Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

MODELO DE DETECCIÓN DE AMENAZAS DIGITALES PARA MITIGAR LOS RIESGOS DE CIBERSEGURIDAD EN LAS ORGANIZACIONES, 2019

Linea de investigación:

Ingeniería de software, simulación y desarrollo de TICS

Tesis para optar el grado académico de

Doctor en Ingeniería de Sistemas

Autor:

Jimenez Chuque, Felix Eloy

Asesor:

Rodríguez Rodríguez, Ciro

(ORCID: 0000-0003-2112-1349)

Jurado

Mayhuasca Guerra, Jorge

Franco Del Carpio, Carlos

Lezama Gonzales, Pedro

Lima – Perú

2022

INDICE

RESUMEN

La ciberseguridad es un aspecto fundamental de las redes, computadoras, software y datos. El objetivo es establecer un Modelo de detección de amenazas digitales para mitigar los riesgos de ciberseguridad en las organizaciones mediante la evaluación de la influencia de la infraestructura de ciberseguridad en el índice global de ciberseguridad. Sin seguridad suficiente, estos activos están vulnerables a amenazas maliciosas (Xiong y Lagerstrom, 2019). Las plataformas tecnológicas ubicadas en los centros de datos de la organización misma o a través de proveedores de servicios a nivel local o en la nube ponen a disposición servicios de comunicaciones, bases de datos, servidores de aplicaciones y servidos de seguridad gestionados, entre otros. En múltiples ocasiones, encontramos que los servicios publicados están comprometidos por diferentes tipos de amenazas digitales que afectan la continuidad operativa de la organización o incluso su reputación. Los servicios digitales se deben atender permanentemente, aún más si tenemos usuarios que consultan de manera constante los servicios ofrecidos en las plataformas. Cada servicio publicado en Internet es siempre atacado por diferentes formas o variantes digitales que infringen o paralizan las aplicaciones que están al servicio del público. En este sentido, es importante entender las formas de identificar una amenaza digital, los criterios utilizados para diferenciar el tráfico correcto de otro que infringe o pretende infringir nuestras plataformas, así como conocer cómo se organizan nuestros servicios digitales, la infraestructura tecnológica, la arquitectura de redes y la seguridad.

Palabras clave: Ciberseguridad, plataformas tecnológicas, centros de datos, proveedores de servicios, amenazas.

ABSTRACT

Cybersecurity is a fundamental aspect of networks, computers, software, and data. The objective is to establish a Digital Threat Detection Model to mitigate cybersecurity risks in organizations by evaluating the influence of cybersecurity infrastructure on the global cybersecurity index. Without sufficient security, these assets are vulnerable to malicious threats (Xiong & Lagerström, 2019). The technological platforms located in the data centers of the organization itself or through service providers locally or in the cloud make available communications services, databases, application servers, and managed security services, among others. Multiple times we find that the published services are compromised by different types of digital threat that compromises the operational continuity of the organization or even its reputation. Digital services must be permanently attended even more if we have users who permanently consult the services offered on the platforms. Every service published on the Internet is always attacked by different forms or digital variants that violate or paralyze the applications that serve the public. In this sense, it is important to understand ways and ways to identify a digital threat; the criteria used to differentiate correct traffic from another that violates or intends to violate our platforms, as well as knowing how our digital services are organized, the technological infrastructure, both network architecture, and security.

Keywords: Cybersecurity, technology platforms, data centers, service providers, threats.

I. INTRODUCCIÓN

La importancia de poder detectar las amenazas digitales en nuestras plataformas de servicios nos permite mitigar cualquier riesgo, garantizando de esa manera la continuidad operativa y la disponibilidad de los servicios digitales.

Las brechas digitales identificadas al momento de construir los sistemas, así como una inadecuada configuración de un equipo de seguridad, red o otra solución genera una clara oportunidad para que una amenaza digital que coincida con dicha vulnerabilidad afecte directamente a la normal operación de los servicios digitales. En ese sentido, los modelos de detección de amenazas son instrumentos capaces de identificar, sugerir o mitigar mediante procesos de decisión oportunos o programados en forma automática de tal forma garanticemos la disponibilidad de los servicios. El presente trabajo de investigación permite establecer la necesidad de disponer un modelo que permita detectar las amenazas digitales y de esa forma mitigar los impactos en los servicios digitales de una organización.

1.1 Planteamiento del problema

La ciberseguridad es un aspecto fundamental de las redes, computadoras, software, y datos. Sin una seguridad suficiente estos activos son vulnerables a amenazas maliciosas (Xiong & Lagerström, 2019).

Las plataformas tecnológicas localizadas en los centros de datos de la propia organización o mediante proveedores de servicios en forma local o en la nube ponen a disposición servicios de comunicaciones, bases de datos, servidores de aplicaciones y servicios de seguridad gestionados entre otros. Múltiples veces encontramos que los servicios publicados se encuentran comprometidos por diferentes tipos de amenaza digital que compromete la continuidad operativa de la organización o más aun su reputación.

Los servicios digitales deben ser atendidos en forma permanente más aún si tenemos usuarios que consultan permanentemente los servicios que se ofrece en las plataformas. Todo servicio publicado en Internet siempre es atacado por diferentes formas o variantes digitales que vulneran o paralizan las aplicaciones que atienden servicios al público.

En ese sentido es importante entender formas y maneras de poder identificar una amenaza digital, los criterios utilizados para poder diferenciar un tráfico correcto de otro que vulnera o pretende vulnerar nuestras plataformas, así también es necesario conocer cómo está organizada nuestros servicios digitales, la infraestructura tecnológica, tanto la arquitectura de red como el de seguridad.

Cuando se establece la arquitectura de ciberseguridad debemos tener un claro conocimiento que tipo de servicios vamos a proteger, cuáles son los criterios por utilizar, qué herramientas de protección disponemos, cuáles son las capacidades de los colaboradores que forman parte del equipo de seguridad digital. Las amenazas tienen diferente nivel, son de diferente tipo, y también de diferente intensidad cómo abordamos problema de esta naturaleza cuáles son los pasos que seguir para entender el problema del otro y que especialista con las capacidades suficiente puede abordar en forma correcta una amenaza digital.

En ese sentido, es necesario mitigar los riesgos de ciberseguridad. Evidentemente la mitigación de riesgos es todo un marco conceptual de la forma y manera como se aborda la presente investigación considera importante establecer en primer lugar lo siguiente:

- Identificar las amenazas digitales.
- Diagnosticar las capacidades de la organización en términos de seguridad digital.

- Establecer políticas de atención y de mitigación de riesgos en ciberseguridad.
- Fortalecer las capacidades de la infraestructura tecnológica.
- Gestionar los activos de protección en seguridad digital.

1.2 Descripción del problema

Existe una dispersión de eventos en cada servicio digital publicado en internet, así como incidencias que se registran en cada servidor, base de datos, servidores de aplicaciones; así también de la infraestructura de seguridad que existe en cada organización.

Las amenazas digitales en sus diferentes variantes mantienen patrones de comportamiento con dispersión aleatoria de los registros o base de datos existentes, sean estas firmas de virus, actualizaciones de sistemas u otros, así como dispositivos periféricos o dispositivos IOT (Internet de las Cosas).

En otros casos tenemos escenarios de mitigación de amenazas de los Firewalls, IPS, IDS, WAF y otras herramientas de análisis, pero estos mantienen un comportamiento lineal o bajo esquemas de aprendizajes supervisados pero que no necesariamente identifican oportunamente la amenaza ingresante en forma escalada de toda la plataforma de seguridad.

En el caso correspondiente del presente estudio, considera la integración de máquinas de aprendizaje en el análisis del comportamiento de los usuarios y de los equipos IOT sean de uso a nivel de centros de datos de confianza, así como de usuarios finales que usan en forma autorizada las plataformas digitales de cualquier organización.

El diseño de una arquitectura de seguridad informática nos permite brindar mejoras en la protección de los activos de toda organización integrada a la plataforma de seguridad y garantizar la continuidad de los servicios digitales que se encuentran en línea.

1.2.1 A nivel global

Las amenazas globales son aspectos que siempre deben ser considerados en toda la plataforma digital de la organización, debido a que existe una integración entre los diferentes servicios que se dispone y la interacción con otras plataformas sean ubicadas dentro de la organización, o fuera de ella. La dinámica de comunicaciones afecta seriamente cualquier programa o sistema digital, en esos escenarios es importante considerar que las amenazas globales siempre afectan a las organizaciones y sus servicios digitales.

1.2.2 A nivel local

Las amenazas internas son las más frecuentes en toda la infraestructura de red, mayormente afectan a los servicios que administra los accesos y la red interna. Considerando que existen diferentes fuentes donde los servicios son afectados, sean puertos USB, correos electrónicos, o navegación en el Internet.

1.3 Formulación del problema

1.3.1 Problema general

¿De qué manera un Modelo de Detección de Amenazas Digitales influye en la mitigación de problemas de los riesgos de ciberseguridad de las organizaciones?

1.3.2 Problema específico

1.3.2.1 ¿De qué manera los equipos de ciberseguridad instalados influyen en el índice global de ciberseguridad?

1.3.2.2 ¿Cómo influye el Numero de certificaciones en ciberseguridad en el índice global de ciberseguridad?

1.3.2.3 ¿En qué medida los equipos de respuesta de incidentes de seguridad influyen en el índice global de ciberseguridad?

1.4 Antecedentes

Actualmente las amenazas digitales han afectado seriamente el quehacer diario de las plataformas y servicios informáticos existentes. La ciberseguridad es el medio donde podemos dar atención a estas amenazas y poder mitigarlas usando diferentes medios y así garantizar la continuidad del servicio correspondiente.

La actual interpretación del comportamiento de los usuarios y equipos informáticos en comportamientos preestablecidos, ante amenazas no previsibles genera un problema mayor, en ese sentido tener amenazas no identificadas de acuerdo con los patrones existentes genera un problema de mitigación.

Los equipos dedicados a redes y seguridad tienen eventos donde podemos integrarlos y centralizarlos para así organizarlos y presentar información estructurada y en función de ello podamos tomar decisiones. Así también, los usuarios tienen formas de realizar consultas ante ciertos sistemas. Es evidente, un sistema registra eventos recurrentes; cualquier evento que escapa del patrón de la línea base de su comportamiento podemos entonces ante registros preexistentes podemos entonces considerar que el usuario tiene un comportamiento fuera de los parámetros establecidos.

1.5 Justificación de la investigación

1.5.1 Justificación de la Investigación

Al presente no existe información disponible de la capacidad instalada de la infraestructura de seguridad digital de las organizaciones en todo el país, el presente trabajo de investigación esboza un panorama general de lo que actualmente existe en el país en torno a sistemas de seguridad digital. Es evidente que, en economías emergentes, existe una creciente demanda de servicios digitales, por lo que resulta necesario garantizar su

continuidad y operatividad, la información que se obtenga de este trabajo permitirá desarrollar nuevas formas y modelos de la manera como tenemos que gestionar los recursos informáticos de una organización.

Así también podremos identificar los problemas de ciberseguridad en las organizaciones de tal forma podamos mitigar en forma estratégica a través de herramientas y soluciones pertinentes. El estudio permitirá también proyectar nuevas investigaciones en torno a la problemática de ciberseguridad, la realidad existente de la infraestructura tecnológica en seguridad informática, las limitaciones de capacidades profesionales debido a la pericia que demanda el sector.

El presente documento establece una línea base de lo que corresponde indicadores e infraestructura de seguridad, amenazas y vulnerabilidades. Así también permite identificar una clasificación de las unidades operativas en seguridad digital de las organizaciones.

La presente investigación es de importancia puesto que permite garantizar la continuidad operativa de la organización. Este sistema de detección de amenazas digitales permitirá prevenir que los sistemas en línea sean atacados y no se afecte la continuidad de los servicios digitales. Es evidente que permitirá advertir en forma oportuna ataques masivos a diferentes servicios digitales y facilitará a los oficiales de seguridad establecer una comunicación más inmediata con los responsables de seguridad y de redes de la organización.

1.5.2 Importancia de la Investigación

Estudiar el impacto de las amenazas digitales en las organizaciones es importante por varias razones. En primer lugar, porque nos permite identificar la influencia en las relaciones entre las plataformas digitales y servicios que generan valor agregado en la organización. En

segundo lugar, establecer las capacidades de la organización el cual permite disponer su tiempo para actuar en escenarios de incidencia en seguridad digital. En tercer lugar, establecer políticas y procedimientos pertinentes para atender incidencias que afectan las operaciones de los sistemas digitales.

1.6 Limitaciones de la investigación

Las limitaciones de la investigación son: a) la información corresponde a registros de diferentes servicios digitales de la plataforma digital del Registro Nacional de Identificación y Estado Civil – RENIEC, b) no existe un listado nacional de infraestructura digital referente a seguridad digital, c) limitada información respecto a incidencias de seguridad digital en el Perú.

1.7 Objetivos de la investigación

1.7.1 Objetivo General

Establecer un Modelo de Detección de amenazas digitales para mitigar los riesgos de ciberseguridad en las organizaciones

1.7.2 Objetivos Específicos

1.7.2.1 Evaluar la influencia de la infraestructura de ciberseguridad en el índice global de ciberseguridad.

1.7.2.2 Determinar la relación existente en organizaciones con certificaciones en ciberseguridad y su impacto en el índice global de ciberseguridad.

1.7.2.3 Determinar la relación existente de los equipos de respuesta de incidentes de seguridad y el índice global de ciberseguridad.

1.8 Hipótesis

1.8.1 Hipótesis General

Si el Modelo de detección de amenazas digitales es implementado entonces influye en la mitigación de riesgos de ciberseguridad en las organizaciones.

1.8.2 Hipótesis Específica

1.8.2.1 Si la infraestructura de ciberseguridad se reduce el índice global de ciberseguridad disminuye.

1.8.2.2 Si las organizaciones se certifican en ciberseguridad se mejora el índice global de ciberseguridad.

1.8.2.3 Si los equipos de respuestas de incidentes de seguridad se incrementan mejora el índice de global de ciberseguridad.

II. MARCO TEÓRICO

2.1 Marco conceptual y bases teóricas

2.1.1 Bases Teóricas

La existencia de diferentes modelos para detectar amenazas digitales permite que toda organización pueda adoptar esquemas de protección de sus activos críticos garantizando la continuidad de sus operaciones digitales. El modelo planteado Gestión de Ciberseguridad Empresarial (Donaldson et al., 2018) permite tener una visión de lo que toda organización debe asumir como rol dentro de la estrategia de detección de amenazas digitales y la manera de prevenirlos.

La ciberseguridad es un aspecto fundamental de redes, computadores, software y datos (Xiong & Lagerström, 2019), sin suficiente seguridad estos activos son vulnerables a amenazas maliciosas. Existen diferentes puntos de vista en torno a ciberseguridad, considerando a los especialistas en ciberseguridad, escaneo de vulnerabilidades filtro de virus en correos electrónicos, protección de la información personal, prevención de la ciberseguridad, servicio de protección de datos todos estos aspectos deben ser considerados en un modelo de detección de amenazas (Thakur et al., 2015). La integridad de los datos es otro aspecto importante para considerar, el daño en la integridad causa serios problemas más que las brechas existentes en su almacenamiento (Gheyas & Abdallah, 2016). Los ataques a la integridad de los datos afectan seriamente a los sistemas de infraestructuras críticas.

Los activos digitales de una organización, así como los activos críticos de una nación son afectados si las vulnerabilidades existentes no son atendidas en los plazos correspondientes. Existe un costo que se incurre por no prestar atención a las necesidades de infraestructura en ciberseguridad (Johnson, 2015). Los ataques APT, Amenazas Avanzadas Persistentes son ataques a la red sofisticados donde el atacante busca ganar información y no

ser detectado por un determinado tiempo, adquiriendo gran cantidad de información y conocimiento de la infraestructura vulnerada. Los ataques APT no son diseñados para causar daño sino adquirir y modificar datos.

2.1.2 Estado del arte

Actualmente existen diversos tipos de amenazas digitales sean estos internos o externos, considerando las intrusiones y vulnerabilidades, malwares. La forma de poder identificarlos depende de los criterios a ser usados y las herramientas a usar. Es por ello, debido a los diferentes tipos de amenaza digital existente se han planteado diferentes herramientas para poder detectarlos. Una herramienta muy usual para la detección de amenazas es la correspondiente de un sistema de computadoras destinadas a imitar los objetivos probables de ciberataques para colectar malwares tipo zero-day, comúnmente llamados honeypots. Una práctica recomendada en la implementación de sistemas de seguridad es lo referente a los servicios de hackeo ético. Este tipo de servicio, de acuerdo con un conjunto de herramientas detecta vulnerabilidades en los servicios digitales de la organización correspondiente, ella recomienda su remediación y eliminar o mitigar la amenaza. El esfuerzo organizacional de implementar técnicas de detección de amenazas, criterios de decisión basados en patrones de comportamiento digital relacionados, enfoques basados en conductas de usuario y esquemas de detección de la forma y manera de usar el acceso al cual el usuario está permitido.

La base fundamental del modelado de amenazas es identificar, comunicar y gestionar las debilidades de seguridad digital.

Esto se logra al comprender las posibles amenazas y ataques que el sistema debe resistir y las correspondientes contramedidas (controles) para esas amenazas. Los ataques

digitales a los sistemas han evolucionado en el tiempo, por ello podemos entender en la línea de tiempo, que estos han sido más sofisticados.

Generaciones de Ataques Digitales

- Generación 1.- A finales de la década de 1980, los ataques de virus en computadoras independientes afectaron a todas las empresas e impulsaron el aumento de los productos antivirus.
- Generación 2.- A mediados de la década de 1990, los ataques de Internet afectaron a todos los negocios e impulsaron la creación del firewall.
- Generación 3.- A principios de la década de 2000, la explotación de vulnerabilidades en las aplicaciones afectó a la mayoría de las empresas e impulsó el aumento de los productos de sistemas de prevención de intrusiones (IPS).
- Generación 4.- Aproximadamente en 2010, el aumento de los ataques dirigidos, desconocidos, evasivos y polimórficos afectó a la mayoría de las empresas e impulsó el aumento de los productos anti-bot y sandboxing.
- Generación 5.- Aproximadamente en 2017, mega ataques a gran escala y multivectores utilizando tecnologías de ataque avanzadas. Las soluciones basadas solo en la detección no son suficientes contra estos ataques de rápido movimiento. Se requiere una prevención avanzada de amenazas.

2.1.3 Marco conceptual

Amenaza digital

Se considera una amenaza digital, cuando los contenidos o los servicios publicados en la plataforma digital procuran ser alterados o vulnerados de tal forma modifican la funcionalidad de un sistema o infraestructura digital.

Se considera una amenaza digital, cuando los contenidos o los servicios publicados en la plataforma digital procuran ser alterados o vulnerados de tal forma modifican la funcionalidad de un sistema o infraestructura digital.

Sistema de Detección

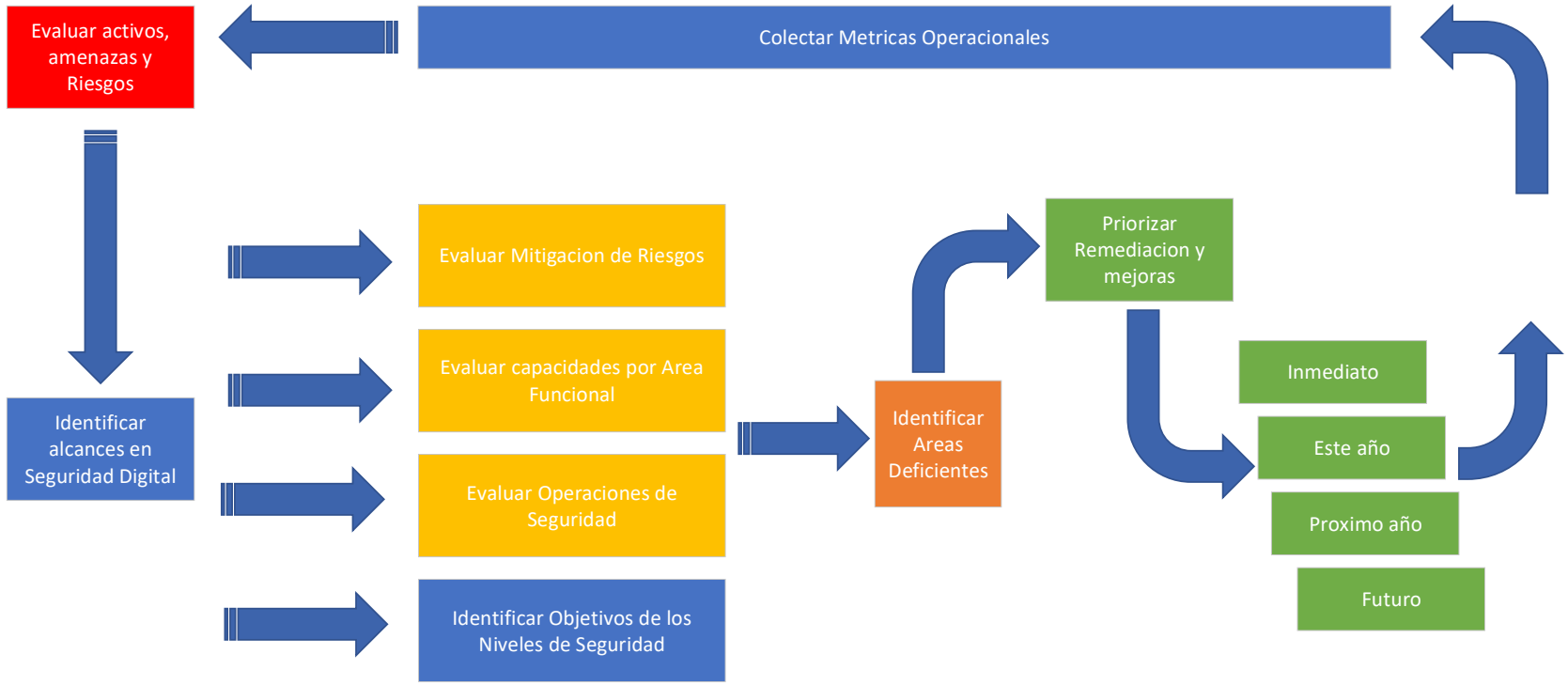
Existen plataformas a nivel de hardware y software que permiten prevenir, bloquear o detener diferentes tipos de amenazas a un servicio publicado en la plataforma digital o al sistema operativo o la funcionalidad del hardware. Los sistemas de detección alertan de estas amenazas y mitigan o eliminan la amenaza digital.

Gobierno Digital

Toda infraestructura o servicio digital que tiene una organización y que cumple una función corresponde a la forma y manera de gobernar un sistema o proceso. Se dice que existe gobernanza digital porque sus procesos de decisión son digitales.

Figura 1

Modelo de Gestión de Ciberseguridad



Servicios Web

Es un conjunto de estándares y protocolos que permite que toda plataforma digital puede operar. Bajo este esquema todos los sistemas de diferentes organizaciones pueden interoperar. Gestión

Plataforma Digital

Es la arquitectura a nivel Hardware, software, directivas, políticas y procedimientos de un sistema u organización.

Amenazas Digitales

Las amenazas digitales son programas maliciosos cuya finalidad principal es vulnerar un servicio o infraestructura digital. Está relacionado con ataques digitales generándose formas y maneras distintas de vulnerar la operatividad o continuidad de un servicio digital de una organización en particular. Sus fines son variados.

Tipos de Amenazas Digitales

Existen varias formas de clasificar los tipos de ataques o amenazas digitales (ENISA, 2019), en la definición de uso común tenemos:

1. Malware
2. Ataques Basados en Web
3. Ataques Aplicaciones Web
4. BotNets
5. Spam
6. Ransomware

7. Amenaza Interna
8. Manipulación física/daño/robo/perdida
9. Kits de explotación (exploit kits)
10. Brecha de Datos
11. Robo de Identidad
12. Fuga de información
13. Ciberespionaje
14. Amenaza Persistente Avanzada (APT)
15. Ataque Fuerza Bruta
16. Ataque Denegación de Servicio (DoS)
17. Ataque Hombre en el Medio
18. Ataque Phishing

Agentes de Amenaza

Son los medios portadores de las amenazas (ENISA, 2019) a las diferentes infraestructuras tecnológicas de la organización.

1. Cibercriminales
2. Empleados (insiders)
3. Naciones (estados)
4. Corporaciones
5. Hacktivistas
6. Ciber terroristas
7. Script kiddie.

Ciclo de vida de un ataque

El concepto de un ciclo de vida de ataque se extiende a amenazas más allá de aquellas que explotan la exposición de los sistemas de una organización en el ciberespacio, a amenazas internas, amenazas a sistemas de control industrial y otros sistemas y la cadena de suministro.

Índice Global de Ciberseguridad

Es un indicador que mide el nivel de compromiso de un país con la ciberseguridad. Tiene un amplio campo de aplicación que abarca industrias y sectores. Analizándose en 5 categorías: Medidas jurídicas, medidas técnicas, medidas organizacionales, creación de capacidad y cooperación.

Gobierno Digital

Acciones orientadas de una organización o país en torno a buenas prácticas de gobierno en el entorno digital. En el caso particular buenas prácticas del RENIEC y de las instituciones del estado tanto públicamente como internamente, de sus servicios puestos en entornos digitales.

Riesgo en ciberseguridad

Estrategias para la gestión de riesgos:

- Evitando riesgos
- Abordar los riesgos
- Aceptar riesgos
- Transferir riesgos

- Ignorar riesgos

Amenaza Persistente Avanzada (APT)

Es un ataque sofisticado y dirigido. Esta amenaza representa un riesgo para todas las organizaciones, específicamente si gestionan datos confidenciales o infraestructuras críticas. Recientemente, el análisis de estas amenazas ha llamado la atención de la comunidad científica. Los investigadores han estudiado el comportamiento de esta amenaza para crear modelos y herramientas que permitan la detección temprana de estos ataques. El uso de Inteligencia Artificial puede ayudar a detectar, alertar y predecir automáticamente este tipo de amenazas y reducir el tiempo que el atacante puede permanecer en una organización de red. El objetivo de este trabajo es una revisión de los modelos propuestos para identificar las herramientas y métodos que han utilizado.

Ciberataque

Un ataque cibernético es un asalto lanzado por ciberdelincuentes que usan una o más computadoras contra una o varias computadoras o redes. Un ciberataque puede deshabilitar maliciosamente computadoras, robar datos o usar una computadora violada como punto de lanzamiento para otros ataques. Los ciberdelincuentes usan una variedad de métodos, que incluyen malware, phishing, ransomware, denegación de servicio, entre otros métodos.

Escenarios de ataques

En referencia a escenarios de ataques vía internet o conexión línea dedicada, tenemos el de denegación de servicios – DDOS (Ataques de denegación de servicio) en ese sentido este tipo de ataques mayormente están centralizados en dejar sin servicio el servicio digital publicado en la plataforma tecnológica de la organización.

En ese sentido los criterios usados para establecer una defensa en la red son diversos y amplios. La existencia de anomalías en la red y la capacidad de poder analizar cada tráfico son muy importantes, de tal forma que mediante acciones correctamente encaminadas se puede garantizar una relativa seguridad digital en toda la plataforma digital.

Es evidente la existencia de enfoques de defensa al tener al frente una amenaza digital que pretende paralizar un servicio (denegación de servicio) o vulnerar la plataforma para la extracción de información (malwares, phishing, virus, troyanos) o extorsionar a los usuarios (ransomware) o afectar la reputación de una organización (defacement). Cada amenaza digital requiere particular atención.

Es claro que la medida adoptada para asumir los riesgos en ciberseguridad se centra en las políticas de defensa a establecer. Lo importante es identificar el tipo de amenaza existente, de tal forma los criterios establecidos indicaran la forma de defensa a realizar. Sean estos de detección, prevención, respuesta y tolerancia. Es claro que los criterios adoptados mediante los estándares correspondientes permitirán una adecuada defensa digital.

El acceso a internet es al presente masivo, en su mayor parte las organizaciones han centrado sus procesos claves en digitalizarlos y ponerlos a disposición de sus usuarios, generando una confrontación directa con amenazas directas a las plataformas digitales.

El análisis del tráfico de red, el sistema de detección de intrusos son actividades importantes al momento de construir plataformas de ciberseguridad y desarrollar un programa detallado de las acciones a realizar al momento de tener un ataque digital a la infraestructura.

No solamente es necesario establecer una política de defensa ante amenazas digitales, sino que es importante disponer una correcta infraestructura tecnológica de defensa y prevención. Los usos de los estándares de seguridad son importantes para garantizar prevención en los usuarios internos de toda organización de tal forma se establezcan los controles necesarios al momento de realizar cualquier actividad vinculada a procesos digitales.

Al presente, las tecnologías de comunicaciones permiten los accesos remotos a todo servicio digital, generando acciones de diferentes medios tecnológicos correspondientes, sean estos de cobre, fibra óptica, microondas, satelital e inalámbricos de todo tipo (bluetooth, wifi y otros) así también los medios de portabilidad digital, smartcard, equipos IOT, celulares, tabletas y otros medios de comunicación móvil.

El desarrollo de las capacidades en los colaboradores es de importancia al momento de construir infraestructuras de ciberseguridad, es muy importante entender que es necesario disponer de especialistas en la gestión de los servicios de ciberseguridad, continuidad de servicio, normas ISO y otros estándares complementarios, así también especialistas en redes y comunicaciones, sean administradores, analistas y operadores estos también deben disponer de una especialidad en ciberseguridad, continuidad de negocios, especialistas en infraestructuras de defensa y prevención digital sean estos firewall, proxys, IDS, IPS, AntiDDOS, Balanceadores de carga, WAF, SandBlast, antispam, correlacionador de eventos, filtro de contenidos, antimalwares, ethical hacking, antivirus y sus variantes y otros necesarios que quienes en coordinación con los administradores de los centros de datos, operadores y especialistas en redes.

III. MÉTODO

3.1 Tipo de investigación

Enfoque de investigación : Cuantitativo

Tipo de Investigación : No Experimental

Según la planificación de las mediciones : Prospectivo

Según Nro. De mediciones Variable : Longitudinal

Según el Numero de variables : Analítico

Nivel de Investigación : Relacional/explicativo

Pruebas No Paramétricas

Muestras relacionadas.

La investigación detalla las diferentes teorías existentes en relación con el problema en estudio. Estas teorías constituyen el soporte teórico-científico del marco teórico; luego formulamos nuestra Hipótesis y las contrastamos con la realidad problemática para arribar a conclusiones teóricas acerca del Modelo de Detección de Amenazas Digitales y la Mitigación de Riesgos de ciberseguridad en las organizaciones.

Nivel de Investigación

La presente investigación se sitúa en el nivel descriptivo-correlacional. Es descriptiva porque vamos a medir y describir la variable independiente Modelo de Detección de Amenazas Digitales y la variable dependiente Riesgos de Ciberseguridad en las organizaciones. Es correlacional porque se establecerá el nivel de correlación entre las variables para, luego llevar a cabo la interpretación respectiva.

Métodos de Investigación

El método principal que se utilizará durante el proceso de investigación será el método descriptivo-correlacional, porque se observaran los datos obtenidos para explicar la relación entre las dos variables, es decir para saber en qué medida la variación de una de ellas afecta a la otra, con la finalidad de conocer su magnitud, dirección y naturaleza. Asimismo, no se descarta el empleo del método analítico-sintético. A través de este método, se descompondrán todas las variables para observar sus relaciones, similitudes, diferencias, causas, naturaleza y efectos hacia otras variables, para luego reconstruirlas a partir de los elementos distinguidos por el análisis.

3.2 Población y Muestra

En el caso de la población, tenemos el universo considerado son 300 organizaciones que tienen una unidad relacionada a gobierno digital, siendo los responsables de las plataformas digitales con mayor presencia nacional.

Con respecto a la muestra, se ha considerado una muestra de 30 responsables de Tecnologías de información a ser revisados en sus plataformas digitales.

3.3 Operacionalización de Variables

3.3.1 Variables

Variable Independiente: Modelo de Detección de Amenazas Digitales.

Indicadores:

- Número de equipos de ciberseguridad instalados.
- Número de certificaciones en ciberseguridad.
- Número de atenciones ante incidentes de seguridad digital.

Variable Dependiente: Riesgos de ciberseguridad en las organizaciones

Indicadores:

- Índice de Gobierno Electrónico
- Políticas de gobierno electrónico en ciberseguridad.
- Índice global de ciberseguridad.

Tabla 1

Operacionalización de variables

VARIABLES	**INDICADORES**	**CONCEPTO**
Variable independiente: Modelo de detección de amenazas digitales	Número de equipos de ciberseguridad instalados.	Equipos de seguridad instalados y vigentes en el año de estudio.
	Numero de certificados en ciberseguridad.	Organizaciones que tienen certificaciones ISO27001, ISO27032, ISO 22301. .
	Número de atenciones ante incidentes de seguridad digital.	Numero de atenciones de incidentes por CSIRT.
Variable dependiente: Riesgos de ciberseguridad en las organizaciones	Índice de Gobierno electrónico	Índice que mide el nivel de avance de gobierno digital de la organización
	Políticas de gobierno electrónico en ciberseguridad.	Numero de Medidas a nivel de gobierno digital impulsados por la organización en el campo de ciberseguridad.
	Índice global de ciberseguridad	Número de ataques y/o amenazas digitales.

VARIABLE INDEPENDIENTE Modelo de Detección de Amenazas Digitales	N.º de Ítems	Nivel de Medición	Categorías	% de ítems	Instrumento
Número de Equipos de Ciberseguridad instalados	1,2,3,4	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	Cuestionario
Numero de certificaciones en ciberseguridad	5, 6, 7, 8	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	
Número de atenciones ante incidentes de seguridad digital	9,10, 11, 12	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	

VARIABLE DEPENDIENTE Riesgos de ciberseguridad en las organizaciones	N.º de Ítems	Nivel de Medición	Categorías	% de ítems	Instrumento
Índice de Gobierno electrónico	1,2,3,4	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	Cuestionario
Políticas de gobierno electrónico en ciberseguridad	5, 6, 7, 8	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	
Índice Global de ciberseguridad	9,10, 11, 12	Ordinal	- Siempre - Casi siempre - A veces - Casi nunca - Nunca	33.3%	

3.4 Instrumentos

Cuestionario: Es un documento que plantea una serie de preguntas, siendo un instrumento de investigación planteando opciones de respuestas.

3.5 Procedimientos

Los datos obtenidos a través de los instrumentos de recolección de datos seguirán el siguiente proceso:

a) Ordenamiento de datos a través de matriz de datos.
b) Técnicas estadísticas para contrastar Hipótesis. –
c) Interpretación y discusión de cuadros y gráficos.
d) Sistematización de Resultados.

3.6 Análisis de datos

La Investigación ha utilizado como estrategia general en lo referente a los datos el uso de la entrevista como instrumento de colección de datos, así como información integrada a los reportes de incidencias de seguridad en toda la organización y su referencia a nivel nacional como indicadores de posicionamiento de uso mundial, de tal forma permita integrarlo a la valoración del modelo a recomendar.

3.7 Consideraciones éticas

El presente proyecto de investigación considera importante establecer los siguientes lineamientos:

- Los documentos utilizados en la presente investigación son referenciados en forma debida, respetando la propiedad intelectual de sus autores.

- Los diseños experimentales realizados para la colecta de la información en la presente investigación se mantienen de acuerdo con las políticas de confidencial en las organizaciones en estudio.
- Se establecerá un protocolo de conocimiento informado de aquellos participantes de los trabajos al momento de realizar la colección de datos y de los resultados que se presenten.

IV. RESULTADOS

4.1 Contrastación de Hipótesis

Para evaluar la veracidad de las hipótesis planteadas, se optó por seleccionar una prueba de correlación, en base a los siguientes aspectos:

Variable 01: Modelo de Detección de Amenazas Digitales.

Variable 02: Riesgos de Ciberseguridad en las Organizaciones

Indicador 1: Número de Equipos de Ciberseguridad Instalados.

Indicador 2: Número de organizaciones con certificaciones en ciberseguridad.

Indicador 3: Numero de equipos de respuesta ante incidentes de seguridad digital.

Indicador 4: Índice de Gobierno Electrónico.

Indicador 5: Políticas Nacionales de Gobierno Electrónico en Ciberseguridad.

Indicador 6: Índice Global en Ciberseguridad.

Debido a que las variables en estudio fueron de tipo normal, se optó por realizar la prueba de Correlación de Pearson.

Prueba de correlación de Pearson

Esta prueba de correlación fue realizada con las siguientes pautas:

Evaluación de significancia

Sirvió para determinar la existencia de correlación, tomando en cuenta los siguientes criterios, según la siguiente tabla:

Tabla 2

Criterios para evaluación de significancia

Valores de significancia	Interpretación
Menores a 0.05	Existe correlación. Se continua con las pruebas
Mayores o iguales a 0.05	No existe correlación. Se rechaza la hipótesis.

Margen de error: 5%

Evaluación del valor de correlación

Sirvió para determinar la fuerza y tipo de correlación, tomando en cuenta los siguientes criterios:

Tabla 3

Criterios para evaluación del coeficiente de correlación

Valores	**Significado**
[-1.00]	Correlación negativa perfecta
<-1.00 — -0.90]	Correlación negativa muy alta
<-0.90 — -0.70]	Correlación negativa alta
<-0.70 — -0.40]	Correlación negativa moderada
<-0.40 — -0.20]	Correlación negativa baja
<-0.20 — - 0.00>	Correlación negativa muy baja
[0.00]	Correlación nula
<0.00 — 0.20>	Correlación positiva muy baja

[0.20 — 0.40>	Correlación positiva baja
[0.40 — 0.70>	Correlación positiva moderada
[0.70 — 0.90>	Correlación positiva alta
[0.90 — 1.00>	Correlación positiva muy alta
[1.00]	Correlación positiva perfecta

Correlaciones deseadas: Positiva alta, muy alta o perfecta.

HIPÓTESIS GENERAL

H1: El Modelo de detección de amenazas digitales influye en la mitigación de riesgos de ciberseguridad en las organizaciones.

Ho: El Modelo de detección de amenazas digitales NO influye en la mitigación de riesgos de ciberseguridad en las organizaciones.

Tabla 4

Resultado de la prueba de correlación

		Variable 02 Riesgos de Ciberseguridad
Variable 1 Modelo de Detección de Amenazas Digitales	Coeficiente de correlación	**0.870**
	Significancia	**0.000**

Dada la condición:

Si la significancia es > 0.05 se acepta la condición H1.

Si la significancia es < 0.05 se acepta la condición Ho

De acuerdo con la tabla 3, el valor de significancia entre las variables "Modelo de Detección de Amenazas Digitales" y "Riesgos de Ciberseguridad en las Organizaciones" (0,00) ha sido inferior al planteado (0,05), por lo tanto, se acepta H1. Del mismo modo, el coeficiente de correlación calculado (0,870) comprueba que la correlación es positiva. Por tanto, se acepta la hipótesis formulada: El Modelo de Detección de Amenazas Digitales influye en los Riesgos de Ciberseguridad de las Organizaciones.

HIPÓTESIS ESPECÍFICA 1

HE01. Existe una influencia directa en la reducción de la infraestructura de ciberseguridad y la reducción del índice global de ciberseguridad

Ho. NO Existe una influencia directa en la reducción de la infraestructura de ciberseguridad y la reducción del índice global de ciberseguridad

Tabla 5

Resultados correlación entre Número de equipos de ciberseguridad instalados y el Índice de Gobierno Electrónico

		Dimensión 01 **Índice de Gobierno Electrónico**
Indicador 1 **Número de equipos de ciberseguridad instalados.**	Coeficiente de correlación	**0.82**
	Significancia	**0.00**

Resultados obtenidos en SPSS

Dada la condición:

Si la significancia es > 0.05 se acepta la condición H1.

Si la significancia es < 0.05 se acepta la condición Ho

De acuerdo con la tabla, el valor de significancia entre las variables “Número de equipos de ciberseguridad instalados.” e “Índice de Gobierno Electrónico” (0,00) ha sido inferior al planteado (0,05), lo cual demuestra la existencia de correlación.

Del mismo modo, el coeficiente de correlación calculado (0,82) comprueba que la correlación es positiva y alta. Por tanto, se acepta la hipótesis formulada: Existe una influencia directa en la reducción de la infraestructura de ciberseguridad y la reducción del índice global de ciberseguridad

HIPÓTESIS ESPECÍFICA 2

HE02: Las organizaciones certificadas en ciberseguridad mejoran el índice global de ciberseguridad.

HEo: Las organizaciones certificadas en ciberseguridad NO mejoran el índice global de ciberseguridad.

Tabla 6

Resultados correlación entre Número de organizaciones con certificaciones en ciberseguridad y el Índice global de ciberseguridad

		Indicador 5 Índice global de ciberseguridad.
Indicador 2	Coeficiente de correlación	**0.72**

Número de organizaciones certificadas en ciberseguridad.	**Significancia**	**0.00**

Resultados obtenidos en SPSS

Dada la condición:

Si la significancia es > 0.05 se acepta la condición HE02.

Si la significancia es < 0.05 se acepta la condición Ho.

De acuerdo con la tabla, el valor de error evaluado entre los indicadores "Número de organizaciones con certificaciones en ciberseguridad" y el "Índice global de ciberseguridad" (0,00) ha sido inferior al planteado (0,00), lo cual demuestra la existencia de correlación. Del mismo modo, el coeficiente de correlación calculado (0,72) comprueba que la correlación es positiva moderada. Por tanto, se acepta la hipótesis formulada: ***Si la infraestructura de ciberseguridad se reduce el índice global de ciberseguridad disminuye.*** De hecho, esta correlación es positiva moderada.

HIPÓTESIS ESPECÍFICA 3

HE03. Existe una influencia directa entre el incremento de los equipos de respuestas a incidentes y la mejora de índice global de ciberseguridad.

HEo. NO Existe una influencia directa entre el incremento de los equipos de respuestas a incidentes y la mejora de índice global de ciberseguridad.

Si los equipos de respuestas de incidentes de seguridad se incrementan mejora el índice de global de ciberseguridad.

Tabla 7

Resultados correlación entre Número de equipos de respuesta ante incidentes de seguridad en el estado e Índice global de ciberseguridad

		Índice global de ciberseguridad.
Indicador 3 Número de equipos de respuesta ante incidentes de seguridad	Coeficiente de correlación	**0.83**
	Significancia	**0.00**

Resultados obtenidos en SPSS

Dada la condición:

Si la significancia es > 0.05 se acepta la condición HE03.

Si la significancia es < 0.05 se acepta la condición Ho.

De acuerdo con la tabla el valor de significancia entre los indicadores "Número de equipos de respuesta ante incidentes de seguridad en el estado." y "Índice global de ciberseguridad." (0,00) ha sido inferior al planteado (0,05), lo cual demuestra la existencia de correlación. Del mismo modo, el coeficiente de correlación calculado (0,83) comprueba que la correlación es positiva alta. Por tanto, se acepta la hipótesis formulada: El incremento de L***os equipos de respuestas de incidentes de seguridad mejora el índice de global de ciberseguridad.*** De hecho, esta correlación es positiva alta.

4.2 Análisis e interpretación

Variable 1: Modelo de Detección de Amenazas Digitales

Variable 1: Modelo de Detección de Amenazas Digitales

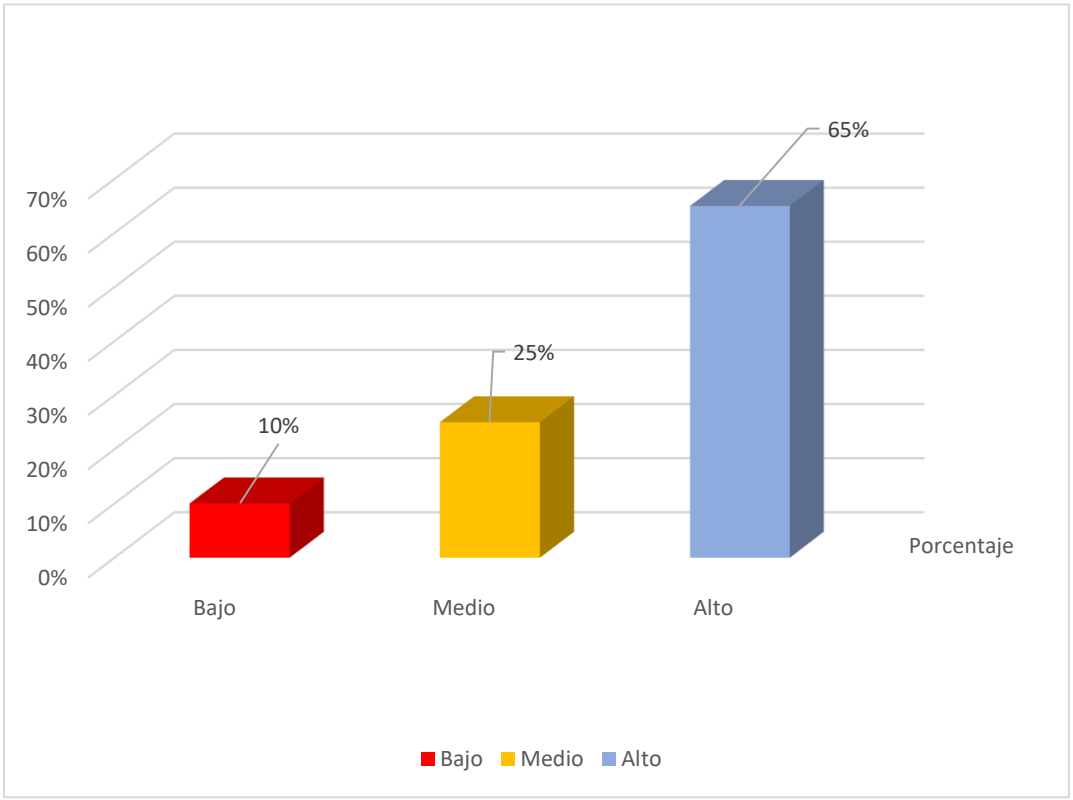
Tabla 8

Tabla de Frecuencias

Nivel	Frecuencia	Porcentaje	Porcentaje valido	Porcentaje acumulado
Bajo		10%	0%	0%
Medio		25%	2%	2%
Alto		65%	98%	100%
Total		100%	100%	

Figura Nº 1

Variable "Modelo de Detección de Amenazas Digitales



Interpretación: De la tabla N° 1 y del gráfico N° 1 se observa un alto nivel para la variable y el Modelo de Detección de Amenazas Digitales.

Donde el 65% de los encuestados considera importante el establecimiento de un modelo de detección de amenazas digitales que permitirá garantizar un nivel de cobertura de protección ante riesgos en ciberseguridad.

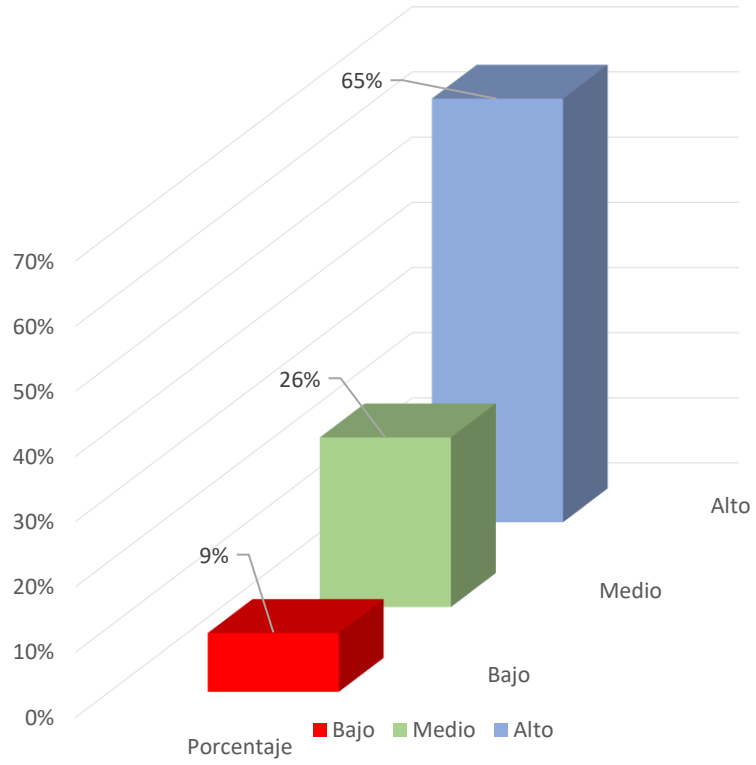
Tabla 9

Variable 2: Riesgos de Ciberseguridad en las Organizaciones

Nivel	**Porcentaje**	**Porcentaje valido**	**Porcentaje acumulado**
Bajo	9%	0%	0%
Medio	26%	14%	14%
Alto	65%	86%	86%
Total	100%	100%	

Interpretación: De la tabla N° 2 y de la figura N° 2 se observa un alto nivel para la variable Riesgos en Ciberseguridad. Donde el 65% de los encuestados considera importante la existencia de un modelo de detección de amenazas digitales.

Figura N° 2:
Gráfica de barras para la variable Riesgos en Ciberseguridad



Indicador: Número de equipos de ciberseguridad instalados

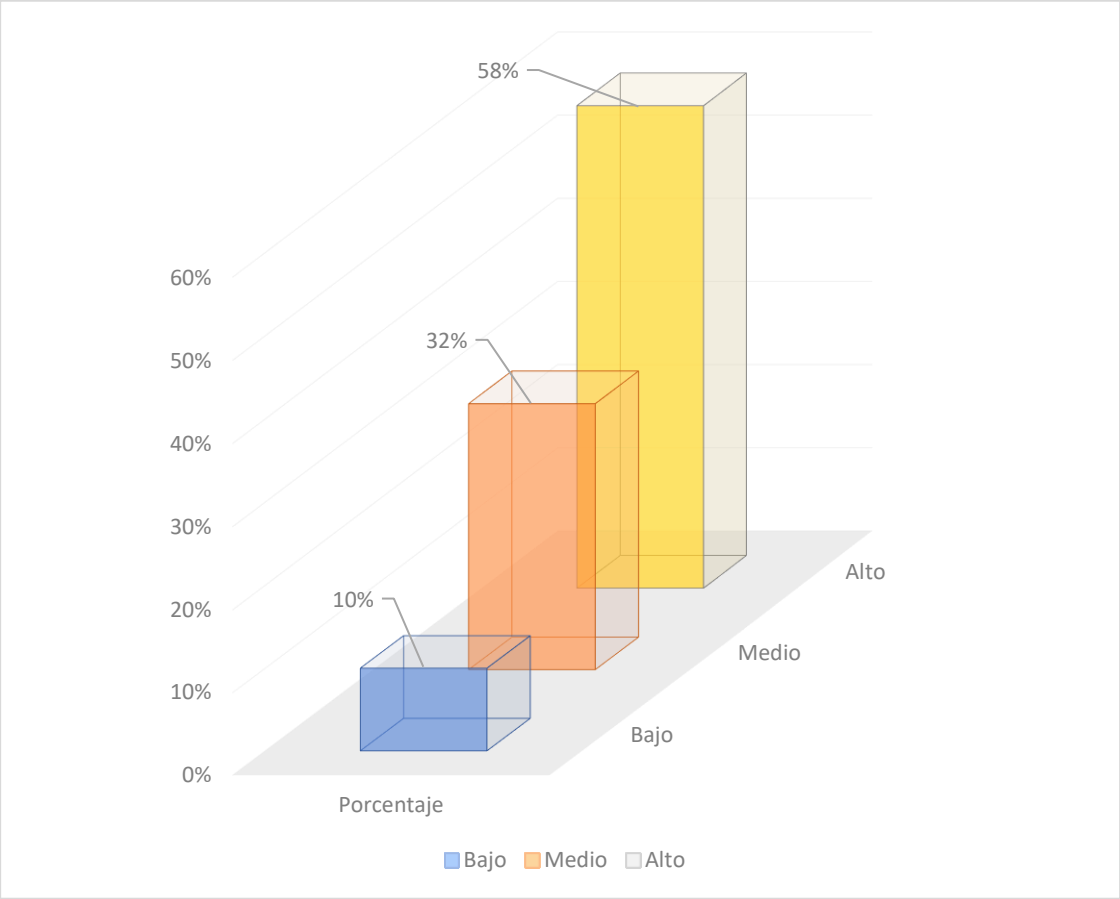
Tabla 10

Tabla de frecuencias para el indicador Número de equipos de ciberseguridad instalados

Nivel	Porcentaje	Porcentaje valido	Porcentaje acumulado
Bajo	**10%**	**0%**	**0%**
Medio	**32%**	**12%**	**12%**
Alto	**58%**	**88%**	**100%**
Total	**100%**	**100%**	

Figura Nº 3

Indicador "Número de equipos de ciberseguridad instalados"



Indicador: Número de equipos de ciberseguridad instalados

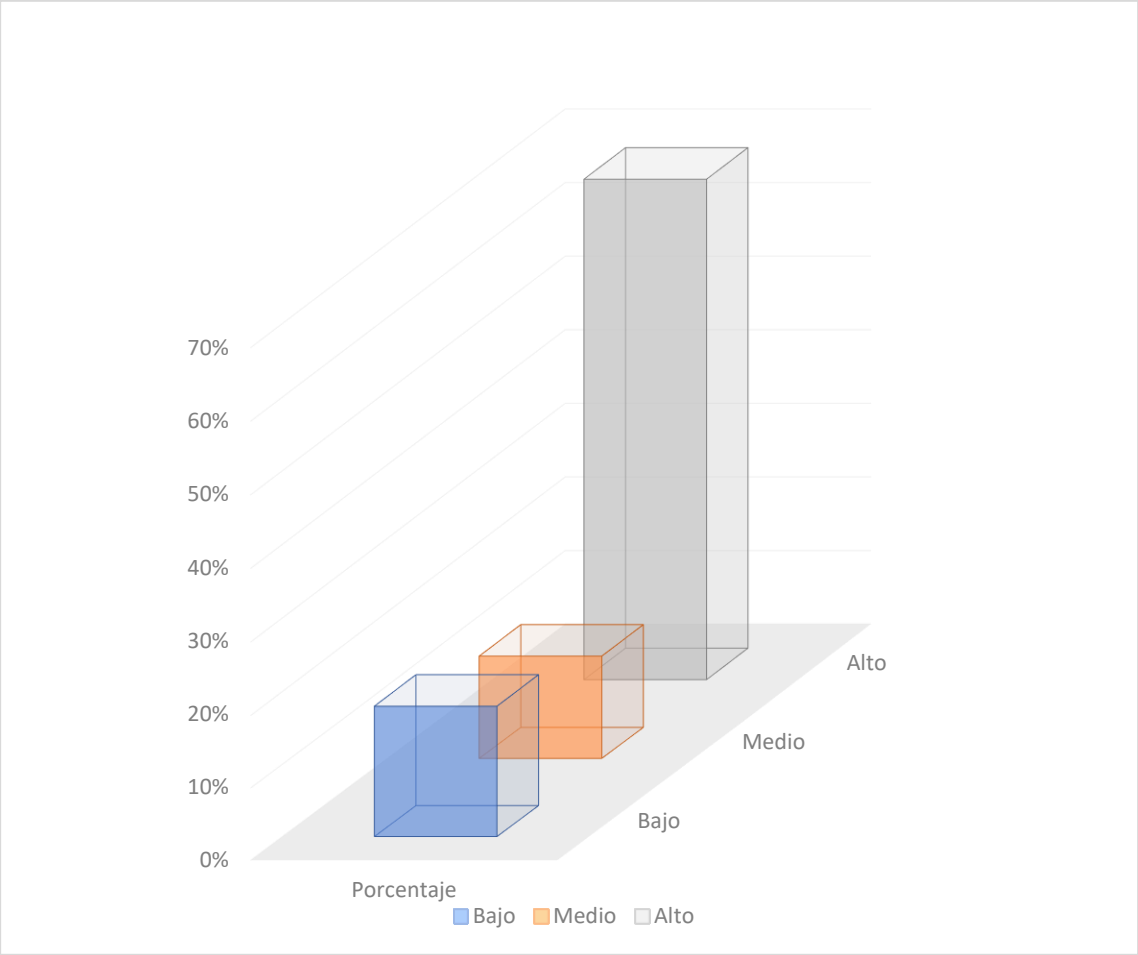
Tabla 11

Tabla de frecuencias para el indicador "Número de equipos de ciberseguridad instalados".

NIVEL	PORCENTAJE	PORCENTAJE VALIDO	PORCENTAJE ACUMULADO
BAJO	**18%**	**0%**	**0%**
MEDIO	**14%**	**2%**	**2%**
ALTO	**68%**	**98%**	**100%**
TOTAL	**100%**	**100%**	

Figura N° 4:

Gráfica de barras para indicador "Número de equipos de ciberseguridad instalados"



V. DISCUSIÓN DE RESULTADOS

5.1 Discusión

Tras haber realizado el trabajo de campo a nuestra muestra seleccionada, se ha obtenido resultados aceptables y óptimos, los cuales permiten llegar a coincidir con las afirmaciones establecidas por los diferentes autores, que fueron citados en la presente investigación.

Los resultados obtenidos nos permiten establecer que existe relación entre las variables Modelo de Detección de Amenazas Digitales y Riesgos de Ciberseguridad en las Organizaciones; del mismo modo, el coeficiente de correlación calculado comprueba que la correlación es positiva y alta. Por tanto, se acepta la hipótesis planteada que “El Modelo de detección de amenazas digitales implementado influye en la mitigación de riesgos de ciberseguridad en las organizaciones”

VI. CONCLUSIONES

Los diferentes escenarios donde las organizaciones se desarrollan consideran aspectos para tener en cuenta en la construcción de plataformas seguras. Cada aspecto debe ser considerado al momento de planificar la estrategia de prevención o defensa de los servicios digitales, considerando que cada tecnología demanda servicios de protección diferente y gestión especializada.

La detección o prevención de los activos digitales ante amenazas demandan un plan de operaciones pretendiendo entender que cada aspecto debe ser considerado al momento de elaborar un plan de mantenimiento en la atención o recuperación ante un activo afectado.

Los colaboradores deben tener las capacidades suficientes en las herramientas de gestión y de los equipos informáticos para atender las alertas que las diferentes plataformas informan a través de las consolas de monitoreo. Es necesario tener presente que una adecuada gestión en los monitoreos de los servicios garantiza una previsión ante las alertas que se presentan en las consolas de administración.

Cada servicio digital critico en la organización exige especialización de parte de la unidad responsable de seguridad digital. Tanto a nivel de la plataforma de servidores sea de aplicaciones o base de datos, así como de las soluciones de seguridad responsables de proteger los activos digitales de la organización.

VII. RECOMENDACIONES

- Es importante identificar los riesgos existentes en la organización, clasificar y establecer una estrategia de atención. Según los criterios establecidos estos deben ser clasificados si serán o no atendidos y si demandan su eliminación como factor determinante al momento de tomar decisiones.
- Es necesario tener la información de las capacidades existentes en la organización con respecto a gestión en seguridad digitales de parte de los colaboradores. Estos deben conocer las herramientas necesarias a fin de atender las alertas que se presenten al momento de las incidencias correspondientes. Las certificaciones son muy importantes de los colaboradores de todas las herramientas existentes, estas deben ser vigentes y actualizados.
- Es necesario mantener un servicio de terceros de una empresa dedicada exclusivamente a servicios de ethical hacking. Esto garantiza como los servicios digitales publicados en la organización son validados y revisados por externos de tal forma se atiendan en función de las observaciones obtenidas producto del servicio.
- Es muy importante establecer políticas de remediación de las vulnerabilidades identificadas

VIII. REFERENCIAS

Donaldson, S., Siegel, S., Williams, C., & Aslam, A. (2018). *Enterprise Cybersecurity.* APRESS.

ENISA. (2019). ENISA Threat Landscape Report 2018. European Union Agency for Network.

Gheyas, I., & Abdallah, A. (2016). Detection and prediction of insider threatsto cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, 1(6). https://doi.org/10.1186/s41044-016-0006-0

Johnson, T. (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. En *Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare*. Taylor & Francis Group.

Thakur, K., Qiu, M., Gai, K., & Ali, M. (2015). An Investigation on Cyber Security Threats and Security Models. IEEE 2nd International Conference on Cyber Security and Cloud Computing.

Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security,* 89, 53-69. https://doi.org/https://doi.org/10.1016/j.cose.2019.03.010

IX. ANEXOS

1. Matriz de consistencia

"MODELO DE DETECCIÓN DE AMENAZAS DIGITALES PARA MITIGAR LOS RIESGOS DE CIBERSEGURIDAD EN LAS ORGANIZACIONES, 2019"

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES
Problema General ¿De qué manera un modelo de detección de amenazas digitales influye en la mitigación de problemas de ciberseguridad en el estado peruano?	**Objetivo General** Diseñar un modelo de detección de amenazas digitales para mitigar el riesgo de ciberseguridad en las organizaciones	**Hipótesis General** El diseño de un modelo de detección de amenazas digitales influye en la mitigación de los riesgos de ciberseguridad en las organizaciones.	**Variable Independiente:** X: Modelo de detección de amenazas digitales Indicadores: X1: Número de equipos de ciberseguridad instalados X2: Número de organizaciones con certificaciones en ciberseguridad X3: Número de equipos de respuesta ante incidentes de seguridad en el estado.
Problemas Específicos: ¿De qué manera los equipos de ciberseguridad instalados influyen en el índice global de ciberseguridad? ¿Cómo influye el número de organizaciones con certificaciones en ciberseguridad en el índice global de ciberseguridad? ¿En qué medida los equipos de respuesta de incidentes de seguridad influyen en el índice global de ciberseguridad?	**Objetivos Específicos:** Evaluar la influencia de la infraestructura de ciberseguridad en el índice global de ciberseguridad. determinar la relación existente en organizaciones con certificaciones en ciberseguridad y su impacto en el índice global de ciberseguridad. Determinar la relación existente de los equipos de respuesta de incidentes de seguridad y el índice global de ciberseguridad.	**Hipótesis Específicas:** Si la infraestructura de ciberseguridad se reduce, el índice global de ciberseguridad disminuye. Si las organizaciones se certifican en ciberseguridad se mejora el índice global de ciberseguridad. Si los equipos de respuestas de incidentes de seguridad se incrementan, mejora el índice global de ciberseguridad.	**Variable Dependiente:** Y: Riesgos de ciberseguridad en las Organizaciones Indicadores: Y1: Índice de gobierno electrónico Y2: Políticas Nacionales de Gobierno Electrónico en Ciberseguridad Y3: Índice global de ciberseguridad-

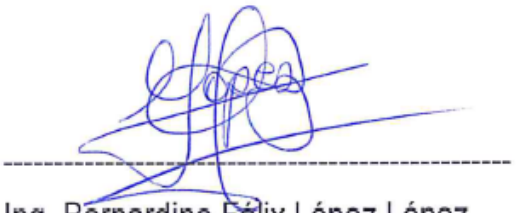
2. Validación y confiabilidad de instrumentos

CONSTANCIA

Visto que en el proyecto del trabajo de investigación denominado: **Modelo de Detección de Amenazas Digitales para Mitigar los Riesgos de Ciberseguridad en las Organizaciones, 2019** perteneciente al Ing. Félix Eloy Jiménez Chuque, se deja constancia que los instrumentos de investigación previsto para el presente estudio son coherentes con la variable, dimensiones, indicadores e ítems que evalúan para el Sistema de Gestión de Calidad; por lo que se recomiendo su aplicación.

Se refrenda la presente para fines que el autor crea conveniente.

Lima, 20 de octubre del 2019



Ing. Bernardino Félix López López
Colegio de Ingenieros del Perú: 69216

3. Confiabilidad de Instrumento

CONSTANCIA

Visto que en el proyecto del trabajo de investigación denominado: **Modelo de Detección de Amenazas Digitales para Mitigar los Riesgos de Ciberseguridad en las Organizaciones, 2019** perteneciente al Ing. Félix Eloy Jiménez Chuque, se deja constancia que los instrumentos de investigación previsto para el presente estudio son coherentes con la variable, dimensiones, indicadores e ítems que evalúan para el Sistema de Gestión de Calidad, por lo que se recomiendo su aplicación.

Se refrenda la presente para fines que el autor crea conveniente.

Análisis de Confiabilidad

Método: Alfa de Cronbach (S.P.S.S.)

****** Method 1 (space saver) will be used for this analysis ******

RELIABILITY ANALYSIS - SCALE (ALPHA)

Reliability Coefficients

N of Cases = 10,0 N of Items = 27

Alpha = ,9708

Lima, 20 de octubre de 2019

Ing. Bernardino Félix López López

Colegio de Ingenieros del Perú: 69216