




UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
UNIDAD DE EPS
Prácticas Intermedias
Carrera: Ingeniería en Ciencias y Sistemas

Malla de Ciberseguridad		
Nombre:	Asunción Mariana Sic Sor	
Correo electrónico:	sicmariana8@gmail.com	
Tipo artículo:	Investigación	
Fecha:	24 de Marzo 2021	
Nombre/Firma de autorización de artículo por el Autor:		

Resumen

La crisis del coronavirus ha demostrado que toca tomarse muy en serio las amenazas digitales. Los ataques de ransomware han arrasado negocios enteros y puesto en jaque a todo tipo de empresas, como Garmin y Adeslas. Pero no basta con simples cortafuegos u otro tipo de tecnologías destinadas a proteger la información más sensible.

Palabras claves:

Seguridad Informática, Malla de Ciberseguridad, Tendencia, Tecnología Emergente 2021.

Introducción:

La pandemia ha acelerado la transformación de la sociedad y la economía. Diferentes expertos valoran si el mundo caminará por la misma senda o aparecerán nuevas realidades y herramientas.



Artículo:

El aumento de los ciberataques, la evolución digital de la fuerza laboral, la mayor importancia de la nube y una mayor cooperación entre los proveedores, serán algunas de las realidades que marcarán tendencia en ciberseguridad para el próximo año.

Esta tendencia la describen en Gartner como malla de seguridad. En su opinión, se trata de aumentar el perímetro de seguridad que protege a la organización. Más que una herramienta en particular, su previsión es más metodológica. Apuestan por una expansión de la ciberseguridad más allá de lo que sería el corazón de la empresa. “Muchos activos existen ahora fuera del perímetro de seguridad tradicional. La malla de ciberseguridad esencialmente permite que el perímetro se define alrededor de la identidad de una persona o cosa. La malla de ciberseguridad es un enfoque arquitectónico distribuido para un control de ciberseguridad escalable, flexible y de confianza”.

Algunas predicciones para el año 2021 son las siguientes, según el portal cybersecuritynews.es:

- Aumento de la actividad interna maliciosa
- La inteligencia artificial y el aprendizaje automático en el punto de mira
- El teletrabajo, la nueva normalidad
- Convergencia Zero-Trust y SASE
- Los beneficios de transformar la red y la seguridad
- Mayor cooperación entre los equipos de red y de seguridad
- Incremento de las regulaciones de privacidad
- Los controles de gobierno de datos se trasladarán a la nube
- GAIA-X ganará fuerza y apoyo
- Mayor colaboración entre los proveedores de seguridad

En definitiva, la unión de fuerzas será lo más relevante para la ciberseguridad el próximo año. Existirá una nueva relación de confianza que favorecerá una colaboración conjunta.

Compartirán conocimientos sobre las amenazas e intercambio de inteligencia, lo que favorecerá a la industria de la ciberseguridad.

La privacidad de la información es algo relevante y se debe trabajar en ello, así es como los expertos proponen que para mejorar ese punto se deben cumplir tres formas:

- Proporcionar un entorno confiable en el que los datos puedan procesarse o analizarse a través de entornos de ejecución de terceros y confiables en el hardware.



- Proporcionar un procesamiento y análisis descentralizados a través del aprendizaje automático federado o consciente de la privacidad.
- Computación que transforme datos y algoritmos antes del procesamiento o análisis, incluida la prueba de conocimiento cero, la computación segura de varias partes y el cifrado homomórfico (utiliza técnicas criptográficas para permitir que terceros procesen datos cifrados y devuelvan un resultado cifrado al propietario de los datos)

Conclusiones:

La ciberseguridad es muy amplia y si se aplica a cabalidad es una herramienta muy eficaz para prevenir, atacar y solucionar amenazas y ciberataques.

El tema principal está en la concienciación a nivel de usuarios y de empresas sobre la seguridad de la información, sobre la privacidad y sobre el acceso restringido a la información.

La confianza en este caso no va de la mano de la ciberseguridad, por el contrario, mientras más desconfiados seamos mejor protegeremos nuestra información.

Debemos tener el hábito de actualizar nuestro sistema informático continuamente, de no abrir correos sospechosos, de no entregar información privada y de no compartir en redes sociales nuestra información personal.

Nunca está demás recordar todas estas recomendaciones, por el bien de todos.

Referencias:

- (1) García, J. (2020). Más nube, mallas de seguridad y algoritmos éticos: tendencias para el año I de la inmersión digital. Marzo 27, 2021, de El País Sitio web: <https://elpais.com/tecnologia/2020-12-30/despues-de-un-ano-tan-digital-cuales-s-eran-las-tendencias-tecnologicas-en-2021.html>
- (2) Iniseg. (2020). Predicciones 2021 en ciberseguridad. Marzo 27, 2021, de Ciberseguridad al día Sitio web: <https://www.iniseg.es/blog/ciberseguridad/predicciones-2021-en-ciberseguridad/>