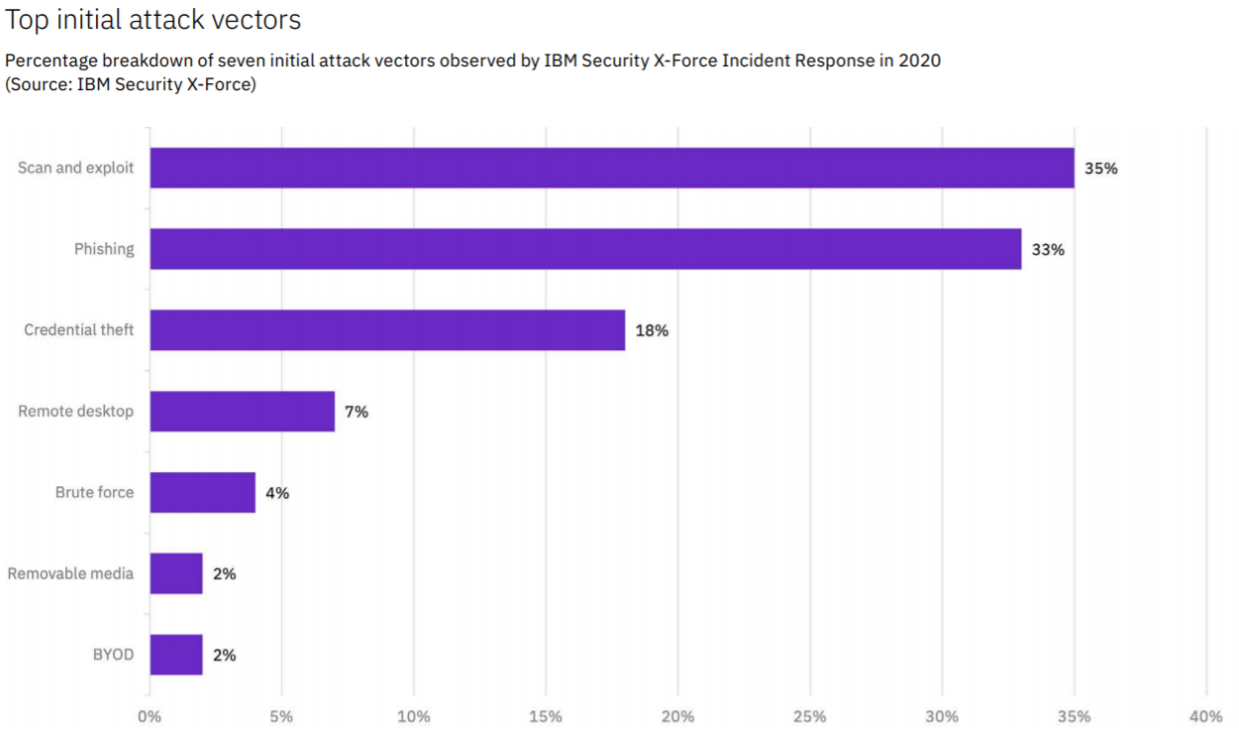
Figura 1. Top de tipos de ataques, 2020 vs. 2019.



Fuente: (IBM security X-Force reports) 2021

Aplicando el instrumento de investigación documental, En la primera investigación se obtuvieron entre los resultados que el Ransomware estuvo en un 20% el 2019 y el 23% 2020. El robo de datos un 5% el 2019, y un 13% el 2020.

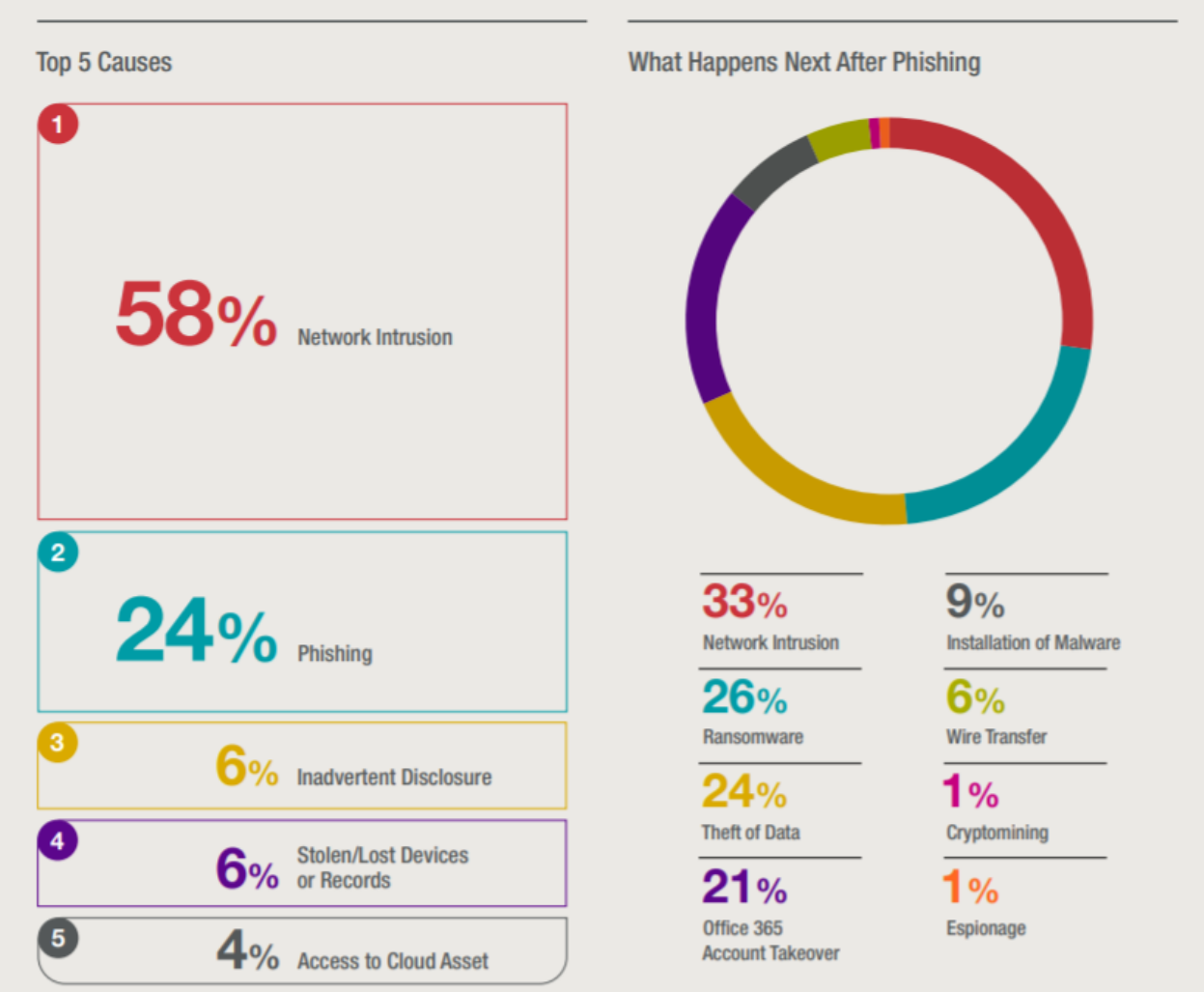
Figura 2. Top de vectores de ataques iniciales.



Fuente: (IBM security X-Force reports) 2021

En esta segunda investigación, se observó el top de vectores de ataques iniciales con un 35% de escaneo y exploit, el Phishing con un 33%, un 18% para el robo de credenciales, escritorio remoto 7%, fuerza bruta 4%, medios removibles 2%, y un 2% BYOD.

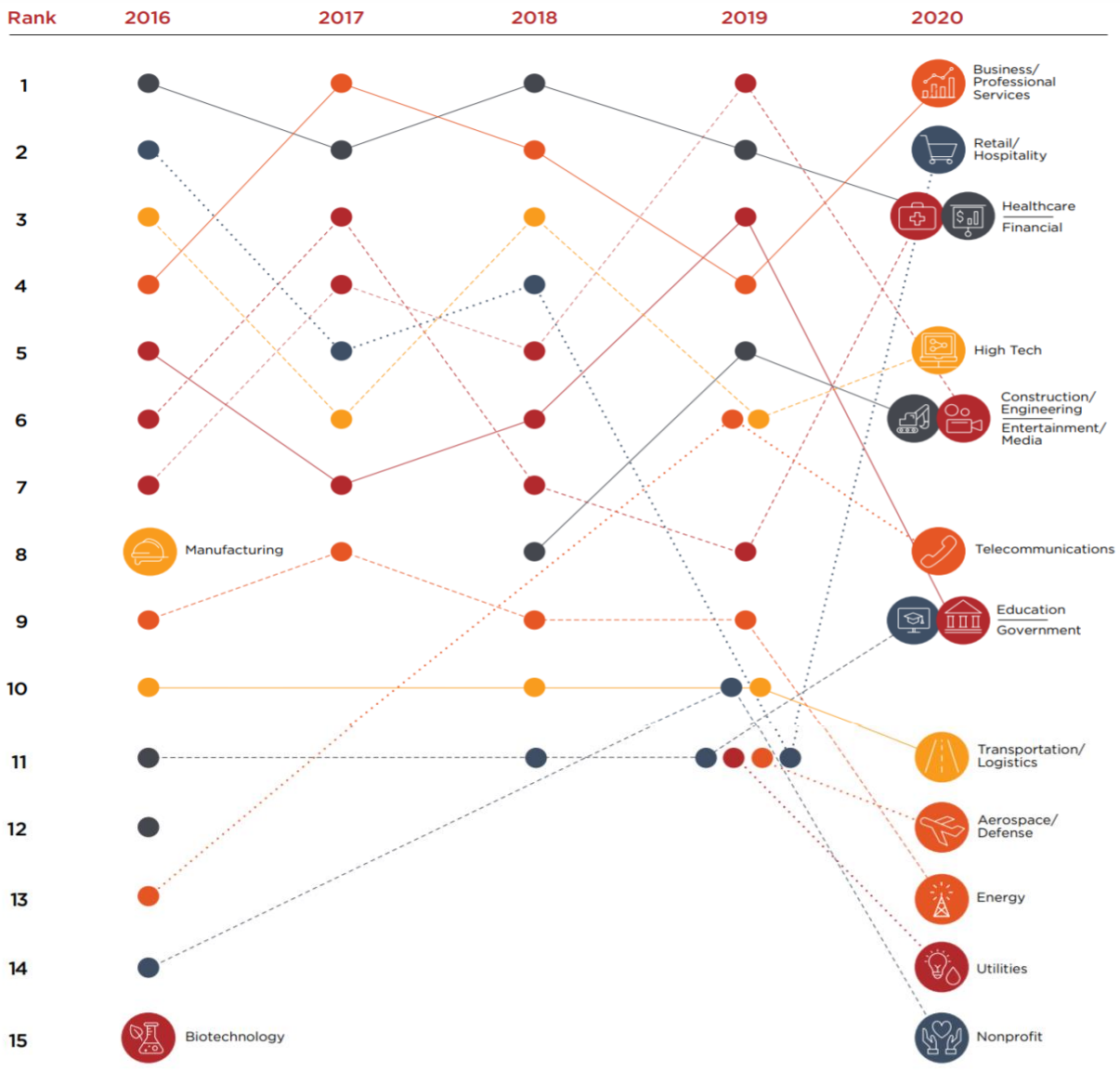
Figura 3. Tendencias de respuestas de incidentes.



Fuente: (BakerHostetler, Data security incident response report) 2021

En la tercera investigación se observa un top 5 de tendencias de respuestas a incidentes, en done las intrusiones a la red con un 58%, phishing 24%, 6% divulgación inadvertida, robos, dispositivos o registros perdidos con un 6%, y un 4% de accesos a los activos de la nube. Además, se resalta el 26% en Ransomware, y 24% de robo de datos después que se realiza el phishing.

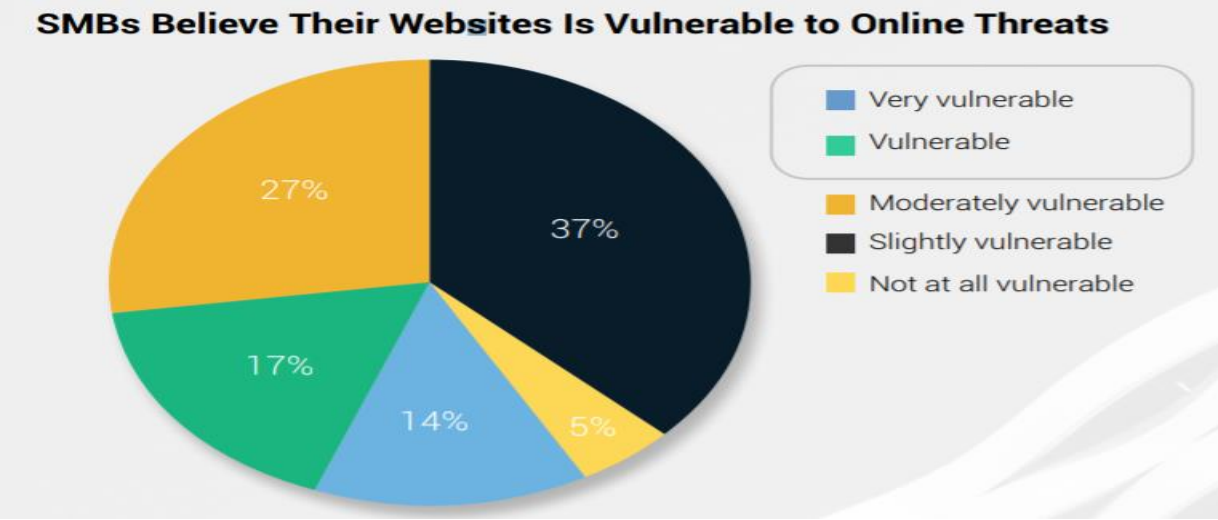
Figura 4. Top de Industrias como objetivos entre 2015 y 2020.



Fuente: (FireEye Trends Report) 2021

En la Cuarta investigación se obtuvieron los resultados del top de industrias como objetivos, empresas/ servicios profesionales del 2016-2020 se ha colocado del 4to hasta el 1er puesto, el sector de comercio minorista/hotelería que desde 2011-2016 estaba en el 11vo puesto, llego a colocarse como 2do en 2020, el Sector de salud en 2016 en 6to puesto hasta un 3er puesto en 2020, el sector financiero del 11vo puesto al 4to.

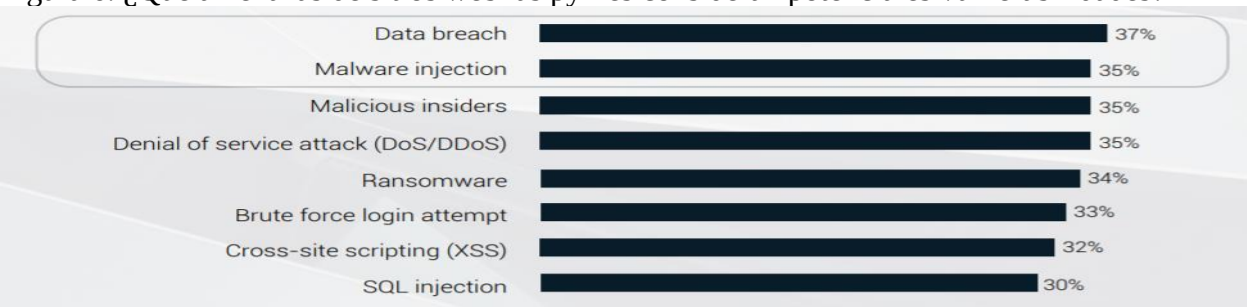
Figura 5. ¿Pymes creen que sus sitios web son vulnerables a amenazas en línea?



Fuente: (Sectigo, State of website security and threat report) 2021.

Quinta investigación, nos indica que creen que su sitio web es muy vulnerable con un 14%, un 17% vulnerable, moderadamente vulnerable un 27%, un 37% ligeramente vulnerable, y un 5% que para nada es vulnerable.

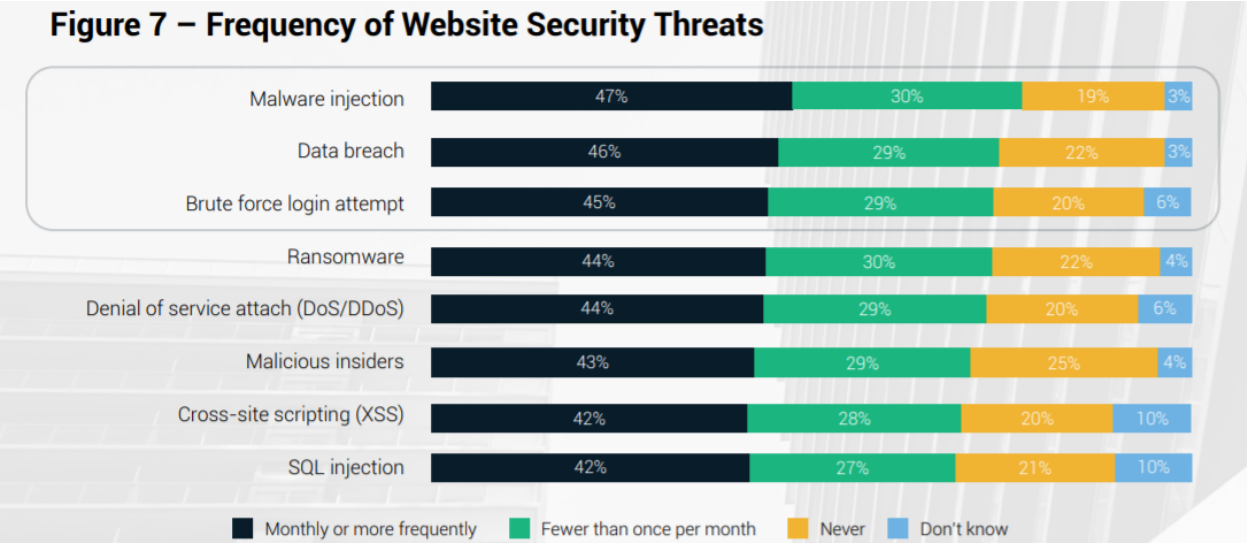
Figura 6. ¿Qué amenazas de sitios web las pymes consideran potenciales vulnerabilidades?



Fuente: (Sectigo, State of website security and threat report) 2021.

Sexta investigación, se observó que la brecha de datos, la inyección de malware, personal malicioso, están entre los primeros con un 37%, y 35% respectivamente, DoS/DDoS 35%, Ransomware 34%, intentos de fuerza bruta 33%, cross-site scripting 32%, SQL injection 30%.

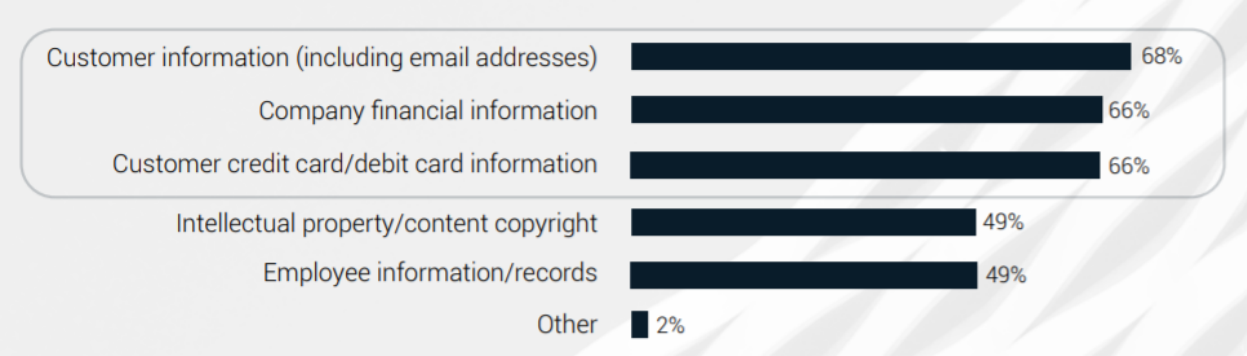
Figura 7. Frecuencia de amenazas de seguridad de sitios web



Fuente: (Sectigo, State of website security and threat report) 2021.

Séptima investigación, En esta encuesta para las pymes, enfocados en la parte de seguridad de sitios web, se observa que la inyección de malware es un 47% mensual o más frecuente, un 30% menos de una vez por mes, 19% nunca, y 3% no sabe. La Brecha de datos un 46% mensual o más frecuente, 29% menos de una vez por mes, 22% nunca, y 3% no sabe.

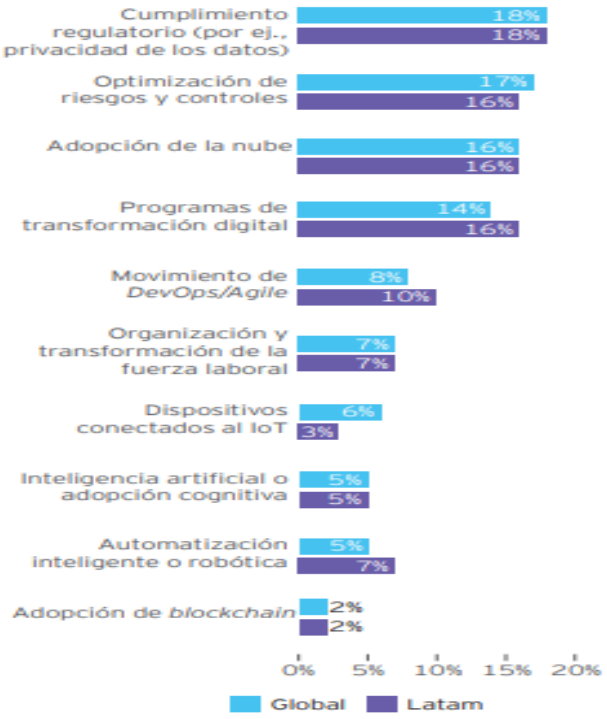
Figura 8. Información que más les preocupa proteger a las pymes.



Fuente: (Sectigo, State of website security and threat report) 2021.

En esta octava investigación, se observó que la información que más le preocupa es la de los clientes con un 68%, las finanzas de la compañía, la información de las tarjetas de crédito/debito con un 66% respectivamente.

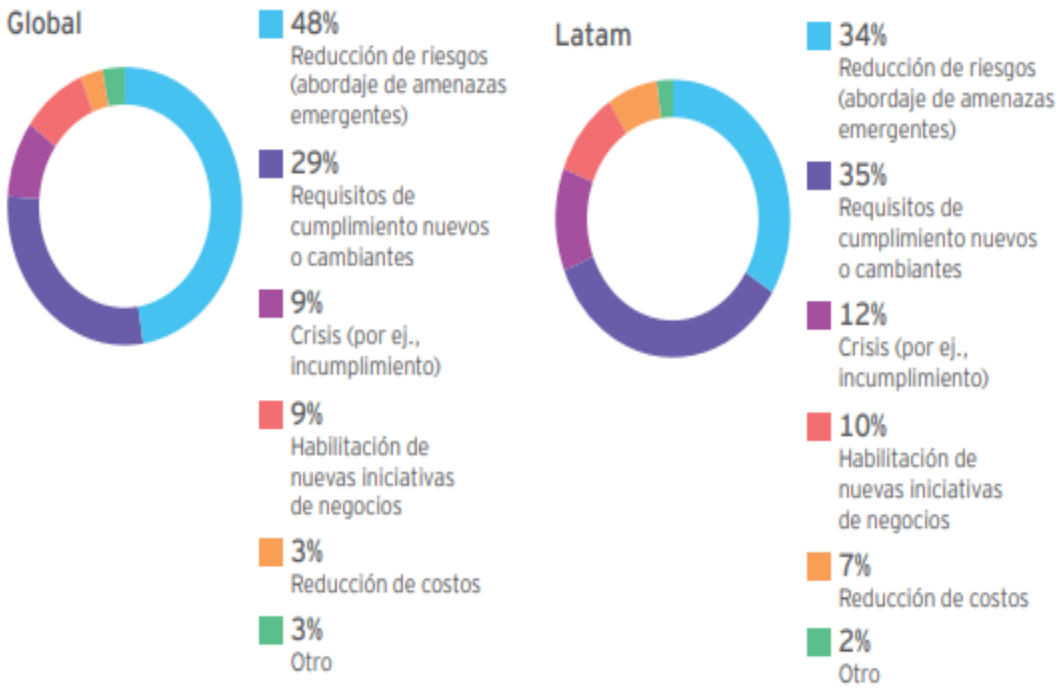
Figura 9. Uso del presupuesto de ciberseguridad.



Fuente: (Encuesta Global de Seguridad de la Información de EY GISS 2019-2020)

Luego de observar los resultados de esta Novena Investigación, el uso del presupuesto global de ciberseguridad está relacionado mayormente con el cumplimiento regulatorio, optimización de riesgos y adaptación de la nube.

Figura 10. Justificación para incrementos en el presupuesto de ciberseguridad.

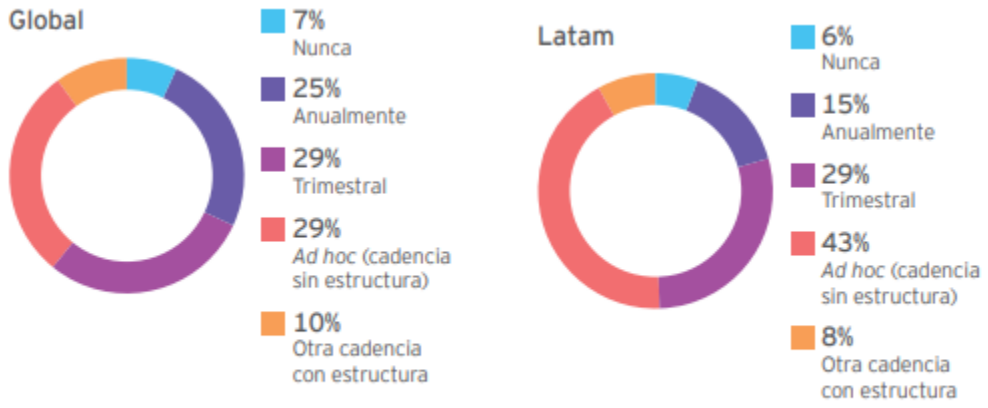


Fuente: (Encuesta Global de Seguridad de la Información de EY GISS 2019-2020)

La justificación de los incrementos de los presupuestos de ciberseguridad, en la décima investigación se pudo notar que en área global un poco menos de la mitad (48%) opinan que se debe a reducción de riesgo.

Mientras que en el área de Latinoamérica este incremento se lo atribuyen mayormente a la reducción de riesgos (34%) y requisitos de nuevos cumplimientos (35%).

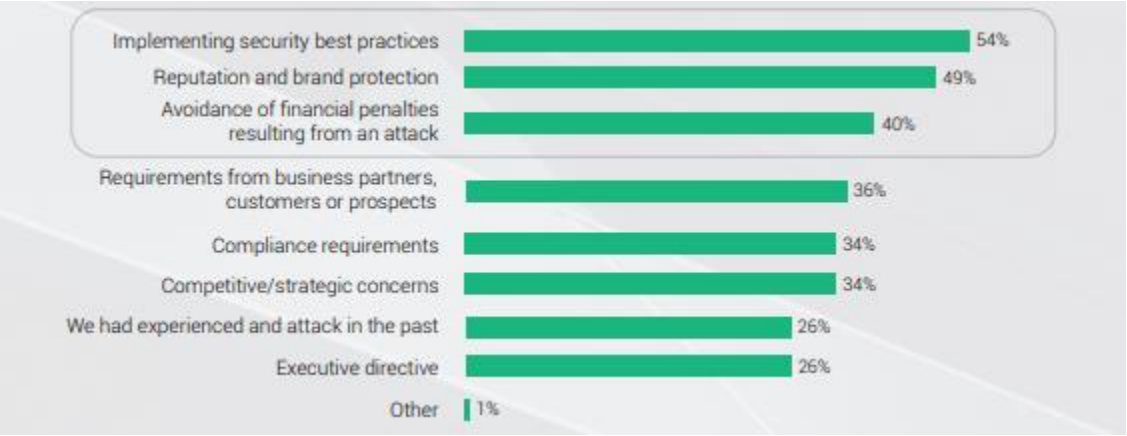
Figura 11. ¿Cada cuánto tiempo la ciberseguridad está en la agenda del Consejo de Administración?



Fuente: (Encuesta Global de Seguridad de la Información de EY GISS 2019-2020)

Con la Onceava Investigación, podemos observar que el 43% de los encuestados a nivel de Latinoamérica coinciden de que no se incluye la ciberseguridad como parte de la agenda del consejo de administración debido a que hay cadencia sin estructura (Ad hoc).

Figura 12. Factores que influyen en el gasto en seguridad del sitio web

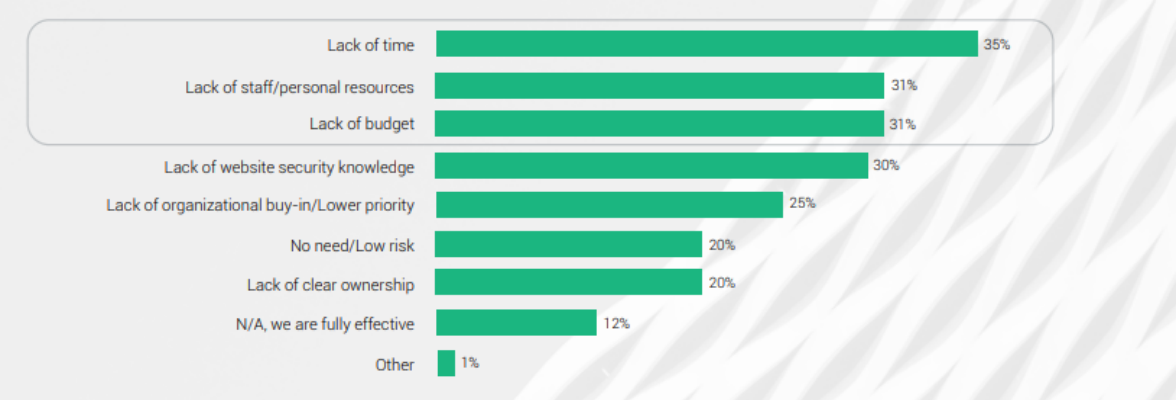


Fuente: (Sectigo, State of website security and threat report) 2021.

Para la Duodécima Investigación, la implementación de mejores prácticas de seguridad es el factor con mayor porcentaje (54%), cuando nos referimos a los factores que influyen en los gastos de

seguridad de sitios web, 49% reputación y protección de la marca, Evitación de sanciones económicas derivadas de un ataque 40%.

Figura 13. Barreras para el uso de tecnologías de seguridad de sitios web



Fuente: (Sectigo, State of website security and threat report) 2021.

Al observar la decimotercera investigación, logramos tener el enfoque de cuáles son las barreras para el uso de tecnología de seguridad en sitios web, destacando que la falta de tiempo (35%) es el factor líder, 31% falta de personal, y 31% falta de presupuesto.

Para la decimocuarta investigación, según un estudio realizado por Google en temas de ciberseguridad de las pequeñas y medianas empresas en España, se menciona que el 99.8% del tejido empresarial español no se considera un objetivo atractivo de un ciberataque. De 1,537 empresas encuestadas tan solo el 36% de las pymes tienen establecidos protocolos básicos de seguridad, y un 30% de las webs no disponen de protocolo https, se menciona que, por falta de medios, tiempo, e inclusión concienciación. Un 60% de las pymes europeas que son víctimas de ciberataques desaparece en los seis meses siguientes de sufrir el ciberataque, muchas veces debido al alto coste.

CAPÍTULO V
ANÁLISIS DE LOS DATOS E INFORMACIÓN

De acuerdo con las investigaciones realizadas, en esta parte del proyecto se analizarán los datos recolectados, de esta forma tener una base fundamental, conocer cuáles son los ataques más comunes, y así las pymes puedan mantener un panorama de las prevenciones a tomar.

En la primera investigación (Figura 1) se observa la comparación de los Top de tipos de ataques entre 2019 y 2020, en donde el Ransomware, los robos de datos, y el acceso a servidores han ido en aumento, el primero de un 20% a 23%, el segundo de un 5% a un 13%, y el tercero de un 3% a un 10%, esto quiere decir que los ciberdelincuentes están enfocando en estos tipos de ataque, lo cual en el último año se vio como las empresas mantenían una fragilidad en sus sistemas de seguridad. No dejando atrás el remote access trojan (RAT) o Troyano de Acceso Remoto, que permite al ciberdelincuente un acceso remoto hacia los hosts, poder subir archivos e instalar software malicioso de un 2% a un 6%, en definitiva, estás cifras han aumentado más ya que cada día se descubren nuevos tipos de Ransomware.

De la segunda investigación (Figura 2) se puede comparar con la tercera investigación (Figura 3) por lo que da una clasificación de los vectores de ataques más comunes, que han incurrido con más frecuencia en el último año.

Por ende, los tipos de ataques más comunes son:
- El del exploit que es igual a las intrusiones a la red.
- Phishing.
- Robos de credenciales.

Se relaciona justamente con en la decimocuarta investigación de este trabajo que menciona que “entre las pymes, los ataques más comunes fueron de ransomware, secuestro de sistemas, fugas de información y ciberestafas; y en ciudadanos, técnicas de engaño como el phishing y los virus informáticos”

En la Cuarta investigación (Figura 4) se observan los tops de industrias como objetivos de 2015

hasta el 2020, y en el 1er lugar se encuentran los servicios profesionales, 2do destacando los comercios minoristas y hotelerías, 3er y 4to lo comparten las industrias de salud y las finanzas, ya de 5to las grandes compañías tecnológicas. Esto nos da una visión de a donde están dirigiendo los ataques, colocando una perspectiva donde las pymes son las que solicitan dichos servicios profesionales a grandes empresas como una firma de abogados, firmas de seguro o firmas de diseño, teniendo en cuenta que están grandes empresas mantienen un portafolio amplio de pymes con la cual trabajan, y los comercios minoristas que de estar en la posición número 11 en el 2019 ya en el 2020 se ubicó en el número 2, un ejemplo pueda ser que mantengan conexiones con otras empresas y estas al ser atacadas los ciberdelincuentes pueden extraer una gran cantidad de datos entre ellos información de PyMes, hacer unas suplantación de identidad y enviar correos de phishing a las pymes, y estás ser afectadas igualmente, todo va en un escalabilidad en la que no solo por el hecho de ser una pyme, hay que dejar a un lado el tema de ciberseguridad.

Para la quinta (Figura 5), sexta (Figura 6), séptima (Figura 7) y octava (Figura 8) investigación se observó una serie de encuestas realizada por la empresa Sectigo donde participaron 9 países: Australia, Brasil, China, Francia, Alemania, India, México, Reino Unido, y Estados Unidos. Cabe resaltar que para las investigaciones de Sectigo se hizo la encuesta con un número de 1167 encuestados. Estas encuestas para las PyMes se enfocan solo en la seguridad de sitios web, con ello damos una parte de todo lo que quiere decir ciberseguridad.

La quinta investigación (Figura 5), se centra en la encuesta de las ¿pymes creen que sus sitios son vulnerables a amenazas en línea?, en donde se observa que una amplia cantidad indica que un 27% es moderadamente vulnerable, un 37% es ligeramente vulnerable, un 5% para nada sean vulnerable, esto puede uno decir que están muy seguras de su seguridad, o que no están tomando en cuenta cuan frágil pueden ser sus infraestructuras, sabiendo que cada día aumentan la cantidad de Ransomware, se observa que algunas aún mantienen la mentalidad que por ser pymes no son vulnerables mucho más que las grandes empresas.

En la sexta investigación (Figura 6), ¿Qué amenazas de sitios web las pymes consideran potenciales vulnerabilidades?, las pymes indican que las filtraciones de datos, inyección de malware, colaboradores maliciosos son las amenazas de sitios web potencialmente vulnerables, al

ver este tipo de encuesta, se compara con la séptima investigación (Figura 7). La frecuencia de estos ataques a los sitios web, la inyección de malware un 47% mensual o más frecuente, un 30% al menos una vez por mes, 19% nunca, 3% no sabe. Filtración de datos 46% mensual o más frecuente, 29% al menos una vez por mes, un 22% nunca, y 3% no sabe, los intentos de inicio de sesión de fuerza bruta un 45% mensual o más frecuente, al menos una vez por mes 29%, nunca un 20% y 6% no sabe, ya de por si se debe mantener una perspectiva que los servicios de comercio electrónico en línea, este tipo de tiendas virtuales, o páginas que recolectan datos, y mantienen una base de datos de usuarios, debe mantener los parches actualizados, las medidas de seguridad adecuadas para que no se filtren los datos de los usuarios que depositan una confianza enorme de brindar nombres, teléfonos, residencia, y hasta número de tarjetas de crédito. Aunque sea una pequeña o mediana empresa deben de asegurar que este tipo de vulnerabilidades disminuyan. Aquí es donde la octava investigación (Figura 8) toma lugar, la información que más le preocupa proteger a las pymes, un 68% la información de los clientes, la información de las finanzas de la compañía en un 66%, la información de las tarjetas de crédito/debito un 66%.

Por otro lado, La Novena Investigación (Figura 9) Uso del presupuesto de ciberseguridad, muestra que Latinoamérica en seguridad de información tiene un gran crecimiento en el área de cumpliendo regulatorio con un 18%, siguiendo con 16% optimización de riesgos y controles, también adaptación de la nube, programación de transformación digital estas 2 con 16%, movimiento de DevOp 10%,organización y formación de la fuerza laboral con 7%, inteligencia artificial 5% y por ultimo 3 % con los dispositivos IoT (internet de las cosas). Podemos observar pequeñas variaciones en los resultados obtenidos entre los datos globales y los datos para Latinoamérica. Algo muy importante para destacar es que un 16 % de las empresas en Latinoamérica utilizan sus presupuestos para programas de transformación digital mientras que el escenario global es un 16%. Esto se debe a que en Latinoamérica se la tenido que hacen un esfuerzo extra para prestar la debida atención a los temas de transformación digital y aún más se agravo el tema con la llegada de la pandemia del COVID 19. Por otro lado, se observa que ambos escenarios (global y Latinoamérica) muestran un 18% en cuanto al cumplimiento regulatorio, como lo es el cumplimiento de privacidad, esto proporcionaría beneficios a la organización.

De tal manera, En la Décima Investigación se representa la justificación de los incrementos en el

presupuestó de seguridad (Figura 10) , tanto en la Novena y Décima Investigación se nota que en la Latinoamérica los incrementos son mayores a diferencia de la global, solo la reducción de riesgos tiene 34% a diferencia del global que es de 48% mayor y también los otros con 2% a diferencia de 3% del global , en Latinoamérica tiene más porcentaje en incrementos de presupuesto en la área de requisitos de cumplimento 35%, crisis 12% , habitación de nuevas iniciativas de negocios 10%, reducción de costos 7%. observando los resultados obtenidos en la encuesta Global de Seguridad de la Información de EY GISS 2019-2020, notamos que en cuantos a la justificación para incrementos en presupuestos de ciberseguridad en Latinoamérica el 35% de los participantes justifican sus incrementos en este presupuesto como un requisito de cumplimiento, esto se debe a que se está intentado generar un nueva cultura de ciberseguridad, con nuevas normal obligando a los CISO de dichas organizaciones a tomas la correctivas pertinentes para el buen funcionamiento de las operaciones y generando enlaces con los departamentos para su cooperación, ya que muy pocos justifican este incremento para reducir costo, pues este 7% de las empresas notan que no es un tema de ahorro económico sino más bien para evitar numerosas perdidas. Curiosamente a nivel global es solo un 3% que comparten esta posición. Un ejemplo claro de esto es que una empresa puede perder millones de dólares de ser víctima de un ciberataque, mientras que, si esta prepara con equipo e implementación para prevenir esto, solo sus pérdidas se verían como una inversión a largo y mediado plazo.

En la Onceava Investigación ¿Cada cuánto tiempo la ciberseguridad está en la agenda del Consejo de Administración? (Figura 11). Arrojan los siguientes resultados para Latinoamérica: Ad hoc 43%; trimestral 29%, anualmente 15%, otra cadencia con estructura 8% y nunca 6%, hay una pequeña diferencia con el global. Se puede destacar que la mayor parte de los participantes en Latinoamérica y a nivel global con un 43% y 29% respectivamente tienen una cadencia sin estructura, lo que nos hace señalar que la mayoría agendan los temas de ciberseguridad ante un consejo administrativo, sin tener una estructura esquemática ni organizacional lo que los arroja a no hacerlo periódicamente, sino en base a las necesidades, y es una cultura que debería cambiar.

Incluso aquellos que tienen estructuras, pero tienen cadencias son mejores su porcentaje esto se debe a que si en una organización se cuenta con la estructura adecuada debería estar la planificación con la que se debería trabajar. Se cree que estos porcentajes pueden variar mucho

para las próximas encuestas, ya que las preparaciones se ven cada vez más en las empresas con personal capacitado.

En la Doceava Investigación (Figura 12) “Factores que influyen en el gasto en seguridad del sitio web” las respuestas obtenida en esta encuesta se observa: la implementación de la mejores practica de seguridad 54%; protección de la reputación y la marca 49$; evitación de sanciones económicas resultantes de un ataque 40%; también contiene: requisitos de socios comerciales clientes o prospectos 36% ; requisitos de cumplimientos 34%; preocupaciones competitivas/ estrategias 34%; experimentaciones y ataques del pasado 26%, directiva ejecutivo 26% y otro 1%, influye muchos factores en los gastos de seguridad. El 54% de las pymes tienen conciencia que se necesita la implementación de mejores prácticas en cuanto a seguridad, partiendo del punto de vista que muchas de estas cuentan con ciertas prácticas de seguridad, pero o no son las correctas o simplemente no cuentan con el personal adecuado para su implementación y supervisión, los que les cuesta mucho a estas empresas y mucho más si nos estamos refiriendo los sitios web, pues estos son focos constantes de los ciberdelincuentes. Y es allí donde entra un 49% de los factores que influyen en gastos de sitio web, pues a estas empresas les toca proteger su reputación ante el cliente, ya que nadie va a confiar sus datos sabiendo que una empresa tiene muy mala reputación y un índice grande de riesgos de ser atacados. Además, tenemos que las pymes evitan ser sancionados, y por eso invierten en la seguridad de sus sitios web según este informe este factor tiene un 40%, siendo estos los 3 factores principales de gastos en seguridad web.

Con relación con la decimotercera investigación (Figura 13) “El uso de tecnologías de seguridad de sitios web” arrojan los siguientes resultados: los 3 primeros factores son Falta de tiempo 35%, falta de personal 31%, falta de presupuestó 31%, los demás como falta de conocimiento de seguridad del sitio web 30%, falta de organización /prioridad más baja 25%, sin necesidad/bajo riesgo 20%, falta de propiedad clara 20%, n/a somos completamente efectivos 12% y otros 1%. Mostrando las dificultades del uso de la tecnología de seguridad de los sitios web.

Con los resultados de la decimotercera y ultima investigación, podemos notar que el mayor porcentaje de las barreras para que las pymes tecnologías de seguridad de sitio web es la falta de tiempo, medios, Además de que la falta de personal y de presupuesto tienen un 31% cada una.

Dato que es muy curioso porque les siguen con 30% la falta de conocimiento de seguridad de sitios web, este se correlaciona con el estudio de Google que de la falta de páginas web con protocolo https. Otro punto notorio dentro de estos datos es que la Falta de aceptación organizacional / Prioridad más baja tienen 25% en las pymes llevándonos a pensar que no es tan importante la seguridad de sitios web para una pequeña parte de las pymes. Bajo riesgo y falta de prioridad clara obtienen 20% cada uno dejando una brecha muy pequeña entre estas barreras y las anteriores, tema de preocupación para las pymes.

CAPÍTULO VI
CONCLUSIONES

A lo largo de este trabajo, con los artículos investigados, ofreciendo datos relevantes que nos llevaron a un análisis de los factores comunes de vulnerabilidades, cuáles son los ataques más comunes durante el aumento de casos de PyMes afectadas, por ello la importancia de que las empresas conozcan las estadísticas, donde están fallando y que esto es el presente, tan solo falta ver como poco a poco las pequeñas y medianas empresas van incluyendo más la Inteligencia Artificial en estos temas para lograr vencer los retos de ciberseguridad se les presentan, e inclusive los dispositivos IoT, por ende, también son una vulnerabilidad para las empresas, donde incluso ya se ven impresoras envueltas en estos temas de ciberataques.

Con este trabajo se observó que algunas de las PyMes están tomando acción ante la ciberseguridad por los eventos acontecidos y estadísticas basadas en datos recolectados durante los últimos años, están anuentes de cuáles son los factores importantes a proteger, en donde no solo se ven afectados por pérdidas económicas, sino a una escala mucho mayor con demandas por incumplimientos, reputación por parte de clientes insatisfechos con la gestión de sus datos, un punto importante, pues gracias a los clientes las empresas logran ser quienes son y tener su reputación.

La seguridad información en la actualidad tiene un gran aporte y es muy importante en toda empresa que desea ampliar y sobrevivir en las demandas de la sociedad que la tecnología está en la vanguardia del futuro. Una buena planificación puede reducir los costos de riesgos y aprovechar las oportunidades del mercado, la tecnología ayuda a la continuidad de la empresa siempre y cuando tengan logística, voluntad de adaptarse en los momentos necesarios para la empresa.

Tener en cuenta el uso del presupuesto para el tema de ciberseguridad, ya que como bien pudimos observar son muy importante en temas de grandes pérdidas económicas que pueda sufrir la empresa. Adaptación de la nube, transformación digital, optimizar riesgos, organización de DevOp, incluir inteligencia artificial también dispositivos IoT estos son los puntos importantes al tomar en cuenta el uso de presupuesto, si es necesario el aumento en algunas también justificar si es importante para la vanguardia de la empresa y de la operación, y de esta manera se reduce el riesgo y crisis cuando se vean envueltos en cambios nuevos en el sector.

Contemplar una planificación trimestral es una tarea importante en la actualidad, viendo que se están realizando muchos avances tecnológicos en todas las áreas, incrementando ataques a empresas que cometen errores al no estar frecuentemente en el en cambio y descuidando la actualización para no escatimar en gatos para la compañía, frecuentemente es descuido de muchas pequeñas y medianas empresas, por ende, incluir una agenda de consejo es un importante factor clave para la supervivencia de las empresas para futuro, ya que incluso antes de la pandemia ya esta problemática se veía incrementar según comparación de las estadísticas.

Se observó que las pequeñas y medianas empresas, que no disponen de sitios web o servicios en medios digitales, en su mayoría las razones son: por dificultades en el uso de la tecnología, falta de tiempo, falta de personal con conocimiento y lo importante por falta de organización y planificación. La falta de personal con conocimiento especializado y profesional es quizás uno de los factores que pueden ser más afectados, pues la pandemia ha agravado esta carencia, ya que como lo mencionamos anteriormente el factor económico está afectando muchos sectores.

La tecnología es una ayuda sumamente importante en la operación de cualquier tipo de empresa que desee subsistir en el futuro, y en cuanto a la seguridad informática la tecnología debería ser incluida como uno de los pilares de una empresa, si bien queda plasmado en este trabajo que según estadísticas aún falta mucho para que las PyMes utilicen estas buenas prácticas como cultura de protección y funcionamiento correcto, obligatorio para las mismas. Y No tener miedo al avance y adaptase cada día más en la vanguardia de la tecnología. Las empresas deben manejar medios tecnologías y herramientas digitales para su mayor servicio a sus clientes.

REFERENCIAS BIBLIOGRÁFICAS

Alberto Urueña, Antonio Hidalgo (2018) Ciberseguridad en la Sociedad digital http://oa.upm.es/54521/1/INVE_MEM_2018_293302.pdf

BakerHostetler (2021) Data security incident response report https://www.bakerlaw.com/webfiles/Privacy/2021/Alerts/2021-DSIR-Report.pdf

Ciudad del Saber (noviembre 18, 2019) LOS NUEVOS RETOS DE HOY EN DÍA PARA LA CIBERSEGURIDAD https://ciudaddelsaber.org/prensa/los-nuevos-retos-de-hoy-en-dia-para-la-ciberseguridad/

Daniel Kundro, We Live Security (2020) – "¿Qué día de la semana es más probable infectarse?" https://www.welivesecurity.com/la-es/2020/02/17/dia-semana-mas-probable-infectarse/

EY (2021) Encuesta Global de Seguridad de la Información de EY GISS 2019-2020 https://assets.ey.com/content/dam/ey-sites/ey-com/es_mx/topics/cybersecurity/ey-22-encuesta-global-de-seguridad-de-la-informacion.pdf

Fernando Alfredo King Bernal (2020) Nivel De La Seguridad Que Perciben Los Usuarios En El Uso De Los Servicios Ofrecidos Por La Nube De G-Suite En Panamá http://www.idi-unicyt.org/wp-content/uploads/2020/05/tesis-Fernando-king-Final.pdf

FireEye (2021) M-Trends Report https://content.fireeye.com/m-trends/rpt-m-trends-2021

Fortinet (2021) Threat Intelligence Insider https://www.fortiguardthreatinsider.com/es/bulletin/Q2-2021

Gabriela González. Lifeder (2 de abril de 2020) – "Investigación documental: características, estructura, etapas, tipos, ejemplos". https://www.lifeder.com/investigacion-documental/.

Gonzalo García Abad (30 de noviembre de 2020) La nube: el trampolín para que tu pyme pueda reinventarse
https://hablemosdeempresas.com/pymes/pymes-nube/

IBM (2021) IBM security X-Force reports
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

Juan José Hurtado Quijada (2021) Estudio comparativo de las tecnologías alternativas: Computación en la nube, computación en el borde y computación en la niebla, para las pyme en panamá.
http://www.idi-unicyt.org/wp-content/uploads/2021/03/Informe-del-Trabajo-de-Grado-de-Juan-Hurado-DEFINITIVA.pdf

Kionetworks (2021) Retos De Ciberseguridad 2021
https://www.kionetworks.com/blog/ciberseguridad/retos-de-ciberseguridad-2021

Martínez-Cortes, J.F., Seguridad de la Información en pequeñas y medianas empresas (pymes), Universidad Piloto de Colombia., 8 (2015)
http://polux.unipiloto.edu.co:8080/00002332.pdf

Notimerica (24 de febrero de 2021) Un estudio revela que el 50% de las PYMES han sufrido una violación del sitio web (1)
https://www.notimerica.com/comunicados/noticia-comunicado-estudio-revela-50-pymes-sufrido-violacion-sitio-web-20210224160823.html

OSPI (2019) Google, Panorama actual de la Ciberseguridad en España
https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Santa Palella – Metodología de Investigación cuantitativa (2006)
https://www.academia.edu/35200587/2006_Metodologia_de_la_investigacion_cuantitativa_Palella_pdf

Sectigo (2021) State of website security and threat report
https://f.hubspotusercontent40.net/hubfs/4887240/Sectigo_StateofSMBSecurity_2.23.21_v3.pdf