Revista de Climatología

Volumen 24 Edición Especial Ciencias Sociales

Vol. 24 (2024): 2273-2280 ISSN 1578-8768

Modelo Proactivo para la Identificación de Ciberataques y sus consecuencias en las PYME

Frano Santiago Capeta Mondoñedo[1]*, Carlos Miguel Franco Del Carpio[1]

[1] Universidad Nacional Federico Villarreal. Perú.

*Autor para correspondencia: Frano Santiago Capeta Mondoñedo

(Recibido: 13-09-2024. Publicado: 31-12-2024.)

DOI: 10.59427/rcli/2024/v24cs.2273-2280

Resumen

La identificación de ciberataques no es una materia exacta, se requiere tener capacidades técnicas, herramientas tecnológicas adecuadas, habilidades prácticas para la identificación in situ de un ataque en curso y sobre todo un modelo operativo proactivo sobre qué hacer durante y después de hacer sido objetivo de los ciberdelincuentes, el enfoque normalmente es sobre el despliegue y la implantación de una herramienta, sea esta un firewall, un WAF u otros complementarios esto genera una falsa sensación de seguridad aunado a la falta de un modelo operativo para la identificación y gestión de los ciberataques hace que cada vez más las PYME tengan consecuencias de todo tipo, consecuencias que podrían ser evitadas si se aplicara un conjunto de procedimientos -modelo operativo y proactivo- adicionalmente las PYME no tienen una conciencia cabal de las causas y consecuencias que un ciberataque puede traer a la organización y solamente después de haber sido afectados toman conciencia de su importancia, ahora bien el modelo proactivo presentado plantea actividades antes -actividades de preparación- actividades durante -identificación y correcta caracterización- actividades después -vuelta a la normalidad, investigación e identificación del vector- estas actividades han sido conceptualizadas y planteadas de tal manera que puedan servir de guía práctica o lista de chequeo lo que permitirá al profesional responsable simplificar su trabajo y sobre todo evitar el tener que buscar en diversas fuentes -muchas veces contradictorias entre si- para de esta manera poder actuar de la manera más rápida posible y eficiente, lo cual redundara en beneficio de la organización a la que sirve y paralelamente permitirá al profesional ganar experiencia y conocimiento sobre la forma correcta de actuar ante la eventualidad de un incidente de ciberseguridad, si bien es cierto que el modelo propuesto no es la única manera de afrontar un incidente, el modelo se caracteriza por ser proactivo y permitir definir un conjunto de tareas previas, las cuales contribuyen a la dotación de medidas de ciberseguridad preventivas que contienen un ataque en sus primeras etapas dando el tiempo necesario para ser identificado y poder desplegar mayores medidas y evitar pérdidas.

Palabras claves: *Ciberseguridad, ciberataque, protección de la información, incidentes.*

Abstract

The identification of cyber attacks is not an exact subject; it requires having technical capabilities, adequate technological tools, practical skills for the on-site identification of an attack in progress and, above all, a proactive operating model on what to do during and after being targeted. For cybercriminals, the focus is normally on the deployment and implementation of a tool, be it a firewall, a WAF or other complementary ones, this generates a false sense of security combined with the lack of an operating model for the identification and management of cyberattacks. increasingly causes SMEs to have consequences of all kinds, consequences that could be avoided if a set of procedures were applied - operational and proactive model - additionally, SMEs do not have a full awareness of the causes and consequences that a cyber attack can bring to the organization and only after having been affected do they become aware of its importance, however the proactive model presented proposes activities before - preparation activities - activities during - identification and correct characterization - activities after - return to normality, research and identification of the vector - these activities have been conceptualized and proposed in such a way that they can serve as a practical guide or checklist, which will allow the responsible professional to simplify their work and, above all, avoid having to search in various sources - often contradictory. each other -

in order to be able to act as quickly as possible and efficiently, which will benefit the organization it serves and at the same time will allow the professional to gain experience and knowledge about the correct way to act in the event of a cybersecurity incident, although it is true that the proposed model is not the only way to deal with an incident, the model is characterized by being proactive and allowing the definition of a set of prior tasks, which contribute to the provision of preventive cybersecurity measures that They contain an attack in its early stages, giving the necessary time to be identified and to be able to deploy greater measures and avoid losses.

Keywords: *Cybersecurity, cyber attack, information protection, incidents.*

1. Introducción

La Ciberseguridad es un tema plenamente vigente en el mundo empresarial, no solo grandes empresas y corporaciones multinacionales sufren los embates de los ciberdelincuentes, sino también sobre todo las PYME son afectadas por estos ciberataques lo cual afecta directamente el resultado económico sobre todo de las PYME pues este tipo de instituciones no posee una disposición de recursos en el día a día como si lo tiene una empresa multinacional. Las tecnologías de la información y las comunicaciones (TIC) han transformado las concepciones de la delincuencia organizada. En concreto, las TIC han influido en la naturaleza de las actividades de la delincuencia organizada y en los tipos de personas que pueden participar en ella. Esta transformación incluye no solo los cambios en los tipos de delitos cometidos y los modus operandi utilizados por los grupos delictivos organizados, sino también la variedad de personas que pueden participar en la delincuencia organizada.

Antecedentes Internacionales:

Diversos países en el Mundo están constantemente bajo ataques de grupos organizados de ciberdelincuentes, teniendo especial incidencia en las Pyme, entidades públicas, las entidades del sector financiero y los sectores que manejan las infraestructuras criticas (centrales de energía, potabilizadoras de agua, control de tráfico aéreo, control de tráfico terrestre, represas, sistemas de transporte masivo, entre las principales) sin embargo son las PYME las más afectadas pues no cuentan con estructuras orgánicas de profesionales y tecnologías que puedan ser usadas en su beneficio para una efectiva protección las hacen las victimas "perfectas" de los ciberdelincuentes, siendo que por lo tanto la implementación de un modelo proactivo para la identificación de los ciberataques y sus consecuencias es de vital importancia, pero esto no solo tiene que ver estrictamente con computadoras, también con los equipos denominados IoT (Internet de las cosas) durante el periodo de sesiones ordinarias del Parlamento Europeo y el Consejo de la UE, se aprobó una ley que afectará a fabricantes de televisores, juguetes, teléfonos móviles, coches, frigoríficos y software, entre otros(https://cincodias.elpais.com/cincodias/2022/09/15/companias/1663236364_939136.html) La nueva norma exigirá que las empresas cumplan con nuevos requisitos de ciberseguridad o si no se enfrentarán a importantes multas. El objetivo de la ley, es regular la comercialización de los objetos conectados, que hasta ahora no están sujetos a ninguna obligación en este ámbito y cuya seguridad generalmente no es la prioridad de sus diseñadores. En definitiva, buscan reducir los ciberataques que estos bienes pueden sufrir a lo largo de su vida útil.

Antecedentes Nacionales:

Según la página web del Congreso de la República,más concretamente https://www.congreso.gob.pe/carpetatematica/2022/carpeta_051/referenciasespecializadas/informacion-estadistica/ menciona con datos estadísticos que "Ciberataques en el Perú incrementaron en un 15 % durante el 2021" más recientemente en diciembre 2022 la empresa multinacional de ciberseguridad ESET indica que "Perú es el país que recibe más ciberataques en América Latina" https://tekiosmag.com/2022/12/21/peru-es-el-pais-que-recibe-mas-ciberataques-segun-un-reporte-de-eset/ , así mismo el diario el comercio (https://elcomercio.pe/tecnologia/actualidad/ciberseguridad-peru-recibio-52-mil-millones-de-intentos-de-ciberataques-en-la-primera-mitad-de-2022-cibercriminales-espana-mexico-colombia-argentina-noticia/?ref=ecr) menciona que "Perú recibió 5,2 mil millones de intentos de ciberataques en la primera mitad de 2022".

Del mismo modo la agencia estatal de noticias andina publica en noviembre 2022 (https://andina.pe/agencia/noticia-peru-registra-mas-123-ciberataques-malware-minuto-918302.aspx) que "Perú registra más de 123 ciberataques de malware por minuto" siendo pues el Perú es el tercer país con más casos de phishing o mensajes fraudulentos en Latinoamérica. obviamente todas estas cifras que son muy altas no todas están pues relacionadas a solamente empresas bancarias o financieras, sino un gran porcentaje de ellas están relacionadas con empresas del segmento PYME. En la actualidad no existen modelos proactivos orientados hacia las PYME que puedan identificar ciberataques y sus consecuencias, cada entidad maneja su propia forma de identificar ciberataques, muchas de ellas son atacadas y estos ataques no son descubiertos hasta después de semanas de haber sucedido o cuando lamentablemente la consecuencia del ataque se manifiesta ya sea mediante el cobre de una extorsión o la publicación de información confidencial en algún sitio público. Es necesario plantear un modelo estandarizado para la identificación de los ciberataques y sobre todo sus consecuencias, económicas, reputacionales, legales, contractuales y de personal que se presentan.

2. Marco Teórico

Ciberespacio

Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas a él, que no existe en ninguna forma física Seguridad del ciberespacio.

Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

Ciberseguridad La ciberseguridad depende de la seguridad de la información, seguridad de las aplicaciones, seguridad de la red, seguridad de internet, para alcanzar sus objetivos, sin embargo, no es sinónimo de ellos.

Información La información se define como un activo "activo de información", pero no se trata obviamente de un componente físico, sino más bien un componente digital, electrónico o virtual y de la misma manera que otros activos contables con vitales para una organización y deben ser protegidos de una manera adecuada desplegando las metodologías, herramientas y tecnologías necesarias.

Del mismo modo la información se transmite, se procesa y se almacena y es en esos tres estados que debe ser también adecuadamente protegida.

Seguridad de la información

Involucra la protección de la confidencialidad, disponibilidad e integridad de la información, y para su debida protección se deben de aplicar medidas tecnológicas, medidas procedimentales y medidas personales.

Seguridad Informática

Se define el concepto de seguridad informática como: cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

hacking

cuando se accede de manera intencional a un sistema informático sea este software, servidores, bases de datos, archivos de datos, sin la autorización del usuario o del propietario.

Ciberataque

Esta referido al acceso o Intento el cual no está autorizado que puede ser exitoso o fallido con la intención de destruir, modificar, dejar fuera de servicio (deshabilitar), robar y publicar en sito web a disposición de terceros la información obtenida producto del ataque.

3. Metodología

La Investigación es de tipo aplicada – tecnológica, ya que se utilizaremos una metodología ágil en la construcción del modelo proactivo y su implementación en el marco de especialización, cuyo propósito es construir desde el conocimiento científico. En el estudio se emplearán los métodos inductivos – descriptivo, analítico y causal, procedimiento que consiste fundamentalmente en establecer la relación causa efecto, de la variable independiente (ciberseguridad) con la variable dependiente (PYME) con la implementación de un modelo proactivo para la identificación de ciberataques y sus consecuencias en las PYME. PARTICIPANTES:

a) Delimitación temporal y espacial

- El desarrollo del proyecto de investigación será realizado durante el período de tiempo que comprende el año lectivo 2023 (enero a diciembre).

- El estudio se desarrollará en el anexo 07 de la Universidad Nacional Federico Villarreal, ubicado en la Av. Oscar R. Benavides 450, Cercado de Lima 15082.

b) Universo y muestra

- El Universo de la presente investigación está conformada por las empresas PYME de la ciudad de Lima.

- La muestra seleccionada para la presente investigación será extraída del universo conformado por aquellas PYME en donde laboren como responsables de la Gerencia de Tecnologías de Información y Comunicación exalumnos de la FIIS-UNFV.

c) Unidad de análisis

- Se considera a las PYMES en estudio.

d) Métodos de muestreo

• El tipo de muestro que se utilizará es el Muestreo Discrecional que permitirá obtener información sobre las actividades relevantes que generan mayor valor a éstos son: las entrevistas online, cuestionarios online, revisión y evaluación de información, clasificación de documentos y creación del diseño instruccional de la línea de cursos y presentado en web.

e) Técnicas

Las principales técnicas que se utilizará en la investigación son:

Entrevistas online.

Cuestionarios online.

Tormenta de Ideas.

Análisis documental.

Revisión bibliográfica.

Hoja de Recolección de datos.

Mapas conceptuales y mentales

Tabulación de datos.

Gráficas de Pareto.

Análisis de resultados.

Matriz de Selección de Causas.

V Heurística.

Diagrama de Procesos.

Muestreo T student.

f) Instrumentos

Entre los principales instrumentos que se requerirán tenemos:

- Guía de análisis documental que está comprendida por:

Entrevistas online a responsables de gerencia de tecnologías de información y comunicación de instituciones públicas y privadas.

Cuestionarios online aplicados a los egresados y docentes de la carrera profesional en estudio.

Cuadros o tablas estadísticas y registros administrativos de las áreas en investigación, para el análisis de datos se utilizarán tablas estadísticas de una y dos entradas (univariable y bivariable) y Gráficos de barras.

Guía de estructuración de cursos de ciberseguridad asíncronos y síncronos donde se detalla la gestión correcta de contenidos.

g) Materiales:

Entre los materiales básicos necesarios que se utilizarán en la presente investigación serán:

- Una Laptop HP o DELL permitirá el desarrollo adecuado de los informes y encuestas.

- Un directorio y espacio en un proveedor de la nube para almacenar la información como backup, este espacio será de 4 GB.

- Una impresora Epson L1210 o similar para la impresión de documentación diversa, así como para impresiones finales del trabajo de investigación.

- Software de Sistema: Se utilizará el sistema operativo bajo entorno de 64 bits (Windows 11).

- Softwares de aplicación: Se utilizará un procesador de textos (Word 365), una hoja de cálculo (Excel 365), un presentador de diapositivas (Power Point 365), para planificación se utilizará el Ms Planner, un Software Estadístico (SPSS 24), conversor de archivos (Ablee Extract 15) entre otros.

- Bolígrafos, utilizados para la transcripción de la toma de datos.

- Block de Notas, utilizados para describir los datos en borrador.

h) Procedimientos

- Se empezará por hacer una búsqueda y análisis de los últimos y más recientes ciberataques y robos de información a empresas del Peru, para identificar los perfiles de ataques, tipos de ataque, modos de operación de los atacantes.

- Se aplicará encuestas online a exalumnos para recoger las problemáticas sobre los ciberataques en sus organizaciones.

- Se aplicará encuestas online a docentes de cursos de ciberseguridad para conocer las medidas técnicas que se aplican para mitigar los ciberataques.

- Se analizará los marcos de acción y los modelos existentes para la identificación y mitigación de ciberataques.

- En base a lo recolectado y analizado estructuraremos un modelo proactivo - prototipo.

- Después de haber creado el prototipo se someterá a una encuesta con docentes especializados y profesionales para conocer su opinión y mejoras al prototipo.

- Con el resultado de las encuestas online haremos la tabulación, la interpretación y determinaremos los resultados del estudio.

Dichos resultados serán plasmados en un software estadístico.

- Para desarrollar la validez de la hipótesis, y conclusiones de la investigación.

4. Resultados

Los análisis de las empresas dedicadas a la ciberseguridad demuestran que durante el periodo de la pandemia los ciberataques se incrementaron de una forma muy significativa, por ejemplo, según cifras publicadas https://twitter.com/isec_pe/status/1374377777630117897 se menciona que el Peru durante el 2020 recibió 2.6 mil millones de ciberataques, sin embargo el año 2022 se recibieron mas de 10,000 mil millones de ciberataques, como podemos observar las cifras son muy grandes, y obviamente muchos de los destinatarios de estos ataques son las PYME, las cuales no están preparadas ni técnicamente ni procedimentalmente para afrontar estos ataques ni para lidiar con las consecuencias post-ataque, observamos entonces que los resultados de las encuestas del presente informe son contundentes, no por falta de interés precisamente si no que no se dispone del conocimiento adecuado, lo cual deriva de otro problema mayor que fue identificado por los autores de este proyecto en su investigación del año 2022 “ https://rclimatol.eu/2023/08/13/ciberseguridad-y-su-relacion-con-la-empleabilidad-para-egresados-de-ingenieria-de-sistemas-en-una-universidad-publica/ “

1. Nivel de la preparación de las PYME para hacer frente a un ciberataque

La conclusión obtenida es que las PYME no están preparadas para hacer frente a un ciberataque de cualquier tipo que se presente, solo un 5 % de PYME declara estar preparado.

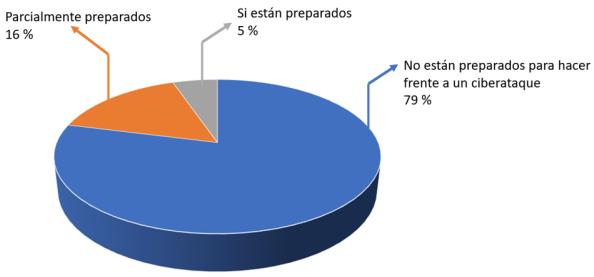

Figura 1: Nivel de preparación para hacer frente a un ciberataque.

Al querer profundizar en el tema y consultar sobre el nivel de conocimiento y/o estudios referidos a las actividades a realizar ente un ciberataque el cual tiene que ver con marcos de trabajo, protocolos, metodologías, se observa que no existe un nivel conocimiento en la mayoría de casos.

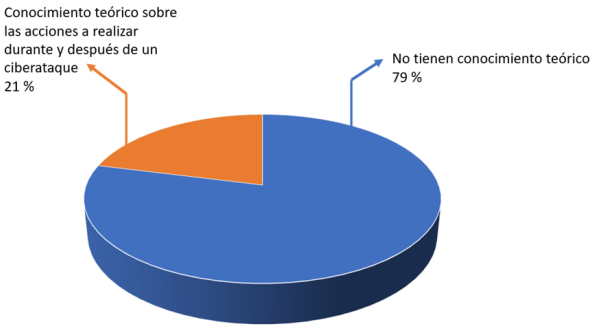

Figura 2: Nivel de conocimiento.

El conocimiento práctico de herramientas sobre ciberseguridad, en particular las relacionadas con el monitoreo y mitigación de ciberataques es muy importante pues conlleva a una efectiva acción durante el ataque, se observa que el conocimiento practico es muy reducido por lo cual se puede decir que existe una deficiencia muy alta en las habilidades para el uso de herramientas.

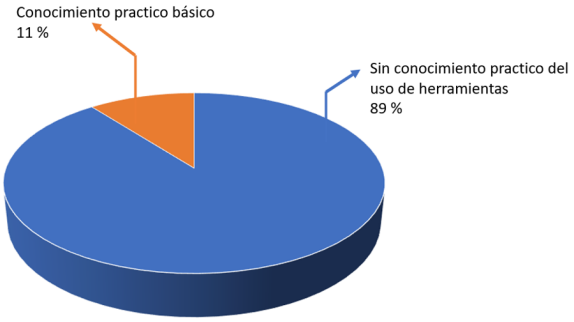

Figura 3: Nivel de conocimiento práctico.

2. Herramientas y conocimientos requeridos

Las herramientas de ciberseguridad son muy variadas y están enfocadas a diversos tipos de protección de la infraestructura de una institución, debido a que los ciberataques no son todos de la misma forma, se requiere por lo tanto del conocimiento y experiencia en el uso de diversas tecnologías, en la figura 4 se aprecia el orden de importancia otorgado por los gerentes de sistemas sobre 4 herramientas puntuales de carácter práctico que son requeridas en las instituciones, siendo la herramienta anti malwares la catalogada como la más importante.

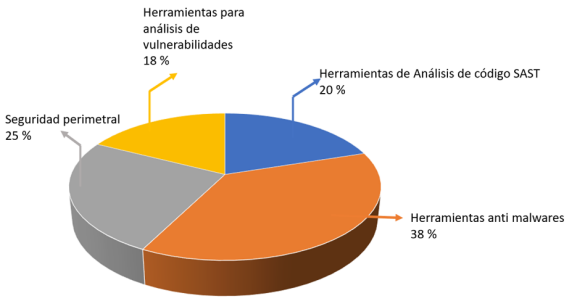

Figura 4: orden de importancia sobre tecnologías de ciberseguridad.

3. Ataques y respuesta a incidentes

La respuesta ante un incidente típicamente un ciberataque es muy importante realizar en tiempo y plazo adecuado para evitar que la entidad (PYME) pueda sufrir los estragos de la intrusión, se observa que en una gran mayoría de casos las empresas parte de la muestra han sufrido ataques.

Una mayoría de empresas encuestadas declaran haber sido víctimas de un ciberataque, lo que se comprueba en la realidad con los resultados de diversas encuestas tomadas como base para esta investigación.

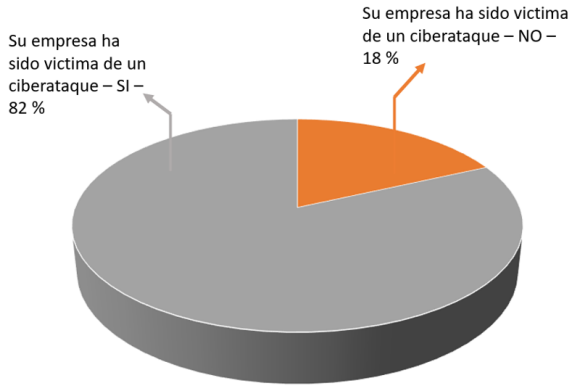

Figura 5: ciberataques en una empresa.

La respuesta efectiva un ciberataque (o sea saber que hacer antes durante y después) es muy importante pues eso permite evitar las consecuencias de este dentro de la PYME la totalidad de encuestados manifestaron la necesidad de contar con un modelo proactivo.

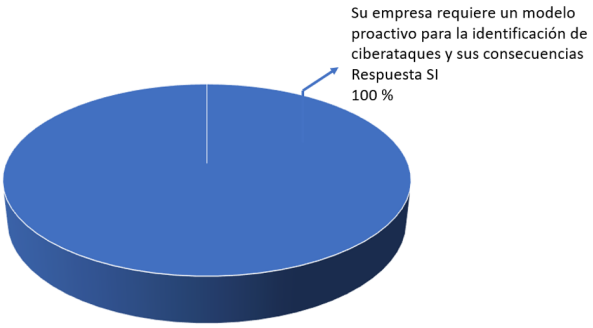

Figura 6: necesidad de un modelo proactivo.

5. Discusión

Es un hecho que durante el periodo más complejo de la pandemia en el año 2020,se origina un crecimiento inusitado de los ciberataques a las entidades de todo tipo (entre ellas las PYME) y los datos más recientes marcan que esa tendencia va en aumento, aunado a esto, la llegada en noviembre del 2022 de la ya famosa aplicación de la empresa OpenAI, nos referimos a chatGPT, (y otras que han ido apareciendo en los últimos 12 meses) esta inteligencia artificial que es usada para diversas aplicaciones e investigaciones también es usada por los ciberdelincuentes para mejorar el perfil de sus ataques y evadir las plataformas de protección, estando aún más expuestas las PYME, adicionalmente en el mercado de proveedores existen diversas soluciones las cuales tienen mayores o menores características de protección, sin embargo las empresas no ven como una necesidad el realizar inversiones en estas tecnologías, teniendo ellos la percepción de que es “un alto costo” y si a esto le sumamos la escasa o nula preparación en las herramientas de mitigación y contención de ciberataques y la falta de un modelo operativo de trabajo que demuestre que hacer en estos casos, se tiene la combinación “perfecta” en detrimento de las empresas receptoras de los ataques. El modelo operativo-proactivo esta orientado a dos objetivos muy claros, por una parte esta la de permitir a las empresas a tener un protocolo y una guía de procedimientos de aplicación directa para la detección y respuesta a ciberataques y por otra parte mejorar las habilidades en el manejo de herramientas y procesos a los encargados de supervisar y gestionar la ciberseguridad en la organización, al evitar que pierdan valioso tiempo tratando de buscar información en Internet vía buscadores y enfocarse directamente en las acciones de mitigación a ser realizadas.

6. Conclusiones

La presente investigación ha permitido identificar la pertinencia de un modelo operativo proactivo para la identificación de ciberataques y sus consecuencias en las PYME y que estas puedan mejorar de manera ostensible su respuesta y gestión posterior, podemos enumerar las siguientes conclusiones:

1. No existen planes, protocolos, guías, directivas, procedimientos ni nada equivalente para que las PYME puedan tener una respuesta eficaz ante un ciberataque.

2. Existe mucha confusión en cuanto a las acciones concretas que se deben de realizar ante un ciberataque, no esta claro que se tiene que hacer o como se tiene que hacer ni quien lo tiene que hacer, esto se deriva que en muchas pymes no existe la función especifica o rol de encargado y/o coordinador de ciberseguridad.

3. No existe pues desde las instituciones formativas la oferta de profesionales que puedan directamente cubrir plazas en el área de ciberseguridad y puedan poner su conocimiento al servicio de la institución.

4. También es evidente que no existen habilidades prácticas que se deben tener para afrontar con éxito la identificación y su posterior contención de un ciberataque.

5. Se pudo evidenciar mediante la encuesta dirigida a ejecutivos que tienen puestos de responsabilidad en el área de sistemas/tecnología de información, que las empresas requieren personal que tenga habilidades prácticas y el no tenerlas es una limitante para su contratación, del mismo modo se pudo conocer que las organizaciones no tienen presupuestos asignados a la capacitación de estos profesionales, por lo tanto lo que está buscando el mercado es adoptar profesionales egresados con conocimientos y habilidades y reducir la curva de aprendizaje que siempre existente.

6. Como conclusión final queda pues evidenciado que existe la necesidad de dotar de un marco de trabajo, esto es el modelo operativo proactivo para la identificación de ciberataques en las PYME dirigida a los especialistas y/o responsables de la ciberseguridad en las instituciones.

7. Referencias bibliográficas

Aguilar, E. (2016). Seguridad Informática para no informáticos. Editorial Palibrio. México.

Castro, S. (2013). Arquitectura de Seguridad Informática: Un manual para gerentes, directores y consultores. 1era edición. CreateSpace Independent Publishing Platform. USA

Cisneros, J. (2019). Ciberseguridad para directores generales, empresarios y altos ejecutivos: Cómo minimizar los riesgos cibernéticos en su organización. Independently published. USA

Fleitas, F. (2018). Guía fundamental en ciberseguridad: Políticas, normas, estándares y buenas prácticas en la seguridad de la información y ciberseguridad. Editorial Académica Española. España

Estándar internacional Norma ISO/IEC 27032. Tecnología de la información — Técnicas de seguridad — Pautas para la ciberseguridad. Primera edición. USA

Estándar internacional Norma ISO/IEC 27001:2013. Tecnología de la información —Técnicas de seguridad — Sistemas de Gestión de seguridad de información— Requisitos. Segunda edición. USA

Estándar Internacional Norma ISO/IEC 27000. Tecnología de la información - Técnicas de Seguridad - Sistemas de gestión de Seguridad de la Información - Información general y Vocabulario. Tercera edición. USA.

Cybersecurity Guide, Guía online de carreras de pregrado de ciberseguridad. Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica. La OEA, el Ministerio de Relaciones Exteriores, el Concytec y la Fundación Citi capacitan a 60 estudiantes peruanos en ciberseguridad.

Reporte de Ciberseguridad 2020. Ciberseguridad, Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. Banco Interamericano de Desarrollo.

Instituto Nacional de Normas y Tecnologías – NIST. Sitio web oficial del CSF.

Instituto Nacional de Normas y Tecnologías – NIST. Historia y creación del CSF.

Instituto Nacional de Normas y Tecnologías – NIST. Estructura del CSF.

Instituto Nacional de Normas y Tecnologías – NIST. Funciones del CSF.

Instituto Nacional de Normas y Tecnologías – NIST. Evolución del CSF.

Instituto Nacional de Normas y Tecnologías - NIST AWS. Cybersecurity Framework – Aligning to the NIST CSF in the AWS Cloud.