https://repository.uaeh.edu.mx/revistas/index.php/xikua/issue/archive
XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan
Xikua
ISSN: 2007-4948
Publicación semestral, Vol. 13, No. 26 (2025) 7-18

Arquitectura de malla de ciberseguridad (CSMA) y nuevas tendencias
CyberSecurity Mesh Architecture (CSMA) and new trends

Héctor Julio Fúquene Ardila [a]

Abstract:

This article identifies and describes the mesh security architecture, highlighting the advantages it offers in the treatment and assurance of information in a diverse environment, where equipment and users demand a particular treatment that includes different locations, services and applications; in addition, an analysis is made of the integration of CSMA with other security frameworks and models that were developed as a result of the confinement caused by the pandemic. The importance of integrating tools in today's world to provide greater agility in the detection and response to different incidents is highlighted; an aspect in which the use of artificial intelligence and Machine Learning (ML) contributes enormously.
Keywords:
Architecture, cybersecurity, cybersecurity mesh, security intelligence, distributed identity.

Resumen:

En el presente artículo de revisión se hace una identificación y descripción de la arquitectura de seguridad en malla, resaltando las ventajas que ofrece en el tratamiento y aseguramiento de la información en un ambiente diverso, en donde equipos y usuarios demanda un tratamiento particular que contempla diferentes ubicaciones, servicios y aplicaciones; además se hace un análisis de la integración de CSMA con otros marcos y modelos de seguridad que se desarrollaron a raíz del confinamiento originado por la pandemia. Se resalta, la importancia que tiene en el mundo actual la integración de herramientas para dar mayor agilidad en la detección y respuesta a los diferentes incidentes; aspecto en cual contribuye enormemente el uso de la inteligencia artificial y el Machine Learning (ML).
Palabras Clave*:*
Arquitectura, ciberseguridad, malla de ciberseguridad, inteligencia de seguridad, identidad distribuida.

Introducción

El impacto de la pandemia en muchos aspectos de la vida de las personas en los ámbitos familiares, lúdicos, educativos y laborales ocasionaron un cambio en los paradigmas y modelos que se utilizaban para garantizar la seguridad de la información digital; aspectos como el aumento de trabajo remoto, creó la necesidad de tener a usuarios y equipos fuera del ambiente empresarial y de red local o corporativa; aspecto que obligó a hacer mucho más granular las estrategias para el aseguramiento y tratamiento de usuarios, recursos, equipos y aplicaciones, y generó la adopción y utilización de metodologías como el de microsegmentación, los microservicios, la virtualización y la adopción de modelos de seguridad de cero confianza o Zero-Trust. El aseguramiento de este nuevo ecosistema demanda de una gran variedad de herramientas con las cuales cubrir cada una de las necesidades de aseguramiento particulares. Otro aspecto a tener en cuenta es el aumento en la inversión en tecnología (uso de diversas aplicaciones), lo cual generó la necesidad del fortalecimiento y cualificación del recurso humano necesario para suplir estas necesidades. Paralelo a esto, se dio un aumento en los incidentes de seguridad que afectaron a numerosas empresas de diversos sectores económicos; hecho que generó la necesidad de crear modelos para facilitar la gestión de la seguridad de la información de forma centralizada; la cual involucra el uso de herramientas de diversos orígenes y tecnologías y el uso de algoritmos de punta y técnicas de inteligencia artificial entre otras. A continuación, se presentan algunos datos estadísticos en el ámbito de la ciberseguridad postpandemia.

Algunos datos del sector de la seguridad de la información

Según un reporte del IC3 (Internet Crime Complaint Center) del FBI (Federal Bureau of Investigation), las denuncias en el ámbito de la seguridad pasaron de 301.580 en 2017 a

[a]*Autor de Correspondencia, Universidad Distrital Francisco José de Caldas, https://orcid.org/0009-0005-3946-8190, Email: hfuquene@udistrital.edu.co*

Fecha de recepción: 25/03/2025, Fecha de aceptación: 30/04/2025, Fecha de publicación: 05/07/2025
DOI: https://doi.org/10.29057/xikua.v13i26.14805

847.376 en 2021, adicionalmente, las pérdidas económicas en el mismo periodo pasaron de 1.4 billones en 2017 a 6.9 billones en 2021. (Fuente: IC3 Report FBI). Una de las causas de este aumento fue el robo de identidad el cual tuvo un aumento de más del 100%. (fuente: Consumer Sentinel Network Data Book del 2020 de la FTC). 1
De otra parte, la cantidad de datos en la web se duplica cada año, lo que genera un gran volumen de información y el aumento de incidentes de seguridad, aspecto que hace más complejo el trabajo de los encargados del área; esto sumado a la diversidad de formas de acceso que demandan que la gestión se realice de forma mas flexible y centralizada, utilizando estrategias que permitan integrar técnicas, modelos, metodologías y marcos de seguridad que se apoyen en herramientas como la inteligencia artificial y el Machine Learning y que contribuyan con a la solución.

Algunas de las consecuencias generadas en la pandemia y que impactaron la seguridad de la información fue el cambio en los modelos de trabajo, el aumento de equipos y usuarios conectados, el aumento en el volumen de los datos digitales en uso, el incremento de la demanda de servicios en la nube y la proliferación de ataques y la utilización de una gran variedad de herramientas para contrarrestarlos. A continuación, se presentan algunos datos publicados por la empresa Fortinet bajo el título "*Automatización de operaciones de seguridad*" y que recoge datos estadísticos especializados del sector de las tecnologías de la información y de las comunicaciones. 2

Algunas de las dificultades de los encargados de la seguridad giran en torno al uso de demasiados endpoints, insuficiencia de personal capacitado, visibilidad inadecuada de datos y sobrecarga de alertas. De otra parte, los adversarios (criminales) utilizan cada vez más la automatización de ataques y el aprendizaje automático (ML Machine Learning) para moverse más rápido y evitar ser detectados; lo que ha generado una mayor demanda y utilización de más productos de seguridad y la adopción de ML; aun así, los centros de operaciones de seguridad (SOC) siguen completamente saturados; se espera que con el uso de ML se puedan solventar gran parte de la problemática.

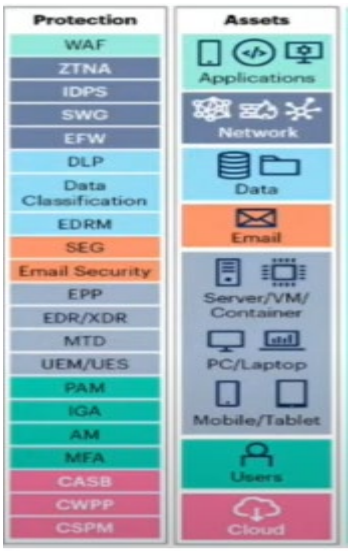
Los estudios presentan como alternativa de solución las mallas de seguridad o CSMA que es un enfoque arquitectónico que facilita la integración y la interoperabilidad entre distintos productos de seguridad para lograr una postura de seguridad más consolidada. Según Gartner, "Para 2024, las organizaciones que adopten una arquitectura de malla de ciberseguridad para integrar herramientas de seguridad, de modo que funcionen juntas como un ecosistema, reducirán el impacto financiero de los incidentes de seguridad individuales en un 90%, en promedio". Con la integración de herramientas se logrará la automatización de muchos procesos, el cierre de brechas de seguridad y la distribución de la gestión de la seguridad lo cual redundará en una gestión más ágil y robusta.
Sobre el particular algunos estudios han identificado que más de la mitad de las organizaciones consideran que el entorno de operaciones de seguridad se ha vuelto más difícil de gestionar en los dos últimos años; el 58% de las organizaciones afirma que solo tiene una cobertura de activos del 75% y que el 83%de las organizaciones no tiene una visión unificada de la gestión de la seguridad en la nube y on premise. 3 4 5 6. De otra parte, la escasez de personal capacitado e idóneo que posea las suficientes habilidades en el área dificultan las operaciones de aseguramiento de la información; se estima que hay un faltante de 3.4 millones a escala mundial de trabajadores en el área. 7. Además, el aumento de falsos positivos que se camuflan en el flujo de alertas y con el aumento de herramientas se hace cada vez más difícil tener un control general de los problemas de seguridad en las organizaciones. 8. La tendencia es que la gran mayoría de las organizaciones están automatizando los procesos de seguridad y utilizando diferentes herramientas para identificar patrones y anomalías, con lo cual contrarrestar la falta de datos y la insuficiencia de reglas y análisis que faciliten la gestión de la seguridad de la información y aumenten el beneficio de corporativo 9 10 11.

En este contexto se resaltan una serie de inconvenientes post pandemia, que hacen que las empresas dedicadas a la ciberseguridad tengan que replantear sus estrategias en torno a garantizar la confidencialidad, la integridad y la disponibilidad de los datos.

Descripción de la problemática

En el último lustro, el campo de la informática y las comunicaciones sufrió una gran transformación; por un lado, el aumento de la demanda de servicios por parte de usuarios en áreas, como el de la educación, el trabajo, de entretenimiento, generó que el número de usuarios y equipos conectados a internet aumentara; hecho que también impulsó el aumento en los riesgos y de los incidentes de seguridad. Para contrarrestar este problema, se generó en el mercado numerosas herramientas que se encargaban de dar soluciones particulares a cada necesidad (on-premise, endpoints, red, usuarios, datos, procesos y cloud), teniendo, además, que dichas herramientas fueron desarrolladas por diversas empresas y con tecnologías diversas; ver figura No. 1. Algunas de las soluciones propuestas fueron el uso de arquitecturas como SIEM y SOAR (Security Information and Event Management, Security Orchestration, Automation and Response), con la cual se podían integrar herramientas que fueran compatibles pero que la gestión no era lo suficientemente ágil como se requería; en la actualidad, existen numerosas herramientas de diversas empresas que utilizan este enfoque arquitectónico. La proliferación de herramientas, la falta de visibilidad de todos los datos, la demora en los tiempos de detección y respuesta, la rigidez de los modelos de seguridad, hacen que aumente la superficie de ataque y cada vez sea más difícil la generación de políticas coherentes que solucionen los problemas de forma ágil y eficaz.

Figura No. 1. Aplicaciones y activos a proteger



Fuente: www.gartner.com

Objetivo

Realizar una revisión del estado del arte de las nuevas tendencias en seguridad de la información en cuanto a las mallas de seguridad con las cuales se garantiza la confidencialidad, la integridad y la disponibilidad de la información en las empresas.

Metodología

El propósito de este artículo es realizar un estudio del impacto que ha tenido el confinamiento y la pandemia en el área de la seguridad de la información y de las nuevas tendencias, estrategias y modelos que se han generado con el fin de garantizar la confidencialidad, la integridad y la disponibilidad de los datos; teniendo como referencia los datos estadísticos que se presentaban pre y post pandemia, para lo cual se realizará una consulta exhaustiva de los datos correspondientes a estudios de compañías especializadas; además, se da una descripción de la problemática generada en los procesos de generación, almacenaje, procesamiento y transferencia de información y se incluirán los aspecto más importantes del modelo de seguridad en malla o CSMA (Cyber Secutrity Mesh Architecture). Para lo anterior se revisó la bibliografía e infografía a partir del año 2019 a la fecha, se analizaron estudios realizados por compañías especializadas en el área como Gartner, ISACA, Forrester, Fortinet, Check Point, Cloudflare , IC3, entre otras.

La búsqueda de información se realizó en torno a las siguientes palabras clave: modelos de seguridad, amenazas cibernéticas, marcos de seguridad, nuevas tendencias en seguridad informática, protección de datos, de red, de aplicaciones, de correo electrónico, de dispositivos y equipos, de servicios en la nube, de procesos y de usuarios; de nuevos riesgos sobre los datos, de control de riesgos, de inteligencia de seguridad, de gestión de identidad distribuida y aspectos referentes a las principales herramientas usadas para la detección, contención y respuesta a incidentes de seguridad.

Mallas de ciberseguridad

El complejo ecosistema de la ciberseguridad demanda de modelos, de arquitecturas, de herramientas y de profesionales que posean conocimientos especializado no solo en el área de la seguridad, sino en todo el entorno de TI (Tecnologías de la Información) y de TO (Tecnologías de la Operación), que conozcan manejen y apliquen las tecnologías de punta y que posea conocimientos en inteligencia artificial, en sus algoritmos y sus aplicaciones.

Fundamentación teórica

¿Qué es una malla de ciberseguridad?

Gartner define una malla de ciberseguridad como *"un enfoque conceptual moderno de la arquitectura de seguridad, que permite a la empresa protegida desplegar y extender dicha seguridad a donde más se necesite". Y es un ecosistema colaborativo de herramientas y controles para proteger una empresa moderna y distribuida. 12*

La arquitectura de malla de ciberseguridad (cybersecurity mesh architecture, CSMA) promueve la interoperabilidad y coordinación de productos de seguridad individuales, lo que da por resultado una política de seguridad más integrada. Esto refuerza la seguridad de la organización al proteger puntos finales individuales, en lugar de intentar proteger todos los activos con una sola tecnología. La CSMA está diseñada para ayudar a la organización a dejar atrás los sistemas autónomos obsoletos y adoptar una estrategia integrada.

La CSMA crea un medio para que los servicios de seguridad individuales se comuniquen e integren, generando así un entorno de seguridad más dinámico en la red.

La CSMA dinamiza la postura de seguridad de la organización. A medida que aumenta la digitalización, las soluciones de CSMA ofrecen una respuesta de seguridad más escalable y flexible.

La CSMA mejora su estrategia de defensa al facilitar la colaboración entre herramientas de seguridad analíticas e integradas. Esto fortalece en gran medida su respuesta a ataques y violaciones.

La CSMA crea un entorno en el que la tecnología de ciberseguridad se puede implementar rápidamente y mantener de manera cómoda. Reduce al mínimo la inversión en soluciones de seguridad específicas para situaciones de necesidad temporal, lo que libera activos, ya sean financieros, tecnológicos o relacionados con el personal, para operaciones más esenciales. 13

Capas de una malla de ciberseguridad

Adoptar una estrategia de malla de ciberseguridad tiene claras ventajas; específicamente, escalabilidad, compatibilidad e interoperabilidad. En su arquitectura se identifican cuatro capas que son: Análisis e inteligencia de seguridad, Tejido de identidad distribuida, Gestión

consolidada de políticas y posturas y Paneles consolidados. 13

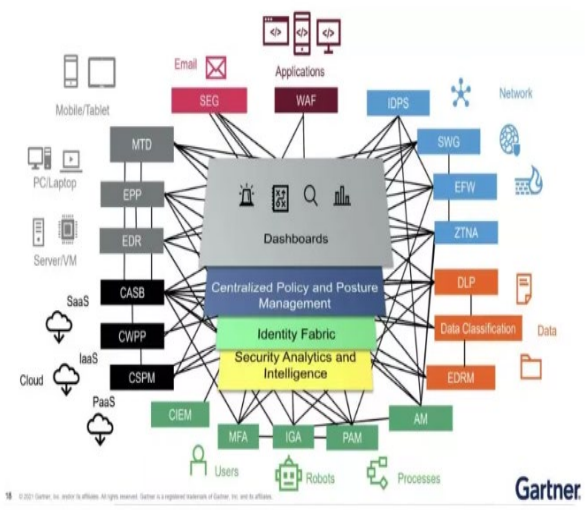
En el argot de la ciberseguridad es común hablar de normas, de estándares, de políticas, de planes, de estrategias, de marcos, de modelos de seguridad y de arquitecturas; en cada uno de estos ítems encontramos un variado número de propuestas que están enfocadas a solucionar dicha problemática desde diferentes perspectivas, teniendo en cuenta las necesidades de empresas de diversos sectores y con características particulares. En los apartes siguientes se presenta una somera descripción de algunos aspectos que son relevantes en la temática abordada.

Qué es una arquitectura en ciberseguridad

La arquitectura de seguridad informática garantiza que el diseño de red principal de una empresa, así como los datos más confidenciales y aplicaciones críticas, estén completamente protegidas contra cualquier amenaza o brecha de seguridad actual o futura.

Una de las estrategias para solventar la problemática, fue la presentada por Gartner, y consiste en una arquitectura de gestión en malla, cuyo nombre es CSMA, Cyber Security Mesh Architecture, ver figura No 2., la cual se describirá en el presente escrito, en donde se identifican su enfoque y su ecosistema de forma general.

Figura No 2. Arquitectura de seguridad en malla CSMA



Fuente: https://ciberseguridad.blog/que-es-cybersecurity-mesh-architecture-csma-y-por-que-es-el-futuro/

La figura anterior, muestra un bosquejo general de la infraestructura tecnológica usada actualmente y de las diferentes herramientas usadas en cada uno de los ambientes de la organización; en apartes posteriores se detallarán los aspectos más relevantes del modelo CSMA. Algunas de las capas que constituyen CSMA son:

Security Analytic and Intelligence: Asocia y crea un historial de los eventos de seguridad de la organización con el fin de prever amenazas y ataques.

Identity Fabric: Permite una gestión de identidades holístico en la organización, contemplando varios servicios de gestión de identidades multiplataforma. Permite el manejo integral de identidades.

Centralized Policy and Posture Management: potencia la capacidad de una organización para detectar, responder y solucionar las amenazas; contempla la capacitación del personal, las aplicaciones y la infraestructura tecnológica, el establecimiento de políticas y procesos en la organización.

Dashboards: Los tableros de datos son herramientas que muestran de forma simplificada y clara relaciones entre datos complejos provenientes de múltiples aplicaciones de diversos orígenes que se encuentran integradas bajo la malla.

Como se ve en la figura No. 1, CSMA contempla los diversos dispositivos y formas de acceso a los sistemas; como es el caso de los dispositivos móviles, de los equipos de escritorio y portátiles, de los servidores físicos y virtuales y de las distintas formas de servicios Cloud, como SaaS, IaaS y PaaS; se contempla igualmente los sistemas de correo electrónico y el aseguramiento en la web y las aplicaciones de la organización.

Se hace énfasis en los usuarios, en la infraestructura de red, en los datos, en los procesos y en las comunicaciones y se contemplan capas de identidad, de política, de postura y Dashboard como se mencionó anteriormente.

Una de las ventajas del modelo es el ahorro en términos económicos y el aumento en la resiliencia empresarial en los casos en que se presenten incidentes de seguridad. CSMA está estructurada de forma tal que representa ventajas respecto a otras herramientas y modelos utilizados como se describe a continuación.

Análisis e inteligencia de ciberseguridad. El uso de SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation and Response) no contemplan este aspecto, hecho que las CSMA han adoptado y que potencia la gestión y reduce costos en el área. La gestión centralizada permite recopilar, consolidar y analizar grandes volúmenes de datos en tiempo real desde una ubicación central; con lo que se optimiza el análisis de riesgos, se reduce el tiempo de respuesta a amenazas y los ataques se minimizan; con los datos y con el análisis realizado se optimiza el tratamiento y respuesta a incidentes.

Tejido de identidad distribuido. Busca proporcionar un acceso adaptable con una gestión de identidades no centralizada, ofrece servicios de

directorio, gestión de acceso y pruebas de identidad.

Gestión centralizada de políticas y posturas. El cumplimiento con la normatividad legal y la adecuada configuración de las diferentes herramientas permiten afinar los sistemas para facilitar su gestión de forma integral y aumentar la capacidad de la organización para detectar, responder y solucionar amenazas teniendo en cuenta la preparación del personal, el software y el hardware, las políticas y los procesos.

Dashboards consolidados. La visualización adecuada del ecosistema de seguridad permite la detección de eventos y el despliegue de respuestas adecuadas a cada incidente de seguridad.14. Tener la posibilidad de contar con herramientas de visualización de datos que se nutran de múltimples fuentes y herrramientas permite identificar y entender mas facilmente la problemática de forma general y global, aspecto que contribuye con la realización de una gestion más ágil y oportuna.

Descripción de aplicaciones de seguridad integradas en CSMA

A continuación se detallan aspectos de algunas de estas aplicaciones, que surgen como resultado a los nuevos hábitos de uso y modelos de trabajo. Una malla de seguridad integra varias soluciones y las gestiona de acuerdo a las necesidades de una empresa dada. Algunas herramientas son:

SIEM: Security Information and Event Management. Es un software que permite visualizar de manera completa el monitoreo de las amenazas. Un SIEM combina la administración de información de seguridad (SIM) y la administración de eventos de seguridad (SEM) en un solo sistema de administración de seguridad. La tecnología SIEM recopila datos de registro de eventos de varias fuentes, identifica la actividad que se desvía de la norma con análisis en tiempo real y toma las medidas adecuadas [15].

CIEM: Cloud Infrastructure Entitlement Management (Administrar derechos de infraestructura en la nube.). Se encarga de la gestión de derechos de infraestructura en la nube y automatizan el proceso de gestión de derechos y privilegios de los usuarios en estos entornos. 16.

MFA: Multi-Factor Authentication. Agrega una capa de protección al proceso de inicio de sesión. Cuando se accede a una cuenta o aplicación, los usuarios deben pasar por una verificación de identidad adicional; por ejemplo, tienen que escanear su huella digital o especificar un código que reciben en su teléfono. 17

IGA: Identity Governance and Administration. Permite a los administradores de seguridad administrar de manera eficiente las identidades de los usuarios y el acceso en toda la empresa. 18

PAM: Privileged Access Management. Solución que protege cuentas, credenciales y operaciones que ofrecen un nivel de acceso elevado ("privilegiado") a las aplicaciones y sistemas del negocio, que pueden permitir funciones de seguridad y mantenimiento, cambios de configuración a nivel de toda una aplicación o sistema, o eludir los controles de seguridad establecidos, a través del acceso como super usuario. 19

AM: Access Management. Componente que permite establecer, hacer cumplir y administrar controles de acceso para identidades internas y externas en tiempo de ejecución, a través de funcionalidades tales como: servicios de directorio y sincronización de identidades, gestión de la autenticación con múltiples métodos, incluyendo MFA (Multi-Factor Authentication) y SSO (Single Sign-On - inicio de sesión unificado), autorización y acceso adaptativo, gestión de sesiones, integraciones BYOI (Bring Your Own Identity) para usar identidades públicas como las de las redes sociales para tener acceso, y capacidades de analítica, reportes y auditoría de eventos de acceso en tiempo de ejecución. 20

PKI/SECRETS/HSM/KSM
PKI: Public Key Infrastructure. Son un grupo de componentes y servicios informáticos que permiten gestionar, controlar y administrar la tarea de generar, brindar, revocar y validar toda clase de certificados digitales.

SECRET: Un "secreto" en este contexto se refiere a las claves de encriptación, claves API, claves SSH, tokens, contraseñas o certificados que permiten que partes dispares de la infraestructura de aplicaciones se conecten entre sí. 21
HSM: Hardware Security Module. Genera y protege las claves y realiza funciones criptográficas dentro de un entorno seguro. 22.
KSM: Key Management Service. La gestión de claves se refiere a la gestión de claves criptográficas en un criptosistema. Esto incluye ocuparse de la generación, el intercambio, el almacenamiento, el uso, la trituración criptográfica y el reemplazo de claves. 23

EDRM: Endpoint Detection and Response Management (Gestión de respuesta y detección de terminales). Es una tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas. 24

DATA Clasification: método para definir y categorizar los archivos y otra información empresarial clave. Se usa principalmente en grandes organizaciones para crear sistemas de seguridad que siguen estrictas normativas de cumplimiento, pero también se puede usar en entornos reducidos. 25

DLP: Data Loss Prevention. Una solución de prevención de pérdida de datos es un sistema que está diseñado para

detectar potenciales brechas de datos/ transmisiones de datos y prevenirlos a través de monitoreo, detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo. 26

ZTNA: Zero Trust Network Access o redes de confianza cero. es una solución avanzada de seguridad diseñada para minimizar la exposición a amenazas externas y asegurar que los recursos internos estén a salvo. 27

EFM: Enterprise Fraud Management. gestión de fraude empresarial. se basa en herramientas diseñadas para detectar el uso no autorizado. Para ello, se ejecutan diversos algoritmos y medidas de seguridad que pueden garantizar que solo los usuarios autorizados accedan al software y sus componentes cruciales. 28

SWG: Secure Web Gateway. Una puerta de enlace web segura, es una solución de seguridad que evita que el tráfico de Internet no seguro entre en la red interna de una organización. 29

IDPS: Intrusion Detection and Prevention System. Los sistemas de detección y prevención de intrusions, son componentes fundamentales de un marco sólido de ciberseguridad, ya que ofrecen capacidades críticas para detectar y prevenir actividades maliciosas en entornos de red. Un IDPS es un dispositivo de software o hardware que monitorea el tráfico de la red y le alerta sobre cualquier actividad sospechosa o maliciosa. 30

PACS: Picture Archiving Communication System. Es un sistema para archivo y comunicación de imágenes. 31

XDR: Extended Detection and Response. recopila y correlaciona automáticamente datos en múltiples capas de seguridad: email, endpoint, servidor, workload en la nube y la red. Esto permite una detección más rápida de las amenazas y una mejor investigación y tiempos de respuesta mediante un análisis de seguridad. 32

WAF: Web Application Firewall. Un firewall de aplicaciones web es un tipo de firewall que supervisa, filtra o bloquea el tráfico HTTP hacia y desde una aplicación web. Se diferencia de un firewall normal en que puede filtrar el contenido de aplicaciones web específicas, mientras que un firewall de red protege el tráfico entre los servidores. 33

SEG: Secure Email Gateway. Una puerta de enlace de correo electrónico seguro (SEG) es un producto de seguridad del correo electrónico que utiliza el análisis de firmas y el aprendizaje automático para identificar y bloquear los correos electrónicos maliciosos antes de que lleguen a las bandejas de entrada de los destinatarios. 34

SCRM: Cybersecurity Supply Chain Risk. La gestión de riesgos de la cadena de suministro es un proceso que las empresas utilizan para gestionar el riesgo de la cadena de suministro. 35

MTD: Mobile Threat Defense. es la protección de los dispositivos móviles. El MTD monitorea en tiempo real las aplicaciones y los dispositivos en busca de comportamientos sospechosos. 36

EPP: Endpoint Protection Platform. Son sistemas de seguridad unificada tradicionales, en los que se incluyen antivirus, antispyware, firewalls y demás soluciones de protección de los endpoints. 37

EDR: Endpoint Detection and Response. La detección y respuesta de puntos finales, también conocida como detección y respuesta de amenazas de puntos finales, es una tecnología de ciberseguridad que monitorea continuamente un "punto final" para mitigar amenazas cibernéticas maliciosas. 38

IOT/OT: IoT Operation Technology. La ciberseguridad en el Internet de las cosas (IoT) se refiere al conjunto de medidas y prácticas que tienen como objetivo proteger los dispositivos conectados a Internet y la red que los interconecta contra posibles ataques cibernéticos en sistemas IT y OT. 39

CASB: Cloud Access Security Broker. Un agente de seguridad de acceso a la nube es un software local o basado en la nube que se ubica entre los usuarios del servicio en la nube y las aplicaciones en la nube, y monitorea todas las actividades y hace cumplir las políticas de seguridad. Se encarga de: 1. Visibilidad · 2. Cumplimiento normativo · 3. Seguridad de los datos · 4. Protección contra amenazas. 40

CWPP: Cloud Workload Protection Platform. es una solución de seguridad en la nube que ayuda a proteger las cargas de trabajo en la nube en entornos híbridos y multi nube. 41

CSPM: Cloud Security Posture Management. (Gestión de la postura de seguridad en la nube). Engloba un conjunto de herramientas diseñadas para mejorar la seguridad de las configuraciones en los entornos en la nube y garantizar el cumplimiento normativo aplicable. Sus funciones son la integración, el monitoreo, la generación de alertas y la corrección. 42

NAC: Netwaork Accses Control. es el proceso de restringir el acceso de usuarios y dispositivos no autorizados a una red informática corporativa o privada. NAC garantiza que solo los usuarios autenticados y los dispositivos autorizados y que cumplan con las políticas de seguridad puedan ingresar a la red. 43

NGFW: Next Genration FireWall. es un servicio de firewall completamente distribuido con capacidades de protección avanzada, microsegmentación y cobertura generalizada para

proteger tus cargas de trabajo de Google Cloud de los ataques internos y externos. 44

vFW: Virtual Firewall. El firewall virtual controla el acceso a las subredes y admite reglas de permiso y denegación para los servicios al cliente. 45
IDS: (Intrusion Detection System) Un IDS es una tecnología de seguridad de red creada originalmente para detectar exploits de vulnerabilidades contra una aplicación o un terminal objetivo; también puede ser un dispositivo solo de escucha que analiza el tráfico de red y genera las alarmas respectivas. 46

UEM: (Unified Endpoint Management). Gestión Unificada de Terminales. UEM, o gestión unificada de puntos finales, es un software que permite a los equipos de TI y seguridad monitorear, administrar y proteger todos los dispositivos de los usuarios finales de una organización, como computadoras de escritorio y portátiles, teléfonos inteligentes, tabletas, dispositivos portátiles y más, de manera consistente con una sola herramienta, independientemente del sistema operativo o la ubicación. 47

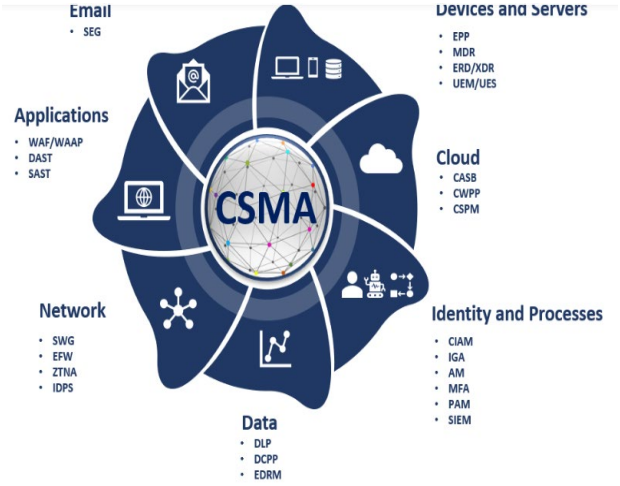
UES (Unified Endpoint Security). Seguridad Unificada de Terminales. Es un enfoque evolutivo hacia la seguridad de puntos finales centrado en la convergencia de múltiples capacidades de seguridad de puntos finales en una única plataforma integrada. 48
EASM: (External Attack Surface Management). Gestión de la superficie de ataque externa. es el proceso de descubrir, supervisar, evaluar, priorizar y remediar continuamente los posibles puntos de entrada en la infraestructura de TI de una organización que podrían ser susceptibles de un ataque. 49

De lo anterior, se puede identificar que existe una gran variedad de aplicaciones enfocadas a solucionar problemas particulares de seguridad; sin embargo, este esquema se vuelve cada vez más complejo y difícil de gestionar; como respuesta, se plantean modelos integradores que faciliten gestionar de forma centralizada, con un control de acceso más adaptable y granular que integren las herramientas que sean necesarias en un ambiente particular, en donde la ubicuidad y la diversidad de equipos y servicios sean el factor predominante.

Desde otra óptica, además del aumento de incidentes se dio un gran desarrollo de la inteligencia artificial, hecho que fue aprovechado por los ciber delincuentes para ser más agiles en acometer los delitos. El panorama planteado, creó el ambiente propicio para que nuevos modelos y arquitecturas de seguridad se implementaran, como es el caso de las mallas de ciberseguridad. Las SCMA integradas con otras herramientas o modelos como ZTNA, la microsegmentación, los microservicios, la virtualización, el uso de redes definidas por software hacen posible integrar la gestión de los recursos, procesos, equipos y usuarios de una forma más ágil; la cual, gracias a sus características permiten su implementación en los escenarios actuales de interacción.

En la Figura No. 3. se muestra el esquema de malla CSMA en donde se puede identificar algunas herramientas y procesos que facilitan la gestión de la seguridad de una forma integral.

Figura No. 3. Integración de aplicaciones de SCMA



Fuente: https://masqueseguridad.info/masqueseguridad/la-red-de-seguridad-cibernetica-por-que-csma-es-el-futuro-de-la-proteccion-digital/

Algunos de los beneficios clave de CSMA incluyen:

Visibilidad de seguridad integrada: CSMA crea una arquitectura de seguridad consolidada en la que todas las soluciones puntuales trabajan juntas. La visibilidad de seguridad mejorada que esto proporciona permite una detección y respuesta a amenazas más efectivas.
Diseño de seguridad inteligente: CSMA define las capas fundamentales y un método para diseñar una arquitectura de seguridad. Esto ayuda a una organización a diseñar una arquitectura de seguridad que proporcionará una protección integral contra las amenazas cibernéticas.
Gestión simplificada: CSMA integra las soluciones de seguridad puntual de una organización en una única arquitectura. Esto hace que sea más fácil para una organización monitorear y administrar su arquitectura de seguridad.
Arquitectura de seguridad flexible: CSMA crea una arquitectura de seguridad con componentes modulares conectados a través de capas fundamentales. Esta arquitectura modularizada facilita a una organización agregar o escalar componentes de seguridad según sea necesario.
Colaboración mejorada: CSMA crea un marco para que las soluciones puntuales de una organización se comuniquen y trabajen juntas. Esto ayuda a una organización a detectar y responder de forma más rápida y eficaz a las amenazas de seguridad.
Aumento de la eficiencia: CSMA reduce el número de paneles y soluciones que los analistas de seguridad necesitan administrar. Al eliminar el cambio de contexto y las tareas

de gestión innecesarias, CSMA mejora la eficiencia del SOC corporativo [50].

Aplicación de Inteligencia Artificial (IA) en ciberseguridad y CSMA

Desde que se propuso el modelo Transformer en 2017, la popularización y uso masivo de aplicaciones inteligentes dejó en evidencia muchas vulnerabilidades en temas relacionado con la gestión de la seguridad de la información; en este aparte se pretende hacer una breve descripción de algunas estrategias y herramientas que se sirven de esta tecnología para fortalecer el aseguramiento de los datos. 51

Casos de uso de seguridad de inteligencia artificial

A continuación, se describen algunos casos de uso de la IA, sus ventajas, su aplicación en algunas herramientas tradicionales usada en seguridad y las áreas de aplicación en dos mundos cada vez más convergentes y cercanos, el IT y el OT; cercanía que fue suscitada por el uso de IIoT (Internet Industria de las Cosas).
Administración de identidades y acceso: identifica patrones en el comportamiento de inicio de sesión y se encarga de la autenticación de usuarios.
Seguridad y administración de puntos de conexión: contribuye con la identificación de los puntos de conexión y la identificación de malware.
Seguridad en la nube: permite aumentar la visibilidad sobre los riesgos y vulnerabilidades en ambientes multinube.
Detección de ciberataques: La IA es utilizada en herramientas como CSMA, XDR y SIEM lo que facilita y agiliza la detección y respuesta a amenazas al responder automáticamente.
Protección de la información: contribuye con una gestión integral de la seguridad de los datos.
Investigación y respuesta a incidentes: la IA es de gran ayuda cuando los volúmenes de datos son enormes y hay la necesidad de identificar y correlacionar datos y responder en lenguaje natural.

Ventajas de usar IA en seguridad

Detecta ciber-amenazas críticas más rápido.
Simplifica la creación de informes.
Identifica vulnerabilidades.
Ayuda a los analistas a ampliar sus aptitudes.
Proporciona análisis e información de ciber-amenazas.

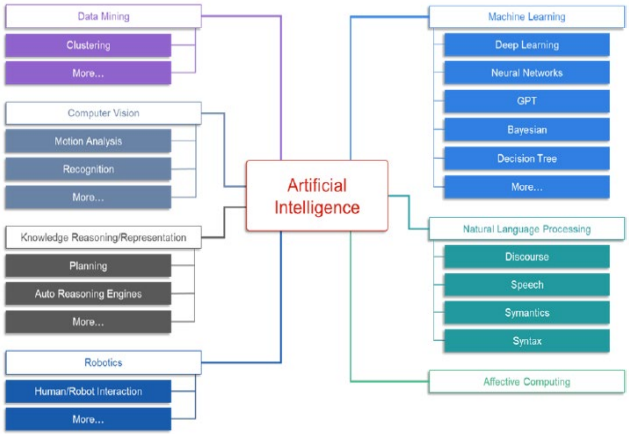
Herramientas con IA

Firewalls e inteligencia artificial de próxima generación: con IA pueden identificar nuevas amenazas
Soluciones de seguridad de puntos de conexión mejoradas para la inteligencia artificial.
Sistemas de prevención y detección de intrusiones de red controlados por inteligencia artificial.
Soluciones de seguridad en la nube e inteligencia artificial.
Protección de dispositivos Internet de las cosas (IoT) con inteligencia artificial.
CSMA, XDR y SIEM La inteligencia artificial ayuda a sintetizar todos los datos recolectados. 52

Áreas de aplicación de la inteligencia artificial

El aumento de los datos y el uso masivo de internet han generado un crecimiento en la superficie de ataque, que aumenta las posibilidades de ataque a los activos de las empresas que pueden estar de forma local o en la nube; esto sumado a la corta distancia que existe en la actualidad entre las Tecnologías de la Información IT y las Tecnologías de Operaciones OT y el uso masivo de dispositivos del internet de las cosas IoT; lo que hace que la labor de aseguramiento sea más dispendiosa y compleja. En la figura No. 4 se aprecia las áreas de aplicación de la inteligencia artificial con la cual se puede afrontar dicha problemática.

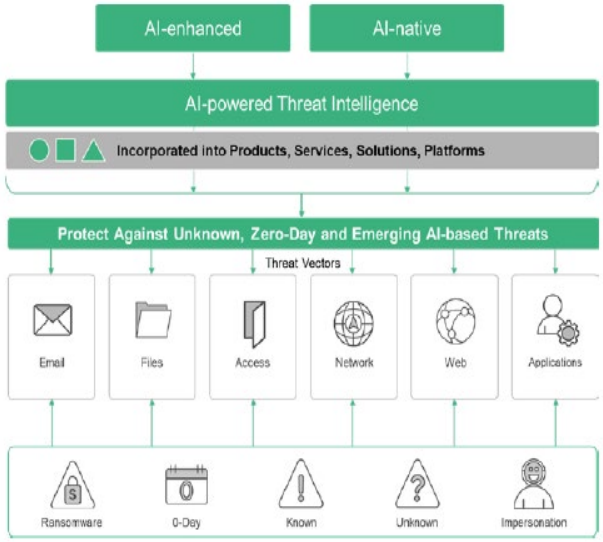
Figura No 4. Áreas de aplicación de la inteligencia artificial



Fuente: www.fortinet.com

El uso de la inteligencia artificial será un factor determinante en las operaciones de seguridad, se debe aprovechar las características de las aplicaciones de mayor trayectoria en la gestión de la seguridad para adoptar y actualizar dichas funcionalidades con la aplicación de estos algoritmos. En la figura No 5, se aprecia un diagrama con las funciones a aplicar frente a las amenazas de diferentes vectores de ataque sobre los activos que van desde el correo electrónico, los datos en reposos, el control de acceso, la infraestructura de red, el ambiente web y las aplicaciones. Es así como se puede aplicar la IA en Firewalls, en análisis de aplicaciones, en herramientas de detección y respuesta de endpoints (EDR), en las herramientas de administración de eventos e información de seguridad (SIEM), en el análisis de imágenes y en las pruebas de penetración, entre otras. 53

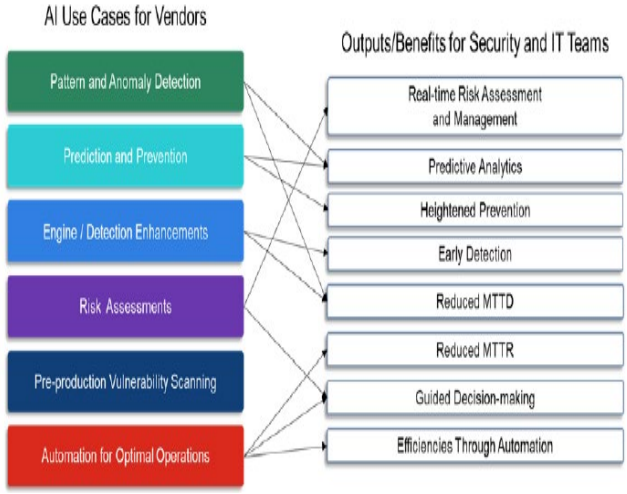
Figura No. 5. Funciones mejoradas con el uso de la inteligencia artificial



Fuente: www.fortinet.com/whitepaper

Se debe tener bien definido que están aplicando las soluciones de seguridad de inteligencia artificial y como esto beneficia las operaciones de seguridad y a la empresa; en la Figura No. 6 encontramos las formas en que los proveedores de aplicaciones de ciberseguridad pueden aplicar la IA en sus soluciones, en los procesos de soporte y sus diversos beneficios, esto es muy preponderante pues contribuye con establecer una buena *postura de seguridad* en la empresa. Algunos de los beneficios son la *evaluación y gestión de riesgos en tiempo real, el análisis predictivo, una mayor prevención, una detección temprana, la reducción del tiempo de detección y de respuesta y una toma de decisiones guiada*. 53

Figura No. 6. Beneficio de la aplicación de IA en seguridad



Fuente: www.fortinet.com/whitepaper

Usos de la IA por la delincuencia

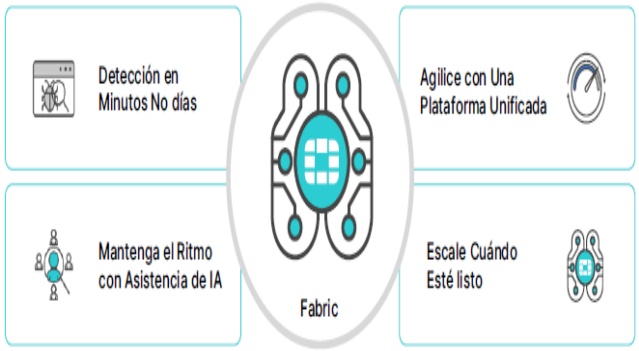
Es importante resaltar que la IA no de uso exclusivo de los encargados de los centros de seguridad y los centros de operaciones de la red, estas herramientas también son utilizadas por el adversario, lo que hace aún más estratégico su aplicación para contener los ataques de los delincuentes. Algunos usos son:

Crear amenazas de día cero.
Incrementan la agilidad en los ataques.
Usan los GPT Transformers Generativos Pre entrenados para suplantar identidades y hacer ingeniería social.
Generan código malicioso con IA y crean nuevo malware.
Usan tecnología de falsificación profunda que consiste en la suplantación de identidad, que se vale de una técnica avanzada de inteligencia artificial que recopila datos sobre movimientos físicos, rasgos faciales e incluso de voz, para procesarlos mediante un algoritmo codificador IA.
Se usa para detectar y aprovechar vulnerabilidades en la cadena de suministro.

Integración de lA en las operaciones de seguridad

La integración de la inteligencia artificial generativa (GenAI) en las operaciones de seguridad (SecOps) implica incorporar capacidades de Inteligencia Artificial (IA) en herramientas y flujos de trabajo de seguridad. Este aspecto puede facilitar la interacción del personal con los interfaces de las aplicaciones usadas. La IA debe admitir múltiples fuentes, incluidas herramientas de administración y análisis centrales como las mallas de seguridad CSMA, sistemas SIEM, plataformas de inteligencia frente a amenazas y soluciones de respuesta y automatización de orquestación de seguridad (SOAR). En la figura No. 7, se muestra un esquema de integración de la IA para aplicar en la gestión de la seguridad de la información en la empresa. 54

Figura No. 7. Integración de la IA en la respuesta a amenazas



Fuente: www.fortinet.com/whitepaper

Que tener en cuenta al aplicar IA en seguridad

Documentar casos de uso de IA Generativa (GenAI) en la empresa.
Comprender la administración de datos de IA.
Evaluar los riesgos externos de GenAI.
Crear una lista de herramientas GenAI aprobadas.
Desarrollar una política de GenAI.
Integrar la GenAI con la infraestructura existente.
Capacitar al personal de seguridad y GenAI.

Automatizar las tareas de rutina.
Mejorar la investigación y respuesta ante amenazas para utilizarlas en el análisis alertas e incidentes, generar resúmenes integrales de escalada y correlacionar de datos de múltiples fuentes
Optimizar las métricas de rendimiento para garantizar mayor agilidad.
Mantener la transparencia y la responsabilidad. 55 56 57

Conclusiones

La implementación de una CSMA permitirá realizar una gestión de la seguridad más simplificada, ágil e inteligente, se proveerá una solución flexible y escalable centrada en la identidad que permitirá integrar gran cantidad de aplicaciones y reducirá los costos asociados al área.

Es preponderante que las empresas y los equipos encargados de la seguridad adopten las herramientas que ofrece la inteligencia artificial con las cuales se reducirán los tiempos de detección y respuesta a amenazas y permitirá la integración con otras herramientas y modelos utilizados en el aseguramiento de los activos de información.

La gran cantidad de datos que se manejan en la actualidad sugieren la adopción de herramientas como la inteligencia artificial que permitan automatizar los procesos de identificación, detección y respuesta a comportamiento anómalos, a amenazas y ataques sofisticados que de forma tradicional requerirían de un mayor esfuerzo y de mayor tiempo de respuesta.

A cerca del autor:

Ingeniero de sistemas, con una maestría en teleinformática de la Universidad Distrital Francisco José de Caldas, con una trayectoria docente de 28 años, docente de la maestría en gestión y seguridad de la información, miembro del grupo de investigación en inteligencia artificial IAFT y la red CICOM. https://orcid.org/0009-0005-3946-8190. hfuquene@udistrital.edu.co

Referencias

[1] Estadísticas de ciberseguridad [Internet] 2022 [consultado en febrero de 2024] Disponible en: https://www.ic3.gov/
[2] Estadísticas de ciberseguridad [Internet] 2022 [consultado en marzo de 2024] Disponible en: https://www.fortinet.com/lat
[3] James Hoover, Pete Shoard, Felix Gaehtgens, “How to Start Building a Cybersecurity Mesh Architecture,” [Internet] 2022 [consultado en junio de 2024] Disponible en: www.Gartner.com.
[4] “2022 State of Security Posture Report," Cybersecurity Insiders, [Internet]2022[consultado en junio de 2024]. Disponible en: https://www.studocu.com/es/document/
[5] “2023 State of Security Posture Report," Cybersecurity Insiders, [Internet]2023[consultado en junio de 2024]. Disponible en: https://www.f5.com/resources/reports/
[6] Seguridad en la nube. [Internet] 2023[consultado en junio de 2024]. Disponible en: https://www.kaspersky.es/resource-center/definitions/what-is-cloud-security
[7] 2023 State of Security Posture Report, Cybersecurity Insiders. [Internet]2023 [consultado en junio de 2024]. Disponible en: https://www.f5.com/resources/reports/
[8] Sydney Lake, “The cybersecurity industry is short 3.4 million workers—that’s good news for cyber wages,” [Internet] 2023[consultado en junio de 2024]. Disponible en: https://fortune.com/
[9] Jon Oltisk, “SOC Modernization and the Role of XDR,” ESG,[Internet]2022[consultado en junio de 2024] Disponible en: www.cisco.com
[10] “2023 State of Security Posture Report," Cybersecurity Insiders, [Internet]2022[consultado en junio de 2024]. Disponible en: https://www.f5.com/resources/reports/
[11] Jon Oltisk, “SOC Modernization and the Role of XDR,” ESG,[Internet]2022[consultado en julio de 2024] Disponible en: www.cisco.com
[12] ¿Qué es una malla de ciberseguridad?,[Internet]2022[consultado en julio de 2024] Disponible en: https://www.gartner.com/
[13] Qué es CyberSecurity Mesh Architecture (CSMA) y por qué es el futuro. [Internet]2024[consultado en agosto de 2024] Disponible en: https://ciberseguridad.blog/que-es-cybersecurity-mesh-architecture-csma-y-por-que-es-el-futuro/
[14] ¿Qué es una Arquitectura de ciberseguridad? . [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-cyber-security-architecture/
[15] Qué es SIEM.[Internet]2023[consultado en agosto de 2024] Disponible en: https://www.microsoft.com/
[16] ¿Qué es la administración de derechos de infraestructura en la nube (CIEM)? .[Internet]2023[consultado en agosto de 2024]. Disponible en: https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-cloud-infrastructure-entitlement-management-ciem/
[17] Qué es: Autenticación multifactor. [Internet]2023[consultado en agosto de 2024] Disponible en: https://support.microsoft.com/es-es/topic/qu%C3%A9-es-autenticaci%C3%B3n-multifactor-e5e39437-121c-be60-d123-eda06bddf661
[18] What is IGA (Identity Governance & Administration)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.oneidentity.com/what-is-iga/
[19] ¿Qué es Privileged Access Management (PAM)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-privileged-access-management-pam
[20] AM (Access Management) [Internet]2023[consultado en agosto de 2024] Disponible en: https://cybersecurity.sek.io/blog/iga-am.

[21] ¿Qué es la gestión de secretos? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cloudflare.com/es-es/
[22] ¿Qué es un módulo de seguridad hardware (HSM)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.entrust.com/es/resources/learn/what-are-hardware-security-modules
[23] AWS Key Management Service [Internet]2023[consultado en agosto de 2024] Disponible en: https://docs.aws.amazon.com/es_es/kms/latest/developerguide/overview.html
[24] What Is Endpoint Detection and Response (EDR)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cisco.com/c/en/us/products/security/endpoint-security/what-is-endpoint-detection-response-edr-medr.html
[25] What is Data Classification?[Internet]2023[consultado en agosto de 2024] Disponible en: https://www.digitalguardian.com/blog/what-data-classification-data-classification-definition
[26] ¿Qué es DLP o prevención de pérdida de datos? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.proofpoint.com/es/threat-reference/dlp
[27] What is Zero Trust Network Access (ZTNA)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.skyhighsecurity.com/cybersecurity-defined/what-is-ztna.html
[28] Enterprise Fraud Management [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.gartner.com/en/information-technology/glossary/enterprise-fraud-management-efm
[29] ¿Qué es una puerta de enlace web segura (SWG)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cloudflare.com/es-es/learning/access-management/what-is-a-secure-web-gateway/
[30] Intrusion Detection and Prevention System [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.redhat.com/en/topics/security/what-is-an-IDPS
[31] What Is PACS (Picture Archiving and Communications System)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://builtin.com/articles/pacs
[32] What Is Extended Detection and Response (XDR)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-xdr.html
[33] ¿Qué es un cortafuegos de aplicaciones web (WAF)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.f5.com/es_es/glossary/web-application-firewall-waf
[34] What Is a Secure Email Gateway (SEG)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-email-security/what-is-a-secure-email-gateway-seg/
[35] Cyber Supply Chain Risk Management (C-SCRM) [Internet]2023[consultado en agosto de 2024] Disponible en: https://csrc.nist.rip/scrm/#:~:text=Cyber%20supply%20chain%20risks%20may,in%20the%20cyber%20supply%20chain.
[36] ¿Qué es la defensa contra amenazas móviles (MTD)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-mobile-threat-defense-mtd/
[37] Endpoint Protection Platform [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.vmware.com/topics/endpoint-protection-platform
[38] What Is Endpoint Detection and Response? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.trellix.com/security-awareness/endpoint/what-is-endpoint-detection-and-response/
[39] Why You Should Care about IoT and OT [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.ontinue.com/resource/why-you-should-care-about-iot-and-ot/
[40] ¿Qué es un CASB? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.netskope.com/es/security-defined/what-is-casb
[41] What is a CWPP? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.microsoft.com/en-us/security/business/security-101/what-is-cwpp
[42] CSPM: qué es el Cloud Security Posture Management [Internet]2023[consultado en agosto de 2024] Disponible en: https://s2grupo.es/cspm-que-es-el-cloud-security-posture-management/
[43] What Is Network Access Control? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html
[44] ¿Qué es un firewall de nueva generación (NGFW)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.cloudflare.com/es-es/learning/security/what-is-next-generation-firewall-ngfw/
[45] ¿Qué es un firewall virtual? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.paloaltonetworks.lat/cyberpedia/what-is-a-virtual-firewall
[46 ¿Qué es un sistema de detección de intrusiones? [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.paloaltonetworks.lat/cyberpedia/what-is-an-intrusion-detection-system-ids
[47] Unified Endpoint Management [Internet]2023[consultado en agosto de 2024] Disponible en: https://www.manageengine.com/latam/desktop-central/gestion-unificada-de-endpoints-uem.html
[48] What Is Unified Endpoint Security (UES)? [Internet]2023[consultado en agosto de 2024] Disponible en: https://expertinsights.com/insights/what-is-unified-endpoint-security/
[49] Administración de superficie expuesta a ataques externos [Internet]2023[consultado en agosto de 2024] Disponible en: https://learn.microsoft.com/es-es/azure/external-attack-surface-management/

[50] Malla de ciberseguridad vs confianza cero [Internet]2023[consultado en agosto de 2024] Disponible en: https://checkpoint.com/es/cyber-hub/cyber-security/what-is-cybersecurity-mesh-architecture-csma/cybersecurity-mesh-vs-zero-trust/

[51] Fúquene H. Procesamiento de Lenguaje Natural, los Transformer y los Bots Conversacionales: algunas generalidades. [Internet]2023[consultado en agosto de 2024] Disponible en: https://repository.uaeh.edu.mx/revistas/index.php/xikua/article/view/12904.

[52] ¿Qué es la IA para la ciberseguridad? [Internet]2024[consultado en agosto de 2024] Disponible en: https://www.microsoft.com/es-co/security/business/security-101/what-is-ai-for-cybersecurity

[53] Utilice la Inteligencia Artificial para combatir las Ciberamenazas. Empodere a los defensores y desarme a los intrusos. [Internet]2024[consultado en agosto de 2024] Disponible en: www. Fortinet.com.

[54] IA Generativa en Operaciones de Seguridad. Incorporación de Inteligencia Artificial en Herramientas y Flujos de Trabajo de Seguridad. [Internet]2024[consultado en agosto de 2024] Disponible en: En www.fortinet.com.

[55] LLM Agents can Autonomously Hack Websites [Internet]2024[consultado en agosto de 2024] Disponible en: https://arxiv.org/html/2402.06664v1

[56] Navigate threats to AI systems through real-world insights [Internet]2024[consultado en agosto de 2024] Disponible en: https://atlas.mitre.org/

[57] Consejos para implementar GenAI en las operaciones de seguridad. [Internet]2024[consultado en agosto de 2024] Disponible en: www.fortinet.com.