Modelo Diamond
Diferenciar entre el modelo de diamante y el proceso de la cadena Cyber Kill.

Orlando Rodríguez
Jean Carlos Inguíl
Carlos Vásconez

I. INTRODUCCIÓN

En el entorno de tecnología es fundamental comprender y aplicar modelos y metodologías que permitan abordar eficazmente tanto los desafíos económicos como las amenazas cibernéticas. Dos de las herramientas conceptuales más relevantes en este campo son el modelo Diamond y el proceso de la cadena Cyber Kill. Estos enfoques ofrecen perspectivas únicas para entender y enfrentar aspectos clave de la competitividad económica y la seguridad cibernética., es esencial familiarizarse con estos modelos y comprender cómo se pueden aplicar en el mundo real para mejorar la competitividad de las empresas y proteger los sistemas de información contra ataques cibernéticos. En este artículo, exploraremos en detalle el modelo Diamond y el proceso de la cadena Cyber Kill, diferenciando entre ellos y destacando sus aplicaciones prácticas en el campo de las TIC.

El modelo Diamond, se centra en los factores concluyentes de la superioridad competitiva de las naciones y las industrias. Este enfoque proporciona un marco analítico para comprender cómo diversos factores, como la infraestructura, la demanda del mercado y la estrategia empresarial, interactúan para influir en la competitividad de una industria en particular. Por otro lado, el proceso de la cadena Cyber Kill es una metodología utilizada en la seguridad cibernética para identificar y contrarrestar ataques cibernéticos, desglosando el proceso de ataque en etapas específicas, desde la identificación del objetivo hasta el impacto en el sistema objetivo. A lo largo de este artículo, examinaremos en profundidad cada uno de estos modelos, resaltando sus diferencias y similitudes, así como su relevancia para los profesionales de las TIC. Al comprender y aplicar estos enfoques, los ingenieros en TIC pueden contribuir significativamente a mejorar la competitividad empresarial y proteger los activos de información crítica en un entorno cada vez más digital y conectado.

I. MODELO DIAMANTE

Es un marco que se utiliza en la ciberseguridad que analiza e interpreta las amenazas y riesgos. Brinda un planteamiento organizado para ver y analizar problemas informáticos facilitando que los técnicos entiendan como actúan los ciber atacantes [1]. Se base en cuatro elementos clave:

- **Adversario:** Es el sujeto o sujetos encargados de las intrusiones informáticas, aquí se obtiene información sobre el atacante como las tácticas, sus motivaciones y procesos, de igual manera su relación con otros grupos de ataque [1].
- **Infraestructura:** Hace referencia a los instrumentos tecnológicos que son usados por el atacante. Implica explorar las herramientas, redes y recursos empleados en la ejecución de actividades. Analizar estos elementos puede facilitar la identificación de patrones y permitir el seguimiento hasta la fuente de la intrusión [1].
- **Capacidad:** Hace referencia a procedimientos y tecnologías empleados por el contrincante, abarcando información sobre el malware, exploits y vulnerabilidades aprovechadas durante la intrusión. Adquirir un entendimiento sobre las disposiciones del adversario resulta fundamental en la detección de vulnerabilidades potenciales y considerar contramedidas adecuadas [1].
- **Víctima**: Se centra en la entidad o entidades impactadas por una intrusión. Abarca detalles relacionados con la organización, objetivo, sus activos y las consecuencias de la intrusión, como la exposición de datos, comprometer al sistema o pérdidas económicas.

Historia

El Modelo Diamante emergió como una solución estratégica frente a la creciente complejidad de las amenazas cibernéticas, respondiendo a la necesidad de un análisis de intrusiones más estructurado. Concebido por David Bianco en el año 2012, este modelo ha ganado una aceptación general en el ámbito de ciberseguridad, al ofrecer un marco comprensible y completo para el análisis y compartición de conocimientos sobre las amenazas en el ciberespacio. Con el transcurso del tiempo, ha experimentado un desarrollo impulsado por las aportaciones de varias entidades, transformándose en un instrumento primordial en la gestión de incidentes, la adquisición de inteligencia sobre amenazas y las actividades de ciberseguridad. Permite a los expertos tomar decisiones anticipadas y bien fundamentadas para resguardar las organizaciones [1].

Una característica destacada del Modelo Diamond es su capacidad para atribuir amenazas en el ámbito cibernético a individuos específicos se logra por medio de análisis de tácticas, infraestructura y capacidades. Esta asignación es crucial para alcanzar motivaciones y pautas, desempeñando un rol primordial en el intercambio de inteligencia relacionada con amenazas [1].

En situaciones prácticas, el Modelo Diamond demuestra su eficacia en escenarios del mundo real, como el examen de APT, ataques de ransomware y ciberespionaje de naciones. Facilita la identificación y mitigación de amenazas, así como la elaboración de planes personalizados de respuesta a incidentes. Es crucial destacar que el Modelo Diamond no permanece estático, sino que se ajusta continuamente para planear las tendencias emergentes en amenazas cibernéticas. Su desarrollo implica la integración de inteligencia artificial, mejoras en el análisis de infraestructura y una mayor eficacia en el intercambio de información sobre ataques. En un entorno de ciberseguridad en constante cambio, el Modelo Diamond se presenta como una herramienta fundamental para el análisis de intrusiones [1].

II. Aplicaciones del modelo Diamond

El Modelo Diamante ha demostrado su eficacia en una variedad de sectores, sirviendo como un marco estructurado y adaptable para fortalecer la seguridad de la información [2]. Algunos ejemplos notables de su aplicación efectiva abarcan:

Ejemplos Destacados de Aplicación Efectiva del Modelo Diamante:

1. **Gobierno:**

- Agencias gubernamentales: Implementaron el Modelo Diamante para salvaguardar información sensible y crítica.
- Formulación de medidas estrategicas de seguridad cibernética: El gobierno de los Estados Unidos utilizó con éxito el modelo en la creación de su Estrategia Nacional de Seguridad Cibernética.

2. **Cuidado de la salud:**

- Organizaciones de atención médica: Mejoraron la seguridad de los registros médicos mediante la aplicación del Modelo Diamante [2].
- Preservación de la privacidad de los pacientes: Utilizando el modelo como herramienta clave.

3. **Finanzas:**

- Instituciones financieras: Implementaron el Modelo Diamante para proteger la información financiera de sus clientes [2].
- Prevención de fraudes y delitos financieros: Utilizando el marco para fortalecer las defensas contra amenazas cibernéticas [2].

4. **Tecnología:**

- Empresas de tecnología: Salvaguardaron sus sistemas y datos contra ataques cibernéticos mediante la aplicación del Modelo Diamante.
- Desarrollo de software seguro: Ejemplos notables incluyen empresas líderes como Google y Microsoft.

5. **Otros Sectores:**

- Industria: Protegieron información confidencial y procesos industriales utilizando el Modelo Diamante.
- Transporte: Garantizaron la seguridad de sistemas de transporte e información de pasajeros aplicando este marco.
- Comercio electrónico: Utilizaron el Modelo Diamante para asegurar transacciones en línea y datos de clientes.

Ejemplos de Éxito:

Gobierno de los Estados Unidos: La implementación del Modelo Diamante contribuyó significativamente al desarrollo y ejecución exitosa de la Estrategia Nacional de Seguridad Cibernética.

Organizaciones de atención médica: Destacando casos como el Hospital Clínico de la Universidad de Chile, donde la aplicación del Modelo Diamante mejoró la seguridad de los registros médicos.

Instituciones financieras: Un ejemplo notable es el Banco BBVA, que logró proteger con éxito la información financiera de sus clientes mediante la implementación efectiva del Modelo Diamante.

Empresas de tecnología: Gigantes tecnológicos como Google y Microsoft utilizaron el Modelo Diamante para salvaguardar sus sistemas y datos, demostrando su eficacia en el sector tecnológico.

Estos ejemplos ilustran cómo el Modelo Diamante se ha convertido en un recurso valioso en diversos sectores, proporcionando un enfoque estructurado y adaptativo para abordar las complejidades de la seguridad cibernética con éxito.

Características principales de modelo diamond y cyber kill

- **Origen Evolución**

Modelo diamond: Desarrollado por David Bianco en 2012, evolucionando con contribuciones de la comunidad de ciberseguridad [3].

Cadena Cyber Kill: Conceptualizado para representar la cadena de eventos que conducen a un ciberataque.

- **Estructura y Enfoque**

Modelo diamond: Proporciona un marco integral y fácil de entender para el análisis de intrusiones. Se centra en la infraestructura, capacidad, víctima y adversario [3].

Cadena Cyber Kill: Secuencia lineal de pasos, desde la identificación del objetivo hasta la consecución de los objetivos del atacante [3].

- **Aplicaciones Principales**

Modelo diamond: Análisis de intrusiones, optimización de la respuesta a incidentes, inteligencia sobre amenazas y toma de decisiones fundamentadas [3].

Cadena Cyber Kill: Seguimiento y análisis de eventos desde la identificación del objetivo hasta la finalización del ataque [3].

- **Flexibilidad y Adaptabilidad**

Modelo diamond: Ha evolucionado con el tiempo, permitiendo contribuciones de diversas fuentes para su desarrollo continuo.

Cadena Cyber Kill: Puede ser modificado y ¿ajustado según las necesidades específicas de una organización o situación [3].

- **Colaboración y Comunicación**

Modelo diamond: Facilita la comunicación entre profesionales de ciberseguridad y estandariza la documentación de incidentes [3].

Cadena Cyber Kill: Fomenta la colaboración al proporcionar un marco común para la comprensión de eventos [3].

- **Enfoque en la Víctima**

Modelo diamond: Aborda el impacto en la organización objetivo, esto abarca filtraciones de datos, compromisos del sistema y pérdidas financieras.

Cadena Cyber Kill: Se enfoca en analizar a la víctima desde el inicio hasta la finalización del ataque.

- **Utilidad en la Prevención**

Modelo diamond: Contribuye a desarrollar contramedidas proactivas para fortalecer la postura de seguridad.

Cadena Cyber Kill: Ofrece información valiosa para diseñar estrategias de prevención y detección anticipada.

- **Adopción en la Comunidad**

Modelo diamond: Ha ganado una adopción generalizada en la comunidad de ciberseguridad.

Cadena Cyber Kill: Aunque es reconocido, puede variar en su aplicación y adopción dependiendo de las prácticas y políticas de seguridad de la organización.

III. DIFERENCIA ENTRE MODELO DIAMOND Y LA CADENA DE CYBER KILL

El modelo diamond es conocida también como modelo de amenazas de diamond es un marco conceptual adoptado en el ámbito de ciberseguridad esto para gestionar varias amenazas que se tiene hoy en día de manera integral este modelo se fundamenta en el concepto de que una amenaza cibernética puede ser representada y comprendida a través de cuatro elementos principales, que forman una estructura similar a un diamante [4]. Estos elementos son:

Actores: Los actores en el Modelo Diamond se refieren a las entidades o individuos que participan en actividades relacionadas con la ciberseguridad. Esto puede incluir hackers, ciberdelincuentes, grupos de hackers, actores estatales, empleados descontentos, entre otros. Identificar quiénes son los actores relevantes en el contexto de una organización o sistema es fundamental para comprender las posibles amenazas que pueden enfrentar [4].

Capacidades: Las capacidades se refieren a las destrezas y recursos que tienen los actores para llevar a cabo actividades maliciosas en el ámbito cibernético. Esto puede incluir conocimientos técnicos, acceso a herramientas de hacking, infraestructura de red, recursos financieros y cualquier otro elemento que les conceda llevar a cabo sus acciones de manera efectiva. Entender las capacidades de los actores ayuda a evaluar el nivel de amenaza que representan [4].

Infraestructura: La infraestructura en el Modelo Diamond se refiere a los sistemas, redes y recursos que son utilizados por los actores para llevar a cabo actividades maliciosas. Esto puede incluir servidores comprometidos, botnets, sitios web falsos, sistemas de comando y control, entre otros. Identificar y comprender la infraestructura utilizada por los actores es crucial para detectar y mitigar las amenazas cibernéticas [4].

Metas: Las metas representan los objetivos que los actores buscan alcanzar a través de sus actividades cibernéticas. Estos objetivos pueden variar ampliamente e incluir el robo de datos, el sabotaje de sistemas, la interrupción de servicios, el espionaje corporativo, entre otros. Comprender las metas de los actores ayuda a anticipar y mitigar posibles ataques cibernéticos.

En conjunto, estos cuatro elementos forman el "diamante" del Modelo Diamond, proporcionando una estructura integral para comprender y gestionar las amenazas cibernéticas. Al identificar y analizar a los actores, sus capacidades, la infraestructura que utilizan y sus metas, las organizaciones pueden desarrollar estrategias más efectivas para protegerse contra ataques cibernéticos y mitigar los riesgos asociados con la seguridad de la información.

El Modelo de Cadena de Ataque, también llamado Kill Chain, tiene un papel importante en la ciberseguridad al proporcionar una comprensión detallada del proceso que sigue un atacante durante un ciberataque. En lugar de considerar los ataques cibernéticos como eventos aislados, este enfoque se fundamenta en la idea de que los ciberataques siguen una secuencia de fases interrelacionadas. Estas etapas, que abarcan el reconocimiento, la entrega, la explotación, la instalación, el comando y control, y la acción, son fundamentales en el proceso general del ataque.
Cada fase del Modelo de Cadena de Ataque está planteada para que las empresas comprendan las formas empleadas por los atacantes en cada periodo. Al aprender estas fases, las instituciones pueden reforzar sus defensas, anticiparse y preparase para futuros ataques, y optimizar su capacidad para descubrir y responder a amenazas cibernéticas. Este enfoque sistemático es fundamental para ejecutar estrategias seguras de ciberseguridad y abordar los retos presentes en el panorama de amenazas.

Este modelo se desglosa en siete fases clave:

1. Reconocimiento: Durante este periodo, el intruso compila datos sobre el objetivo, como la información de sistemas, el análisis de información relacionada con empleados y la recopilación de datos relevantes [4].
2. Arma: En esta fase, el intruso obtiene o crea las herramientas y exploits útiles para empezar el ataque, ya sea buscando vulnerabilidades conocidas o creando malware personalizado [4].
3. Entrega: Aquí, el atacante facilita el canal para ejecutar el ataque en el objetivo, Incluyendo tácticas como el phishing a través de correos electrónicos o la explotación de fallos en servicios web.
4. Explotación: Durante esta etapa, el atacante busca aprovechar las vulnerabilidades en el sistema objetivo, ejecutando código malicioso o explotando debilidades de software o hardware.
5. Instalación: Después de obtener acceso al sistema, el atacante busca establecer una presencia persistente mediante la instalación de puertas traseras u otras medidas.
6. Comando y Control: En este punto, el intruso inicia una comunicación discreta con los sistemas comprometidos, lo que le posibilita retener el control y enviar instrucciones adicionales.
7. Acción: la fase final implica que el intruso realiza la acción conclusiva para alcanzar sus objetivos, Tales como la extracción de datos o la alteración intencionada de sistemas. Este enfoque holístico ayuda a las organizaciones a identificar posibles vulnerabilidades y desarrollar contramedidas proactivas en cada etapa del proceso de ataque, mejorando así su capacidad para prevenir, detectar y mitigar ciberataques y proteger sus activos y datos críticos.

IV. VENTAJAS Y DESAFÍOS DEL MODELO DIAMOND

Ventajas del Modelo Diamond:

- Comprensión Integral de las Amenazas Cibernéticas: El Modelo Diamond proporciona un marco holístico para comprender las amenazas cibernéticas al considerar no solo los actores involucrados, sino también sus capacidades, infraestructura y metas. Esto permite una comprensión más completa de los riesgos cibernéticos que enfrenta una organización.

- Priorización de Recursos y Respuestas: Al identificar y categorizar las amenazas cibernéticas según los elementos del modelo, las organizaciones pueden priorizar sus recursos y respuestas. Esto les permite enfocar sus esfuerzos en las áreas de mayor riesgo y potencial impacto.

- Adaptabilidad y Escalabilidad: El Modelo Diamond es lo suficientemente flexible como para adaptarse a diferentes contextos y escalas, lo que lo hace aplicable tanto a pequeñas empresas como a grandes corporaciones. Es adaptable para cumplir con los requisitos particulares de cada organización.

Desafíos del Modelo Diamond

- Complejidad en la Identificación de Amenazas: Identificar y categorizar adecuadamente las amenazas

cibernéticas según los elementos del Modelo Diamond puede ser un desafío debido a la complejidad y la evolución constante del panorama de amenazas. Requiere una comprensión profunda de las tácticas y técnicas utilizadas por los actores malintencionados.

- Dependencia de la Información de Inteligencia: Para utilizar eficazmente el Modelo Diamond, las organizaciones dependen en gran medida de la información de inteligencia cibernética actualizada y precisa. Esto puede ser un desafío, ya que la obtención de información de inteligencia puede ser costosa y requerir recursos significativos.

- Integración con Otros Marcos y Procesos de Ciberseguridad: Integrar el Modelo Diamond con otros marcos y procesos de ciberseguridad existentes puede ser complejo. Requiere una cuidadosa coordinación y sincronización para garantizar una gestión de riesgos coherente y eficaz en toda la organización.

- Para aprovechar al máximo el Modelo Diamond, las organizaciones deben comprometerse a implementarlo de manera integral en toda la empresa. Esto puede requerir cambios culturales, capacitación del personal y asignación de recursos adicionales.

V. Aplicaciones Prácticas del modelo Diamante en la inteligencia sobre amenazas

Las instituciones encuentran en el modelo Diamond una herramienta valiosa para el análisis y la compartición sistemática de inteligencia sobre amenazas. Al comprender las relaciones los elementos, las instituciones pueden reconocer patrones y tipos recurrentes de los actores de amenazas. Este método permite a las entidades protegerse proactivamente contra adversarios identificados y ajustar sus medidas de seguridad en consecuencia.

Incorporación del Modelo en los Planes de Respuesta a Incidentes:

El Modelo Diamante se integra de manera eficaz en los protocolos de respuesta a incidentes de las entidades. Los analistas lo emplean como un marco organizado para recopilar y registrar información durante un incidente. Esto simplifica la toma de decisiones informadas sobre los esfuerzos de contención, eliminación y recuperación, basándose en un entendimiento más completo de la dinámica de la intrusión.

Beneficios y Limitaciones de sus Aplicaciones Prácticas:

Beneficios: El modelo Diamond brinda un método organizado y holístico para la observación de intrusiones, optimizando la capacidad de las organizaciones para entender, responder y protegerse de ataques cibernéticas. Facilita el intercambio eficaz de inteligencia sobre amenazas y contribuye a decisiones informadas durante la respuesta a incidentes.

Limitaciones: Sin embargo, el modelo no es una opción segura. La atribución sigue siendo un obstáculo, y la evolución constante de los actores de ataques dificulta un rastreo puntual de la infraestructura y capacidades. También, su implementación puede solicitar una práctica considerable y recursos. Cabe destacar que no todas las intrusiones encajan de manera precisa en el modelo modelo, y algunos ataques pueden mostrar características distintas.

VI. Criticas y Perspectivas en evolución

Críticas y Limitaciones del Modelo Diamante:

1. Una crítica frecuente al Modelo Diamond es su excesivo énfasis en la atribución, lo cual puede resultar complicado y, en ocasiones, poco práctico. Determinar la identidad del responsable no siempre es el objetivo principal del análisis de intrusiones, y centrarse demasiado en este aspecto puede llevar a una visión limitada de la situación [5].

2. Algunos analistas sostienen que la simplicidad inherente al modelo puede simplificar en exceso la compleja realidad de las amenazas cibernéticas, volviéndolo menos adecuado para el análisis avanzado de amenazas o la comprensión de ataques altamente sofisticados y matizados [5].

3. La carencia de una orientación formal o pautas directas para la aplicación del modelo puede resultar en variaciones en la interpretación y aplicación del mismo [5].

VII. Ejemplos en el mundo real

Ejemplos en el mundo real
APT29

En el ámbito de la ciberseguridad, APT29, conocido como "Cozy Bear," ha emergido como un actor destacado, caracterizado por sus tácticas avanzadas y su vinculación con agencias de inteligencia rusas. Este artículo profundiza en la amenaza presentada por APT29, explorando sus actividades y características a través del modelo diamante [6].

Contexto de APT29: APT29, un grupo de amenazas avanzadas persistentes (APT), ha mantenido una presencia activa durante varios años, centrando sus actividades en ciber espionaje dirigido a gobiernos y sectores estratégicos[6].

Amenazas: La notoriedad de APT29 radica en su capacidad para llevar a cabo ciberataques sofisticados y operaciones de espionaje cibernético, apuntando a sistemas gubernamentales y desencadenando campañas de ciberataques a gran escala[6].

Capacidades: Este grupo exhibe destrezas técnicas avanzadas, haciendo uso de herramientas personalizadas como "CozyDuke" y "HammerToss." Estas habilidades les permiten operar de manera sigilosa y evadir detecciones [6].
Motivaciones: Las motivaciones de APT29 están vinculadas a objetivos geopolíticos e inteligencia, evidenciadas por su participación en eventos significativos como las elecciones presidenciales de EE. UU. en 2016 [6].
Oportunidades: APT29 capitaliza oportunidades para infiltrarse en sistemas, empleando tácticas de phishing altamente sofisticadas. La identificación de vulnerabilidades y puntos de entrada es esencial para defenderse contra este grupo.
Atribución y Vínculos con Rusia: Aunque la atribución en el ciberespacio presenta desafíos, diversas fuentes de inteligencia han señalado vínculos entre APT29 y agencias de inteligencia rusas, aportando una dimensión geopolítica a la amenaza.

Tendencias Futuras en el Análisis de Intrusiones

Las tendencias en el campo de ataques cibernéticas señalan el creciente empleo de inteligencia artificial y el aprendizaje automático por parte de los actores de amenazas. Este enfoque se traduce en la mejora de la sofisticación de los ataques, englobando varias técnicas y la explotación
automatizada y algo importante que es el phishing más efectivo.

Ataques a Cadena de Suministro

La creciente incidencia en ataques a la cadena de suministro destaca la vulnerabilidad de software y hardware, comprometiendo a numerosas organizaciones. Este panorama subraya la necesidad imperante del análisis integral sobre las amenazas y las evaluaciones de riesgos [7].

Vulnerabilidades de IOT y de la Infraestructura Crítica:

Con el impacto del Internet de las cosas (IoT), delincuentes de robo de información y Estados-nación aprovechan algunas vulnerabilidades de dispositivos conectados, priorizando objetivos como son redes eléctricas e instalaciones de tratamiento de agua. [7].

Desafíos de Seguridad en la Nube:

Los servicios en la nube presentan desafíos significativos en cuanto a seguridad. Los atacantes ajustan tácticas para ellos de una u otra manera vulnerabilidad varias cosas a su vez configuraciones erróneas en entornos de cloud [7].

Evolución del Ransomware:

Los ataques cada vez han ido evolucionando desde lo que llamamos el cifrado de datos hasta tácticas más complejas como el robo de datos y la extorsión. Se observa una tendencia hacia la doble extorsión, con amenazas de filtrar datos de total confidencialidad esto siempre y cuando si no se logra satisfacer el rescate.

Adaptaciones del Modelo Diamante a Nuevos Desafíos:

La evolución del modelo diamante incorpora IA y el aprendizaje automático dentro del análisis de las amenazas. Esta actualización facilita identificaciones de patrones y de alguna que otra anomalía en varios conjuntos grandes de datos, esto con el fin de ayudar a los analistas que se anticipen ante amenazas que puedan ocurrir y ajustar sus barreras de manera proactiva [7].

Ampliación del Análisis de Infraestructura:

Este modelo se actualiza para que pueda abordar ataques a la cadena de suministro, los analistas expanden su comprensión de la estructura para poder ingresar componentes y puntos de compromisos que puedas hacerse posible [7].

Análisis Centrado en la Nube:

El modelo diamante proporciona una visión más clara de las amenazas en cuanto en entornos de cloud. En el análisis de intrusiones moderno, resulta esencial tener un profundo entendimiento de la infraestructura y las capacidades particulares de los entornos en cloud [7].

Intercambio Mejorado de Inteligencia sobre Amenazas:

En un contexto de ataques sofisticados, se destaca la importancia del intercambio mejorado de inteligencia en amenazas en organizaciones y sectores. Este modelo se convierte en una herramienta importantes para la cual nos serviría para estructurar y estandarizar dicha inteligencia en posibles ataques, mejorando así la defensa.

Técnicas de Atribución Avanzadas:
La atribución siempre ha venido siendo un desafío, dicho modelo diamante incorpora técnicas de atribuciones mejores lo cual nos ayudaría a identificar varias características de los actores de amenazas incluso cuando estos se esfuerzan por mantenerse ocultos.

Conclusión:

En conclusión, el modelo Diamond y el proceso de la cadena Cyber Kill emergen como dos pilares fundamentales en el panorama de la ingeniería en Tecnologías de la Información (TIC). Mientras que el modelo Diamond nos brinda una visión holística de

factores que influyen en la competitividad económica a nivel nacional e industrial, el proceso de la cadena Cyber Kill nos sumerge en el intrincado mundo de la ciberseguridad, desglosando los ataques cibernéticos en etapas comprensibles.

Es crucial comprender y aplicar estos modelos y metodologías dentro y en un futuro en el campo profesional. Desde identificar oportunidades para mejorar la competitividad empresarial hasta implementar medidas efectivas para proteger los sistemas de información contra amenazas cibernéticas, el conocimiento de estas herramientas nos posiciona para hacer contribuciones significativas en un mundo digitalmente interconectado.

Para finalizar podemos decir que estos conceptos no solo enriquecen nuestra comprensión teórica, también nos equipa con las habilidades necesarias para poder combatir los desafíos y saber aprovechar oportunidades en un entorno tecnológico que bien sabemos esta siempre evolucionando cada día y asi seguir poder aprendiendo mas sobre la rama de la tecnologías que cada día crece más.

REFERENCIES

[1] Strayer, W. T., & Smith, R. S. "The Diamond Model of Intrusion Analysis." *Computers & Security*, vol. 28, no. 1-2, pp. 1-12, 2009.
[2] J. M. Quecano Clavijo and M. O. Caro Hernandez, "Guía Metodológica para la Creación y Gestión de CDUs SIEM MITRE ATT&C," 2023.
[3] T. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," in Security in Computing and Communications: Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015. Proceedings 3, pp. 438-452, 2015, Springer.
[4] M. J. Assante and R. M. Lee, "The industrial control system cyber kill chain," SANS Institute InfoSec Reading Room, vol. 1, pp. 24, 2015.
[5] C. Calle “The Diamond Model: A Useful Tool, but Not a Panacea” Sepember 9-115, 2015. Proceedings 3, Springer.
[6] V. T. Rivera and D. J. Salcedo, "¿Seguridad sin fronteras, seguridad en abstracto? Tendencias en el estudio de la ciberseguridad y la ciberdefensa," Revista Política y Estrategia, no. 138, pp. 141-164, 2021.
[7] D. López, O. Pastor, y LJ Garcia Villalba, "Concepto y Enfoques sobre el Análisis y la Gestión Dinámica del Riesgo en Sistemas de Información," en Actas de la XII Reunión Española de Criptología y Seguridad de la Información (