Revista INNDEV ISSN 2773-7640. Abril-Julio 2024 Recibido (Received): 2024/04/20
Vol 3, Núm 1, pp 127-141 *https://doi.org/10.69583/inndev.v3n1.2024.94* Aceptado (Acepted): 2024/04/28.

TECNOLOGÍAS DE DEFENSA FRENTE A INTELIGENCIA DE AMENAZAS Y CIBERATAQUES
DEFENSE TECHNOLOGIES AGAINST THREAT INTELLIGENCE AND CYBER ATTACKS

Luis Ramírez Quevedo
Instituto Superior Tecnológico con Condición de Universitario Compu Sur

RESUMEN

La "Inteligencia de Amenazas y Ciberataques" es un campo crucial en el ámbito de la ciberseguridad, dedicado a recopilar, analizar y aplicar información relevante sobre posibles amenazas cibernéticas. Este proceso implica la recolección de datos provenientes de diversas fuentes, como bases de datos de vulnerabilidades, foros de hackers y registros de incidentes de seguridad, para luego analizarlos y detectar patrones y tendencias que puedan comprometer la seguridad de sistemas informáticos. El objetivo principal de esta disciplina es proporcionar a las organizaciones información oportuna y relevante que les permita anticipar, prevenir, detectar y responder eficazmente a posibles ataques cibernéticos. En un entorno digital en constante evolución, la inteligencia de amenazas y ciberataques se ha convertido en un elemento esencial para fortalecer la resiliencia de las organizaciones y proteger sus activos digitales frente a las crecientes amenazas en el mundo cibernético actual. En este resumen, se destaca la importancia crítica de la inteligencia de amenazas y ciberataques en la defensa activa contra las crecientes amenazas digitales en el entorno cibernético actual.

PALABRAS CLAVE: Inteligencia, amenazas, ciberataques, seguridad informática.

ABSTRACT

Cyber Attack and Threat Intelligence" is a crucial field in the field of cybersecurity, dedicated to collecting, analyzing and applying relevant information about possible cyber threats. This process involves collecting data from various sources, such as vulnerability databases, hacker forums and security incident logs, to then analyze it and detect patterns and trends that may compromise the security of computer systems. The main objective of this discipline is to provide organizations with timely and relevant information that allows them to anticipate, prevent, detect and respond effectively to possible cyber-attacks. In a constantly evolving digital environment, threat and cyber-attack intelligence has become an essential element to strengthen the resilience of organizations and protect their digital assets against the growing threats in today's cyber world. This brief highlights the critical importance of threat and cyber-attack intelligence in actively defending against growing digital threats in today's cyber environment.

KEYWORDS: Intelligence, threats, cyber-attacks, computer security
.

INTRODUCCIÓN

En la era digital contemporánea, el panorama de la seguridad informática enfrenta constantes desafíos y amenazas en evolución. La proliferación de ciberataques sofisticados y la creciente interconexión de sistemas y dispositivos han elevado la importancia de la inteligencia de amenazas como una herramienta vital en la defensa cibernética. La inteligencia de amenazas y ciberataques se ha convertido en un campo

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

fundamental en la protección de activos digitales, donde la anticipación y comprensión de las tácticas, técnicas y procedimientos de los actores maliciosos son cruciales para mitigar riesgos y fortalecer la resiliencia de las organizaciones frente a las adversidades cibernéticas.

En el vasto y complejo paisaje digital de hoy, la ciberseguridad se ha convertido en una prioridad crítica para gobiernos, empresas y usuarios individuales por igual. La constante evolución de las tecnologías y el crecimiento exponencial de las amenazas cibernéticas han dado lugar a la necesidad de un enfoque proactivo y estratégico para defenderse contra los ataques maliciosos.

En este contexto, la inteligencia de amenazas y los ciberataques emergen como pilares fundamentales en la protección de la infraestructura digital. Esta disciplina combina el análisis de datos, la comprensión de la psicología del atacante y la aplicación de técnicas avanzadas para identificar, prevenir y responder a las amenazas cibernéticas con eficacia.

En esta introducción, explicaremos los conceptos fundamentales, las metodologías clave y el impacto significativo que la inteligencia de amenazas y ciberataques tiene en la seguridad informática en la actualidad.

DESARROLLO

Inteligencia de Amenazas

La progresión tecnológica en el campo de las tecnologías de la información y la comunicación (TIC) ha transformado y sigue transformando nuestra sociedad en lo que se conoce como la aldea global.

Este avance tecnológico plantea una serie de dilemas debido a las diversas facetas que abarca. Además de los beneficios significativos que aporta a la humanidad, nos enfrentamos a las repercusiones derivadas del uso indebido, ya sea intencional o no, de estas tecnologías, en diferentes ámbitos como el gubernamental, empresarial y ciudadano (Bejarano, 2013).

La importancia de la inteligencia artificial (IA) radica en su influencia creciente. Con el aumento de la amenaza de ciberataques que pueden impactar las decisiones, la seguridad en los modelos de IA se vuelve esencial.

Este estudio se centra en evaluar cómo las técnicas de defensa en los sistemas de IA pueden mitigar esta amenaza. Se analizó el marco AI TRiSM (Gestión de Confianza,

Riesgo y Seguridad en IA) y se proporcionó una guía de buenas prácticas para su implementación. Se destaca la importancia de abordar proactivamente la gestión de la confianza, el riesgo y la seguridad en la IA para enfrentar desafíos de gobernanza y cumplimiento (Natale, 2023).

Los ataques cibernéticos representan una preocupación primordial, evidenciando los riesgos tangibles de la delincuencia informática mediante datos concretos.

La seguridad informática está constantemente en evolución y requiere la aplicación de técnicas de Inteligencia Artificial para detectar y abordar las amenazas a las que se enfrentan las organizaciones.

Con el avance de las tecnologías de la información y las comunicaciones, es fundamental implementar medidas de ciberseguridad que aseguren la confidencialidad, integridad y disponibilidad de la información, así como desarrollar habilidades para identificar y gestionar eficazmente las nuevas amenazas (Flores, 2021).

La inteligencia de amenazas desempeña un papel crucial en la prevención o mitigación de estos ataques, al proporcionar información contextual, como la identidad de los atacantes, sus motivaciones y capacidades, así como los indicadores de compromiso en los sistemas afectados.

El objetivo principal de mejorar la eficacia en la detección y gestión de amenazas cibernéticas. Esta metodología se complementa con el uso del framework de MITRE ATT&CK.

Como resultado de esta investigación, se busca desarrollar una solución innovadora que aproveche las capacidades tanto de la plataforma como de las herramientas seleccionadas, permitiendo una mayor flexibilidad y adaptabilidad personalizada para las organizaciones, con el fin de mitigar el riesgo de ciberamenazas (García-Font &

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

Ángel F, 13 junio del 2023).

En la investigación de Rodríguez en el artículo de investigación de Análisis de las ciberamenazas el ciberespacio ha introducido una nueva dimensión en las sociedades, favoreciendo el progreso gracias a las nuevas tecnologías y al uso extensivo de internet.

No obstante, en el ciberespacio es importante identificar nuevos retos a los que no se sustraen los diferentes actores políticos, principalmente los Estados. Entre estos desafíos se encuentran el ciberespionaje; las acciones de grupos terroristas y de corte yihadista; la ciberdelincuencia; y la protección y recuperación de los sistemas de infraestructuras críticas, entre otros (Rodríguez, 2022).

En la presente investigación de Pons Gamón en el artículo científico Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad el analizar la visión que tienen diversos autores sobre la aparición del ciberdelito en materia de terrorismo (ciberterrorismo) y la respuesta de las naciones en defensa cibernética es importante.

Así, desde esta misma óptica, siguiendo a Curtis (2011), podemos describir al espacio cibernético, o ciberespacio, como un dominio artificial construido por el hombre, diferenciado de los otros cuatros dominios de guerra (tierra, aire, mar y espacio); aunque se haya formalizado recientemente, el ciberespacio puede afectar a las actividades en los otros dominios y viceversa (Gamón, 2017) .

En la presente investigación según Martínez en el trabajo final de investigación Inteligencia de Amenazas Cibernéticas la inteligencia de amenazas puede definirse como inteligencia basada en conocimiento, Gartner (Sandoval, 2018) lo define como información basada en evidencias, incluido el contexto, los mecanismos, indicadores, implicancias y acciones recomendadas sobre una amenaza existente o potencial sobre los diferentes activos, que pueden ser usados para la toma de decisiones, acerca de la posible respuesta a esa amenaza o peligro (MARTINEZ, 2020).

En la presente investigación de Robayo las amenazas cibernéticas a menudo son asociadas con grandes organizaciones e instituciones financieras, lo que definitivamente es una mala interpretación del entorno existente (Tirumala, Valluri, & Babu, 2019).

Es posible que las personas que poseen ciertas habilidades de piratería informática no inviertan tiempo y esfuerzo en piratear bases de datos seguras de grandes organizaciones, en la actualidad, el sector social es uno de los entornos más utilizados para robar información individual y datos privados (VILLARROEL, 2022).

En el presente artículo de Oscar Sandoval Carlos en Uso de la inteligencia de ciberamenazas como apoyo a la comprensión del adversario aplicada al conflicto Rusia – Ucrania.

En organizaciones militares como el ejército, la Inteligencia de Ciberamenazas (CTI) apoya las operaciones cibernéticas proporcionando al comandante información esencial sobre el adversario, sus capacidades y objetivos mientras opera a través del ciberespacio. Este trabajo, combina la CTI con el marco MITRE ATT&CK para poder establecer un perfil de adversario (Sandoval, 2018) .

En la presente investigación de Christian Paul Quispe García en PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR. La importancia de la ciberseguridad radica en la preservación de los medios humanos, tecnológicos, financieros e informáticos adquiridos por las entidades para lograr los objetivos; y en la reducción de las amenazas, limitando las averías resultantes o daños, lográndose reanudar las operaciones tras un incidente informático, en un plazo de tiempo razonable y a un coste admisible, esto se recalca como un factor de inversión y una

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

necesidad de fomento de capacitación y formación de los responsables de la seguridad informática (García, 2021).

CIBERESPACIO

Mundo digital

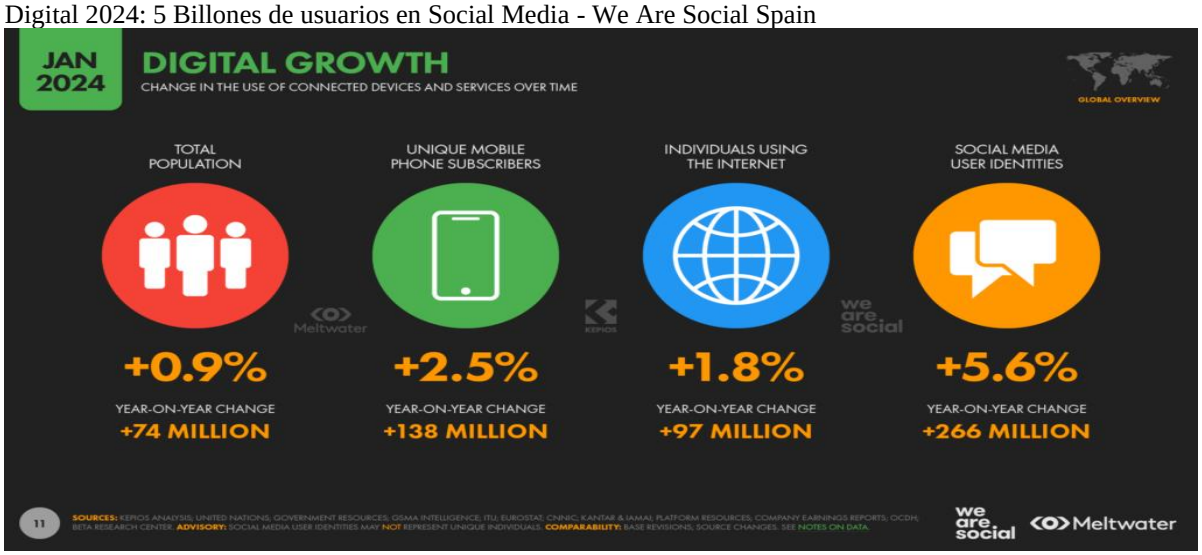
El ciberespacio representa un vasto entorno digital donde la información se convierte en unidades binarias de 0 y 1, lo que permite almacenarla, procesarla y transmitirla a través de diversas plataformas técnicas. Esta esfera digital ha tenido un gran impacto en la sociedad moderna y ha cambiado radicalmente la forma en que nos comunicamos, recibimos información y conectamos entre nosotros.

La tecnología digital, capaz de procesar datos en forma de bits binarios, ha propiciado la difusión de la electrónica. . dispositivos como computadoras, teléfonos inteligentes e Internet de las cosas (IoT) de dispositivos conectados que forman la infraestructura central del ciberespacio. Estos dispositivos producen grandes cantidades de datos, desde mensajes de texto hasta imágenes, videos y transacciones financieras.

La conectividad global a través de Internet ha creado importantes vulnerabilidades que han expuesto a personas, empresas e instituciones a diversas amenazas cibernéticas. , como malware, phishing, robo de datos y ataques de piratas informáticos.

En este contexto, la ciberseguridad se ha convertido en una cuestión clave para proteger la integridad, la confidencialidad y la disponibilidad de los datos en el ciberespacio. Se necesitan medidas preventivas como el uso de firewalls, cifrado de datos, autenticación de usuarios y actualizaciones de seguridad para reducir los riesgos y proteger la infraestructura digital de posibles ataques y violaciones de seguridad (Alegsa, 2023).

Figura 1.
Digital 2024: 5 Billones de usuarios en Social Media - We Are Social Spain



Nota: Imagen tomada de Wearesocial (España, 2024)

En la figura 1, Se nota que el usuario promedio de redes sociales ahora dedica alrededor de 2 horas y 23 minutos diarios a sus plataformas preferidas, lo que representa una disminución respecto a las 2 horas y 31 minutos registradas en 2023.

Además, mensualmente utiliza aproximadamente 6,7 plataformas diferentes.

Ciberinteligencia: "La ciberinteligencia consiste en utilizar la inteligencia en el ámbito digital. Engloba áreas tecnológicas como el análisis de malware, botnets y amenazas avanzadas persistentes (APT), todas tratadas desde una óptica militar y de seguridad defensiva." (Alumnos)

Ciberamenaza

El Instituto Nacional de Estándares y Tecnología NIST, (2023). Una amenaza se puede definir como cualquier evento que tenga el potencial de causar perjuicio a las operaciones de una organización, incluyendo su misión, funciones, imagen o reputación, así como a sus activos o

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

propiedad personal, a través de la manipulación no autorizada de sistemas de comunicación de información, que puede implicar acceso indebido, destrucción, divulgación, alteración y/o negación de información.

Además, se contempla la posibilidad de que el actor detrás de la amenaza pueda aprovechar una vulnerabilidad específica en el sistema de información para llevar a cabo sus acciones (Oas.org, s.f.).

Ciberataque

En la investigación de los siguientes autores Rosenzweig, P., Dean, E., & Choucri, N. (2002). Los ciberataques son ataques perpetrados mediante el uso de sistemas informáticos o redes de computadoras, con el objetivo de comprometer la seguridad de la información, causar daño o robar datos. Estos ataques pueden manifestarse de diversas formas, incluyendo malware, phishing, ransomware, entre otros (Oas.org, s.f.).

DEFENSA CIBERNÉTICA

Identificación de Amenazas Cibernéticas

Según la empresa Kriptos, (2023). En los últimos tiempos, la ciberseguridad se ha vuelto crucial a escala global, sobre todo para las compañías que gestionan datos confidenciales y sensibles. Por lo tanto, es esencial entender las diversas formas de ataques cibernéticos, cómo operan y qué medidas de precaución son necesarias para prevenirlos.

Figura 2.
Top 15 de amenazas en 2020

Nota: Imagen tomada de Instituto Nacional de Ciberseguridad (España, 2020)

En la figura 2, se describen los principales tipos de riesgos a los que las organizaciones pueden enfrentarse. El Instituto Nacional de Ciberseguridad busca ofrecer una perspectiva completa de las amenazas cibernéticas más relevantes en la actualidad."(INCIBE, 2021)

Inteligencia de amenazas

La Inteligencia de Amenazas implica la recolección, evaluación y aplicación de datos significativos con el fin de reconocer potenciales peligros para la seguridad de una entidad.

Este proceso se nutre de diversas fuentes, como registros de seguridad, informes de inteligencia de amenazas, estudios de malware y actividades de hacking. Al analizar esta información, es posible detectar amenazas emergentes y adoptar medidas preventivas para evitar ataques cibernéticos.

- La generación de inteligencia de amenazas generalmente surge a través del examen de datos provenientes de diversas fuentes, que abarcan:
- Herramientas de seguridad como cortafuegos, sistemas de detección de intrusiones y programas antivirus.
- Datos disponibles públicamente, como noticias, publicaciones en redes sociales y debates en foros.
- Fuentes privadas, como proveedores de seguridad y entidades especializadas en inteligencia.

Recopilar datos relevantes, como inteligencia de amenazas y análisis de software malicioso, permite a las empresas detectar patrones y comportamientos inusuales, así como anticiparse a posibles peligros.

De esta forma, se puede salvaguardar la organización frente a amenazas conocidas y desconocidas, lo que posibilita la implementación de medidas proactivas para reducir los riesgos de seguridad. Además, la integración de la inteligencia puede potenciar la eficiencia de los equipos de ciberseguridad al permitirles tomar decisiones más rápidas y fundamentadas

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

ante las amenazas emergentes.(Sousa, 2023)

Una parte esencial de la seguridad informática moderna consiste en tener un conocimiento detallado de las amenazas, lo cual resulta fundamental para que las empresas se mantengan actualizadas respecto al panorama en constante cambio.

Al estar al tanto de posibles amenazas, las organizaciones pueden anticiparse y adoptar medidas preventivas para protegerse, reduciendo así el riesgo de sufrir ataques exitosos y resguardando sus activos más importantes.

El concepto de desarrollar capacidad cognitiva para enfrentar los retos de seguridad informática abre la puerta a la exploración de herramientas que faciliten la investigación y la recopilación de datos pertinentes durante el proceso investigativo.

PRINCIPALES TIPOS DE AMENAZAS CIBERNÉTICAS

Malware

Es un término general para referirse a cualquier tipo de «malicious software» (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños e interrupciones en el sistema o robar datos (Belcic, 2023).

Figura 3.
Tipos de Malware 2024

Nota: Imagen tomada del reporte ¿Qué es el malware y cómo protegerse de los ataques? 2024, AVAST

En la figura 3, se describen diferentes tipos de malware y sus funciones. Se puede identificar el ransomware, un software malicioso que bloquea el acceso a dispositivos y archivos hasta que se pague un rescate al hacker, seguido del spyware, que recopila información para enviarla al atacante, y del adware, que bombardea dispositivos con anuncios no deseados para generar ingresos. Los gusanos, diseñados para replicarse y extenderse, y los troyanos, que se hacen pasar por software legítimo para infiltrarse, también son mencionados. Por último, se puede ver las botnets, redes de equipos infectados utilizados para ejecutar malware y realizar diversas actividades maliciosas.

Ransomware

Los ransomware se dividen en dos tipos:

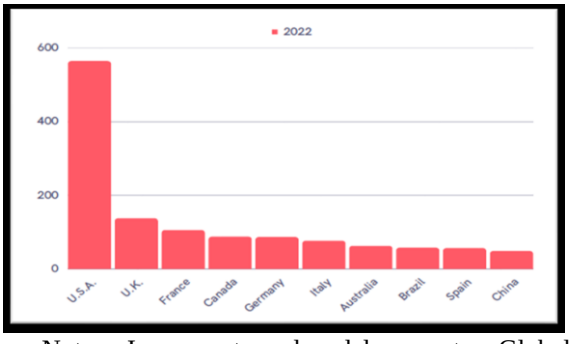
Ransomware de bloqueo. Este tipo de software malicioso está diseñado para limitar las funciones esenciales de una computadora.

Puede bloquear el acceso al escritorio del sistema y limitar parcialmente el funcionamiento del teclado y el mouse. El usuario solo puede interactuar con la ventana que solicita el pago de un rescate, mientras que las demás funciones del equipo quedan inaccesibles.

Aunque el ransomware de bloqueo restringe el uso del equipo, generalmente no afecta los archivos, lo que significa que la información de la víctima rara vez está en riesgo de desaparecer.

Este software se difunde mediante archivos adjuntos en correos electrónicos maliciosos, sitios web de dudosa reputación, aplicaciones poco confiables y dispositivos de almacenamiento infectados con virus. Su objetivo es encriptar y bloquear los datos en la computadora del usuario.

Figura 3.
Países objetivos para ataques Ransomware en 2022



Nota: Imagen tomada del reporte Global Ransomware 2022, SOCRadar

En la figura 3, se presentan los países que experimentaron una alta incidencia de

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

ataques durante el año 2022. La influencia radica en la considerable población de Estados Unidos, la abundancia de empresas, así como el hecho de que muchas sedes corporativas a nivel global se encuentren en dicho país. Además, la presencia de grupos de ransomware habitualmente asociados con Rusia añade otra capa de vulnerabilidad para las empresas estadounidenses.

Evolución de las Amenazas Cibernéticas

El mundo digital cambia constantemente y, con él, las ciberamenazas evolucionan y se vuelven más sofisticadas. Ser consciente de estas amenazas es esencial para proteger sus datos, sistemas y privacidad.

En este artículo, exploramos la evolución de las ciberamenazas y lo que necesita saber para mantenerse seguro en línea (SALDAÑA, 2023).

Tabla 1.
Amenazas Cibernéticas

El Auge del Malware
El malware ha sido una de las ciberamenazas más persistentes a lo largo de la historia. El malware ha evolucionado significativamente desde los primeros virus informáticos hasta los troyanos y ransomware actuales. Las infecciones de malware pueden provocar la pérdida de datos, el secuestro del sistema y la exposición a amenazas cibernéticas.
Phishing y Ataques de Ingeniería Social
El phishing y la ingeniería social son estrategias mediante las cuales los delincuentes manipulan a las víctimas para que divulguen datos confidenciales. Con la creciente conciencia pública sobre los correos electrónicos de phishing, los atacantes han refinado sus tácticas, empleando mensajes más persuasivos y dirigidos. Asimismo, la ingeniería social se ha extendido a las redes sociales, donde los atacantes pueden obtener información personal y dirigirse de forma más precisa a sus objetivos.
Ransomware y Extorsión
El ransomware ha mostrado un crecimiento significativo en los últimos años. En este tipo de ataque, los delincuentes cifran los datos de las víctimas y solicitan un pago a cambio de la clave de descifrado. Además, algunos casos de ransomware han incorporado la táctica de "doble extorsión", donde los atacantes amenazan con revelar información sensible si no se cumple con el pago exigido.
Ataques Dirigidos y APTs
Los ataques dirigidos, denominados Advanced Persistent Threats (APTs), son acciones cibernéticas de gran complejidad y selectividad, generalmente respaldadas por estados o grupos delictivos organizados. Estos APTs se concentran en objetivos de gran importancia, como empresas, entidades gubernamentales o centros de investigación, y suelen ser difíciles de identificar.
Internet de las Cosas (IoT) y Vulnerabilidades
El crecimiento de los dispositivos IoT ha expandido el área vulnerable para posibles ataques, dado que frecuentemente estos dispositivos carecen de medidas de seguridad sólidas. Los ciberdelincuentes pueden aprovechar estas vulnerabilidades en los dispositivos IoT para llevar a cabo diversas formas de ataques, como la formación de botnets para realizar ataques distribuidos de denegación de servicio (DDoS).
Ciberespionaje y Guerra Cibernética
El ciberespionaje y los conflictos cibernéticos han adquirido mayor relevancia a nivel global. Gobiernos y entidades estatales emplean el ciberespionaje para obtener información confidencial, mientras que los ataques cibernéticos pueden generar consecuencias de importancia en lo que respecta a la seguridad nacional.

Nota: Tabla recuperada de (SALDAÑA, 2023)

En la Tabla 1, se destacan las principales amenazas y tendencias en el ámbito de la ciberseguridad. Se abordan temas como el malware, el phishing, el ransomware, los ataques dirigidos y las APTs, las vulnerabilidades del Internet de las Cosas (IoT) y la importancia del ciberespionaje y la guerra cibernética. En conjunto, resalta cómo estas amenazas representan desafíos significativos para la seguridad digital tanto a nivel individual como a nivel gubernamental y empresarial.

OWASP TOP 10

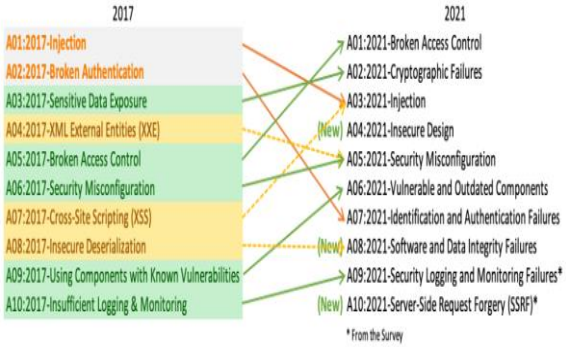
OWASP ha elaborado una variedad de recursos que detallan las vulnerabilidades más frecuentes que afectan a diversos

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

sistemas, como aplicaciones web, API, dispositivos móviles, entre otros. Entre estos recursos, destaca el OWASP Top Ten, que identifica las diez vulnerabilidades más comunes y significativas presentes en aplicaciones web en producción.

Este listado se actualiza periódicamente, basándose en datos obtenidos de pruebas de seguridad y encuestas realizadas a profesionales de la industria (BasuMallick, 2021).

Figura 4.
OWASP TOP 10 2021



Nota: Imagen tomada de OWASP Foundation 2021

En la figura 4, se observa la versión más reciente del OWASP Top Ten fue publicada en 2021. Este recurso ofrece información detallada sobre las vulnerabilidades más prevalentes, incluyendo ejemplos ilustrativos, buenas prácticas para prevenir su explotación, y descripciones sobre cómo pueden ser aprovechadas.

Además, cada vulnerabilidad hace referencia a las especificaciones relacionadas con la Common Weakness Enumeration (CWE), que detallan instancias específicas de dichas vulnerabilidades. Por ejemplo, el uso de contraseñas codificadas (CWE-259) se incluye como parte de la vulnerabilidad de fallos en la identificación y autenticación dentro del listado de las diez principales de OWASP.

Metodología del OWASP TOP 10

La selección de las Diez Principales de OWASP se fundamenta en un análisis combinado de datos proporcionados por la comunidad y una encuesta dirigida a expertos de la industria. Basándose en la información compartida por los miembros de la comunidad, el equipo de OWASP identifica las ocho vulnerabilidades más predominantes, ofreciendo así una visión clara de las debilidades más habituales presentes en el código de producción actual (BasuMallick, 2021).

Las organizaciones fueron invitadas a enviar las CWE que detectaron durante sus pruebas, junto con la cantidad de aplicaciones examinadas que contenían al menos una instancia de una CWE. Los 400 CWE resultantes fueron evaluados según su impacto y facilidad de explotación, clasificando así ocho de ellas como las principales categorías dentro de la lista de las diez principales:

1. Control de acceso roto
2. Fallas criptográficas
3. Inyección
4. Diseño inseguro
5. Mal configuración de seguridad
6. Componentes vulnerables y obsoletos
7. Fallos de identificación y autenticación
8. Fallas de integridad de datos y software
9. Fallos de registro y monitoreo de seguridad
10. Falsificación de solicitudes del lado del servidor

TECNOLOGÍAS DE DEFENSA

Defensa Perimetral

Firewall

Un firewall se refiere a un dispositivo de seguridad de red que supervisa el tráfico de datos, tanto de entrada como de salida, y toma decisiones sobre si permitir o bloquear cierto tráfico en base a un conjunto predefinido de reglas de seguridad.

Los firewalls han sido una piedra angular en la protección de redes durante más de 25 años, sirviendo como la primera línea de defensa en seguridad de red. Su función principal es establecer una barrera entre las redes internas, consideradas seguras y confiables, y las redes externas, como Internet, que no se consideran de confianza.

Existen firewalls que pueden ser implementados tanto en hardware como en software, o en una combinación de ambos, dependiendo de las necesidades y configuraciones específicas de seguridad de una red (CISCO, 2021).

Tipos de Firewall

Diferenciamos dos tipos de firewalls, destinados a diferentes tipos de

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

infraestructuras y tamaños de red.

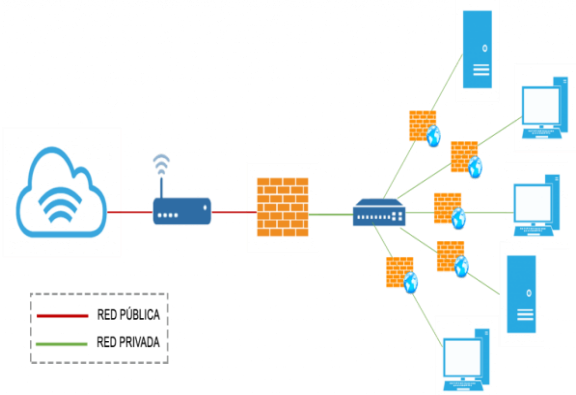
Firewall por Hardware: Este tipo de sistema se implementa en los routers utilizados para conectarse a Internet, asegurando la protección de todos los dispositivos conectados a través del router, con excepción del propio firewall. La mayoría de los routers ya incluyen un firewall integrado, lo que hace recomendable optar por aquellos que cuentan con esta función desde el inicio, dado que instalar un firewall posteriormente puede ser complicado debido a la complejidad del proceso.

Firewall por Software: Existen opciones gratuitas de firewalls diseñadas para computadoras personales, las cuales ofrecen funciones básicas de monitoreo y bloqueo del tráfico de Internet según sea necesario. En la actualidad, la mayoría de las PC ya vienen equipadas con un firewall integrado, independientemente del sistema operativo instalado.

Funciones de un Firewall

1. Crear una barrera que permita o bloquee intentos para acceder a la información en su equipo.
2. Evitar que usuarios no autorizados accedan a los equipos y las redes de la organización que se conectan a Internet.
3. Supervisar la comunicación entre equipos y otros equipos en Internet.
4. Visualizar y bloquear aplicaciones que puedan generar riesgo
5. Advertir de intentos de conexión desde otros equipos.
6. Advertir de intentos de conexión mediante las aplicaciones en su equipo que se conectan a otros equipos.
7. Detectar aplicaciones y actualizar rutas para añadir futuras fuentes de información

Figura 5.
Funcionamiento del Firewall



Nota: Imagen tomada de CISCO 2021

En la figura 5, se puede observar la función de filtrado es una medida de seguridad diseñada para resguardar el dispositivo al examinar y controlar el tráfico de red que entra y sale del mismo. Este proceso de filtrado puede basarse en diferentes criterios, como las direcciones IP de origen y destino, el protocolo IP, o los números de puerto de origen y destino.

Métodos de filtrado del tráfico

Políticas de Firewall: Las políticas de firewall definen qué tipo de tráfico de red se permite o bloquea según reglas predefinidas. Estas reglas establecen qué comunicaciones son aceptadas, bloqueando todas las demás para mantener la seguridad de la red.

Anti-Spam Firewall: El firewall anti-spam se encarga de proteger contra el correo no deseado, el phishing y otras formas de correo electrónico malicioso.

Antivirus Firewall: Este servicio, integrado en algunos firewalls, constituye la primera línea de defensa contra ataques provenientes de Internet o de enlaces WAN.

Filtrado de Contenido: El filtrado de contenido permite a los administradores bloquear ciertos tipos de contenido web mediante reglas predefinidas, sin tener que hacerlo manualmente para cada URL.

Servicio Gestionado WAP: Este servicio permite controlar y administrar los dispositivos de punto de acceso inalámbrico (WAP) para garantizar un uso seguro y autorizado por parte de los usuarios y servicios definidos.

Servicios de DPI: Los servicios de Inspección Profunda de Paquetes (DPI) permiten al administrador examinar el

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

contenido de los paquetes de datos en profundidad.

Zonas Desmilitarizadas (DMZ)

Una zona desmilitarizada (DMZ) es una red perimetral que protege una red de área local (LAN) interna del tráfico no confiable. El significado general de DMZ es una subred que se encuentra entre la Internet pública y las redes privadas.

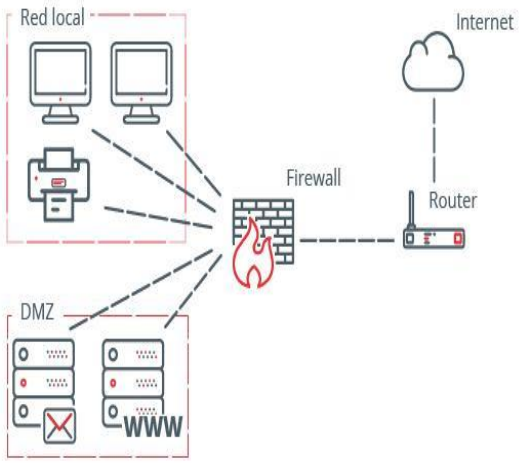
Expone las redes no confiables a servicios externos y agrega una capa adicional de seguridad para proteger los datos confidenciales almacenados en las redes internas mediante el uso de firewalls para filtrar el tráfico.

El objetivo final de una DMZ es brindarle a una organización acceso a redes no confiables, como Internet, asegurando que su red privada o LAN sea segura. En la DMZ, las organizaciones suelen almacenar servicios y recursos externos, como DNS, FTP, correo electrónico, proxy, voz sobre protocolo de Internet (VoIP) y servidores de alojamiento web (FORTINET, 2022).

Los servicios de una DMZ incluyen:

- Servidores DNS
- Servidores FTP
- Servidores de correo
- Servidores proxy
- Servidores web

Figura 6.
Funcionamiento de una DMZ



Nota: Imagen tomada de INCIBE 2022

En la figura 6, se puede observar cómo la zona desmilitarizada (DMZ) está expuesta a un mayor riesgo de ataques, por lo que es aconsejable emplear otras herramientas de vigilancia, detección y prevención. En este sentido, se recomienda el uso de sistemas de detección y prevención de intrusiones (IDS e IPS). Es crucial mantener actualizados a la última versión los sistemas ubicados en la zona desmilitarizada para garantizar una seguridad óptima.

Sistema de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (IDS) puede agilizar y automatizar el proceso de identificación de posibles amenazas en la red al notificar a los administradores de seguridad sobre riesgos conocidos o emergentes.

Puede enviar alertas a una plataforma centralizada de seguridad, como un sistema de gestión de eventos e información de seguridad (SIEM), donde se pueden integrar con datos de otras fuentes para facilitar la identificación y respuesta por parte de los equipos de seguridad ante amenazas cibernéticas que puedan eludir otras capas de seguridad (IBM, 2022).

Tipos de detecciones de un IDS

- Detección basada en firmas

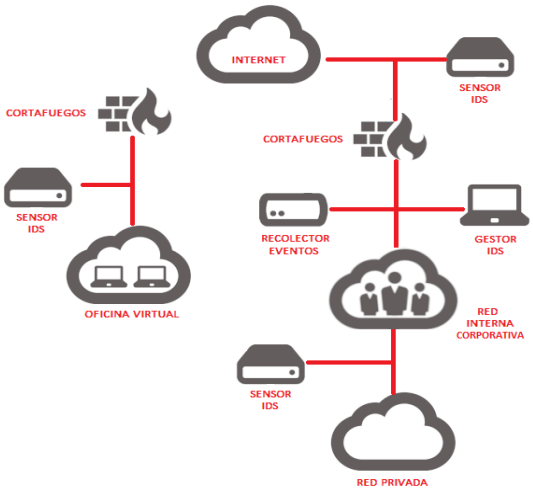
Un sistema de detección de intrusos (IDS) basado en firmas mantiene una base de datos de estas firmas de ataque y compara los paquetes de red con ellas. Si hay una coincidencia, el IDS identifica el paquete como potencialmente malicioso. Sin embargo, para mantener su eficacia, estas bases de datos de firmas deben actualizarse con regularidad para incluir nueva inteligencia sobre amenazas a medida que surgen nuevos tipos de ataques o evolucionan los existentes.

- Detección basada en anomalías

Por otro lado, la detección basada en anomalías emplea técnicas de aprendizaje automático para crear y mejorar constantemente un modelo de actividad típica de la red. Este modelo se utiliza para comparar el tráfico de red actual y señalar desviaciones significativas, como un aumento repentino en el consumo de ancho de banda o la apertura de puertos inusuales en dispositivos.

Figura 7.
Funcionamiento de un IDS

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28



Nota: Imagen tomada de INCIBE 2022

En la figura 7, se puede observar a los sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.

Sistema de Prevención de Intrusos (IPS)

Las soluciones de prevención de intrusiones (IPS) han evolucionado a partir de los sistemas de detección de intrusiones (IDS), que están diseñados para detectar y reportar amenazas al equipo de seguridad. Un IPS realiza las mismas funciones de detección y notificación de amenazas que un IDS, pero además cuenta con capacidades automatizadas para prevenir tales amenazas. Por esta razón, los IPS a veces se conocen como "sistemas de detección y prevención de intrusiones" (IDPS).

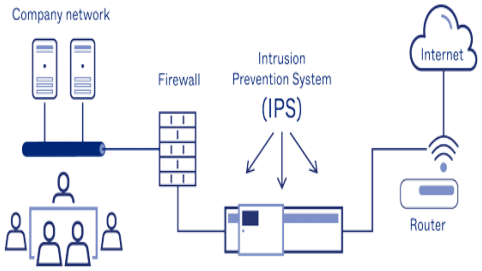
Métodos de detección de amenazas menos comunes

A pesar de que la mayoría de los IPS emplean los métodos de detección de amenazas mencionados anteriormente, algunos utilizan técnicas menos convencionales.

La detección basada en la reputación identifica y bloquea el tráfico proveniente de direcciones IP y dominios vinculados a actividades maliciosas o sospechosas.

Por otro lado, el análisis de protocolos con seguimiento de estado se enfoca en el comportamiento del protocolo; por ejemplo, puede detectar un ataque de denegación de servicio distribuido (DDoS) al identificar una única dirección IP que realiza múltiples solicitudes de conexión TCP simultáneas en un corto período de tiempo (IBM, 2022).

Figura 8.
Funcionamiento de un IPS



Nota: Imagen tomada de ABC XPERTS 2022

En la figura 8, se puede observar al sistema que asiste a las organizaciones en la detección de tráfico malicioso y en la adopción de medidas proactivas para bloquear el acceso a la red.

Indicadores de Compromiso (IOC)

Un Indicador de Compromiso (IOC) representa un conjunto de información relacionada con un objeto o actividad que sugiere un acceso no autorizado al sistema (compromiso de datos).

Por ejemplo, una serie de intentos fallidos de inicio de sesión en el sistema podría ser considerado un indicador de compromiso.

El análisis de IOC implica la identificación de estos indicadores de compromiso en el sistema y la implementación de medidas de respuesta adecuadas frente a posibles amenazas.

Funcionamiento IOC

La instrucción IOC es una de las múltiples instrucciones de trading automatizadas que cuentan con condiciones predefinidas específicas. Las órdenes IOC se ejecutan de inmediato, ya sea total o parcialmente. Si las condiciones no se cumplen, incluso de manera parcial, la orden se cancela en su totalidad (KASPERSKY, 2023).

Figura 8.
IOC (Indicadores de compromiso)

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

Supported OpenIOC Term	Data Type
ArpEntryItem/CacheType	string
DnsEntryItem/DataLength	int
EventLogItem/CorrelationActivityId	string
FileItem/FileExtension	string
PortItem/CreationTime	datetime
ProcessItem/arguments	string
RegistryItem/Hive	Тип данных string
ServiceItem/arguments	string
UserItem/description	string
VolumeItem/ActualAvailableAllocationUnits	int
SystemInfoItem/MAC	string

Nota: Imagen tomada de KASPERSKY 2023

En la figura 8, se puede observar la información pertinente que caracteriza cualquier incidente de seguridad cibernética, actividad sospechosa y/o elemento malicioso se identifica a través del análisis de sus pautas de conducta.

CYBER KILL CHAIN

Explica el procedimiento típico que siguen los ciberdelincuentes para completar un ataque cibernético con éxito.

La Intrusion Kill Chain es un proceso dirigido contra un objetivo con la intención de conseguir unos efectos deseados.

Se trata como una cadena porque se compone de una serie de pasos necesarios donde una mitigación en cualquiera de ellos supone la ruptura de la cadena, reflejada en una frustración del atacante (INCIBE, 2020).

Funcionamiento del CYBER KILL CHAIN

- **Reconocimiento:** Se trata de la fase en la que el ciberdelincuente recopila información sobre su objetivo. Para ello, observa los detalles que la organización publica en abierto y busca información sobre la tecnología que utiliza, así como datos en redes sociales e incluso realiza interacciones por correo electrónico.
- **Preparación:** En esta fase se prepara el ataque de forma específica sobre un objetivo. Por ejemplo, un atacante podría crear un documento PDF o de Microsoft Office e incluirlo en un correo electrónico que suplante la identidad de una persona legítima con la que la empresa interactúa normalmente.
- **Distribución:** En esta etapa se produce la transmisión del ataque, por ejemplo, mediante la apertura del documento infectado que había sido enviado por correo electrónico, accediendo a un phishing, etc.
- **Explotación:** Esta fase implica la «detonación» del ataque, comprometiendo al equipo infectado y a la red que pertenezca.
- **Instalación:** Fase en la que el atacante instala el malware en la víctima. También puede darse la circunstancia de que no se requiera instalación, como en el robo de credenciales o en el fraude del CEO. En cualquier caso, la formación y concienciación en ciberseguridad
- **Comando y control:** En este punto el atacante cuenta con el control del sistema de la víctima, en el que podrá realizar o desde el que lanzar sus acciones maliciosas dirigidas desde un servidor central conocido como C&C (Command and Control), pudiendo sustraer credenciales, tomar capturas de pantalla, llevarse documentación confidencial, instalar otros programas, conocer cómo es la red del usuario, etc.
- **Acciones sobre los objetivos:** Esta es la fase final en la que el atacante se hace con los datos e intenta expandir su acción maliciosa hacia más objetivos.

GESTIÓN DE AMENAZAS Y RESPUESTA A INCIDENTES

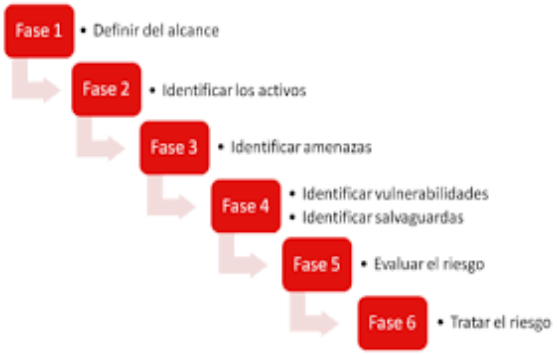
Metodología MAGERIT

El término MAGERIT es la abreviatura de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones. Este método abarca la fase AGR (Análisis y Gestión de Riesgos).

En el contexto de la gestión integral de la seguridad de un sistema de información basado en la norma ISO 27001, MAGERIT se considera el elemento central que guía todas las acciones organizadas en este ámbito. Ejerce influencia en todas las fases de carácter estratégico y condiciona el alcance de las fases de índole logística.

Figura 9.
Fases de la metodología MAGERIT

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28



Nota: Imagen tomada de Universidad Piloto de Colombia 2015

En la figura 8, se puede observar como el proceso comprende seis etapas, que comienzan con la identificación de los activos pertinentes, seguida de la evaluación de las amenazas a las que están expuestos, la definición de medidas preventivas, la evaluación del impacto residual y, por último, la estimación del riesgo residual.

Buenas prácticas de la Metodología MAGERIT

1. Identifica las posibles dificultades de los riesgos.
2. Analiza los posibles problemas de los riesgos.
3. Prioriza el posible efecto de los riesgos.
4. Aborda un plan para abordar los riesgos.
5. Monitorea continuamente las posibles amenazas de los riesgos.

Aplicación de MAGERIT en la Inteligencia de Amenazas

El objetivo perseguido en sucesivas versiones de MAGERIT (ESGINNOVA, 2015) es la evaluación, homologación y certificación de Seguridad de Sistemas de Información (SSI) según ISO 27001:

1. Es importante considerar los criterios de ITSEC para evaluar la seguridad de las tecnologías de la información, siguiendo una recomendación del Consejo Europeo.
2. Además, se toma en consideración la referencia de los Criterios Comunes para evaluar la seguridad de productos y sistemas de información.
3. MAGERIT se utiliza específicamente cuando se necesita realizar un Análisis y Gestión de Riesgos (AGR) para evaluar los criterios de seguridad.

METODOLOGÍA

Tipos de investigación

De Campo

Para el siguiente trabajo de investigación propuesto se hará uso de este tipo de investigación se apoya en informaciones que provienen entre otras, de artículos científicos, entrevistas, cuestionarios, observaciones, adicionalmente podemos complementar este tipo de investigación junto a la investigación de carácter documental, ya que se recomienda que primero se consulten las fuentes documentales, a fin de evitar una duplicidad de trabajos.

Exploratoria

Con el fin de abordar los análisis de caso de estudio se hará uso de la investigación exploratoria, esta ya que este tipo de investigación se ha considerado como el primer acercamiento científico a un problema, se debe recalcar que se utiliza cuando éste aún no ha sido abordado o no ha sido suficientemente estudiado y las condiciones existentes no son aún determinantes. Considerando que nuestro proyecto es investigativo se pretende destacar los aspectos fundamentales de una problemática determinada “colocar sobre el tema propuesto” y de esta forma se definirán los procedimientos adecuados para elaborar una investigación posterior.

Método de Investigación

Los métodos de investigación son las estrategias, procesos o técnicas utilizadas en la recolección de datos o de evidencias para el análisis, con el fin de descubrir información nueva o crear un mejor entendimiento sobre algún tema, dentro de ellas para fundamentar este proyecto aplicaran varias técnicas de investigación.

Técnicas de investigación

- Revisión bibliográfica: Se puede realizar una revisión bibliográfica exhaustiva para recopilar información relevante y actualizada sobre el “Inteligencia de Amenazas y Ciberataques” Esto implica revisar publicaciones científicas, informes

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

técnicos, sitios web especializados y otras fuentes confiables.

- Investigación de campo: Se pueden realizar entrevistas con expertos "sobre Inteligencia de Amenazas y Ciberataques" Se pueden llevar a estudios de factibilidad o análisis comparativos para evaluar su efectividad y determinar cuáles son las mejores opciones.
- Análisis de casos de estudio: Se pueden analizar casos de estudio "basados en el tema propuesto", de manera que permite analizar las experiencias de otros y recomendar futuros proyectos en base a estos casos de éxito o investigaciones relacionadas con "el tema de investigación"
- Encuestas: Para el presente proyecto de investigación no se realizarán encuestas direccionadas a una población o muestra seleccionada, esto contemplando que el estudio propuesto está basado en un análisis de caso de estudio, de manera que se aplicará una muestra extrapolar de las fuentes de investigación utilizadas en el proyecto, esto en el caso de su aplicación.

CONCLUSIONES

La amenaza cibernética es una realidad cada vez más presente en el panorama actual, con ataques sofisticados y variados que pueden comprometer la seguridad de organizaciones y usuarios en todo el mundo.

Las tecnologías de defensa han evolucionado significativamente para hacer frente a estas amenazas, adoptando enfoques proactivos y basados en inteligencia artificial para detectar, prevenir y responder a los ataques de manera eficiente.

La colaboración entre diferentes actores, tanto públicos como privados, es fundamental para mejorar la protección cibernética, compartiendo información y recursos para fortalecer las defensas y anticiparse a las nuevas tácticas utilizadas por los ciberdelincuentes.

La capacitación y concientización del personal son aspectos clave en la estrategia de defensa, ya que una buena higiene cibernética y el conocimiento de las prácticas seguras pueden reducir significativamente el riesgo de éxito de los ataques.

A pesar de los avances en las tecnologías de defensa, la amenaza cibernética seguirá evolucionando, por lo que es necesario mantenerse constantemente actualizado y adaptar las estrategias de seguridad en consecuencia.

REFERENCIAS BIBLIOGRÁFICAS

Alegsa, L. (2023). *Alegsa*. Obtenido de https://www.alegsa.com.ar/Dic/mundo_digital.php#h1

Alumnos, A. (s.f.). ¿Qué es y para qué sirve la Ciberinteligencia? *LISA Institute*. Obtenido de https://www.lisainstitute.com/blogs/blog/ciberinteligencia-que-es-y-para-que-sirve

BasuMallick, C. (2021). *f5*. Obtenido de https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/

Bejarano, M. (2013). Más sobre la amenaza cibernética. *Pre-bie3*, 4, 6.

Belcic, I. (2023). *¿Qué es el malware y cómo protegerse de los ataques? ¿Qué Es el* . Obtenido de https://www.avast.com/es-es/c-malware#:~:text=Malware%20es%20un%20t%C3%A9rmino%20general,el%20sistema%20o%20robar%20datos.

CISCO. (2021). *CISCO*. Obtenido de CISCO: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html#:~:text=Un%20firewall%20es%20un%20dispositivo,durante%20más%20de%2025%20años.

ESGINNOVA. (2015). *PMG-SSI*. Obtenido de https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Flores, C. S. (2021). Inteligencia Artificial, Machine Learning, Deep Learning aplicados a la Ciberseguridad. *INF-FCPN-PGI Revista PGI (7)*, 11, 13. Obtenido de https://ojs.umsa.bo/ojs/index.php/inf_

Recibido (Received): 2024/04/20
Aceptado (Acepted): 2024/04/28

fcpn_pgi/article/view/96

FORTINET. (2022). *FORTINET*. Obtenido de https://www.fortinet.com/lat/resources/cyberglossary/what-is-dmz

Gamón, V. (2017). Revista Latinoamericana de Estudios de Seguridad. Internet, la nueva era del delito:. 21.

García, C. (2021). PROCEDIMIENTO DE GESTIÓN PARA CIBERSEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DEL SECTOR FINANCIERO SEGMENTO 1 REGULADO POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA (SEPS) EN EL CANTÓN AMBATO – ECUADOR. . *UNIVERSIDAD TÉCNICA DE AMBATO*.

García-Font & Ángel F. (13 junio del 2023). Implementación de una plataforma de Inteligencia de Amenazas (Threat Intelligence). Obtenido de https://openaccess.uoc.edu/handle/10609/148311

IBM. (2022). *IBM*. Obtenido de https://www.ibm.com/mx-es/topics/intrusion-detection-system

INCIBE. (2020). Obtenido de INCIBE: https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces

KASPERSKY. (2023). *KASPERSKY*. Obtenido de https://support.kaspersky.com/KESWin/11.7.0/es-MX/213408.htm

MARTINEZ, L. (2020). inteligencia de Amenazas Cibernéticas. *Buenos Aires: Carrera de Especialización en Seguridad*.

Natale, A. (2023). IA segura mediante IA TRiSM: reducción de ciberataques y brechas de seguridad.

Oas.org. (s.f.). Obtenido de https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Rodríguez, J. (2022). Inteligencia, ciberespacio, ciberamenazas, riesgos, amenazas, ciberseguridad, ciberataques, CERT. . *Análisis de las ciberamenazas*, 42.

SALDAÑA, J. R. (2023). *deustoes*. Obtenido de https://deustoes.com/2023/12/10/la-evolucion-de-las-amenazas-ciberneticas-lo-que-debes-saber/

Sandoval, C. (2018). Using cyber threat intelligence to support adversary understanding applied to the Russia-Ukraine conflict. 27.

VILLARROEL, I. (2022). MODELO DE MEJORA DEL ESTADO DE LA CIBERSEGURIDAD . *Pontificia Universidad Católica del Ecuador*.