BLOCKCHAIN® IN HEALTHCARE TODAY

REVISIÓN NARRATIVA/SISTEMÁTICA/METAANÁLISIS

Tendencias emergentes en ciberseguridad: Una visión holística de las amenazas actuales, la evaluación de soluciones y el impulso de nuevas fronteras

Taskeen Zaid, PhD[1] y Suman Garai, MBA[(2*)]

[1]Profesor asociado de TI, Jain (Deemed to be University), Bengaluru, Karnataka, India; [2]Kalinga Institute of Industrial Technology, Bhubaneshwar, Odisha, India

*Autor correspondiente: Suman Garai, Correo electrónico: mr.sumangarai.3122@gmail.com DOI:

https://doi.org/10.30953/bhty.v7.302

Palabras clave: análisis comparativo, ciberdefensa, ciberseguridad, panorama de las amenazas digitales, marco innovador, salvaguardar la información

Resumen

En una era dominada por los avances digitales, la ciberseguridad desempeña un papel fundamental en la protección de la información y los sistemas frente a las amenazas en constante evolución. La creciente sofisticación de las ciberamenazas exige un examen crítico de la eficacia de las defensas actuales. Reconociendo las limitaciones y lagunas de las soluciones actuales, esta investigación introduce un marco pionero destinado a reforzar las ciberdefensas. Motivado por una exploración exhaustiva de artículos de investigación, encuestas, medios de comunicación en línea y estudios prácticos, este estudio escudriña las complejidades de las ciberamenazas y evalúa los puntos fuertes y débiles de las soluciones existentes. Los marcos propuestos surgen de un meticuloso estudio de viabilidad y viabilidad práctica, aprovechando las ideas recogidas de fuentes en línea di-versas. El "cómo" abarca un análisis comparativo, evaluando el nuevo marco frente a las soluciones establecidas para delinear sus respectivos méritos y deficiencias. El objetivo de esta investigación es ofrecer información valiosa a investigadores, profesionales y responsables políticos que se enfrentan a los múltiples retos de la ciberseguridad. Navegando a través de las complejidades de las soluciones existentes e introduciendo marcos innovadores, este documento pretende orientar los esfuerzos para reforzar las ciberdefensas. En última instancia, esta investigación prevé un ciclo continuo de mejora y evolución en el ámbito de la ciberseguridad a medida que las partes interesadas se esfuerzan colectivamente por adaptarse a un panorama de amenazas digitales en constante cambio.

Enviado: 24 de febrero de 2024; Aceptado: 19 de abril de 2024; Publicado: 30 de abril de 2024

En este artículo, los autores pretenden investigar exhaustivamente el panorama actual de las ciberamenazas, analizar las soluciones de seguridad existentes y proponer nuevos marcos de mejora. Los objetivos principales son examinar a fondo el panorama actual de las amenazas, analizar las amenazas a la seguridad, evaluar las soluciones existentes y señalar sus limitaciones inherentes. La investigación presenta dos soluciones innovadoras dirigidas a ámbitos específicos de la ciberseguridad y lleva a cabo análisis comparativos detallados con medidas de seguridad ya establecidas, dilucidando sus respectivos puntos fuertes y débiles. Las metodologías empleadas incluyen una amplia revisión bibliográfica, estudios de viabilidad y viabilidad práctica, y un análisis comparativo, estableciendo un una base sólida para generar ideas, mejoras prácticas e identificar futuras líneas de investigación.

Perspectiva histórica

En la ajetreada era digital, nuestras vidas se entrelazan a la perfección con los hilos invisibles de Internet. Hacemos operaciones bancarias en línea, compartimos pensamientos en las redes sociales y confiamos nuestros secretos al almacenamiento en la nube. Pero bajo esta comodidad se esconde un mundo de amenazas digitales, en el que los malintencionados tratan de explotar las vulnerabilidades y poner en peligro nuestros valiosos datos. Este ámbito, conocido como ciberseguridad, ha evolucionado desde los dominios de los espías y los descifradores de códigos hasta convertirse en un campo de batalla crítico para individuos, empresas y naciones por igual. Comprender su trayectoria -desde los primeros

de encriptación a los sofisticados entornos de ataque de hoy en día- es crucial para navegar por este terreno en constante cambio.

Las semillas de la ciberseguridad se sembraron en medio del caos de la Segunda Guerra Mundial. En un intento desesperado por proteger las comunicaciones militares, naciones como Alemania desplegaron avanzadas máquinas de cifrado como la Enigma, creando complejas claves que desconcertaron a los servicios de inteligencia aliados durante años. La historia del descifrado de Enigma, encabezado por un brillante equipo de Bletchley Park, es un testimonio del ingenio y la determinación que sustentan este campo. Incluso antes de que el mundo adoptara los ordenadores, la criptografía constituía la primera línea de defensa contra los adversarios que intentaban robar secretos y perturbar las operaciones[1].

Tras la revolución digital, la atención se desplazó de los códigos físicos a la protección de los sistemas informáticos y las redes. Los primeros tiempos se caracterizaron por incidentes aislados, como el ataque del gusano Morris en 1988, pero a medida que Internet crecía, también lo hacían la sofisticación y la frecuencia de las ciberamenazas. Los piratas informáticos, motivados por la maldad, el espionaje o el beneficio económico, explotaron las vulnerabilidades de los sistemas operativos, los sitios web y el comportamiento de los usuarios. Proliferaron los virus, gusanos y programas maliciosos contra infraestructuras críticas, empresas e incluso particulares. El auge de los sindicatos de ciberdelincuentes añadió una capa de malicia organizada, alimentando ataques como la violación de datos y el robo de identidades[2]

A medida que estos adversarios digitales evolucionaban, también lo hacía el arsenal de los defensores de la ciberseguridad. El software antivirus, los cortafuegos y los sistemas de detección de intrusiones se convirtieron en herramientas esenciales para la defensa de la red. Los gobiernos se apresuraron a crear agencias de ciberseguridad y a formular políticas. La cooperación internacional se hizo vital, dando lugar a tratados y acuerdos destinados a combatir la ciberdelincuencia y promover un comportamiento responsable en línea. Hoy, la ciberseguridad es una industria multimillonaria que emplea a un ejército de profesionales cualificados de diversos campos: hackers éticos, ingenieros de seguridad de redes, analistas de malware y especialistas en respuesta a incidentes[3].

Sin embargo, la carrera armamentística continúa. Los piratas informáticos innovan constantemente, explotando tecnologías emergentes como la inteligencia artificial (IA) y blockchain para lanzar nuevos ataques. El ransomware, las estafas de phishing y los ataques a la cadena de suministro son solo algunos ejemplos de la evolución del panorama de amenazas. Lo que está en juego es más importante que nunca: las infraestructuras críticas, los sistemas sanitarios e incluso los procesos democráticos son objetivos potenciales. A medida que nos precipitamos hacia un futuro cada vez más interconectado, la necesidad de medidas sólidas de ciberseguridad nunca ha sido mayor[4].

El viaje de la ciberseguridad es un testimonio del ingenio humano y de la lucha constante entre el ataque y la defensa. Desde el mundo clandestino del descifrado de códigos en tiempos de guerra hasta los complejos campos de batalla digitales de hoy, la historia pone de relieve la importancia de la concienciación, la vigilancia y la colaboración para salvaguardar nuestras vidas digitales. Mientras navegamos por un panorama cibernético en constante evolución, comprender su historia y los retos del presente nos capacita para construir un futuro más seguro y resistente para todos.

Riesgos para la seguridad digital en los últimos tiempos

La gravedad y la cantidad de las amenazas a la ciberseguridad han aumentado significativamente en los últimos años, lo que ha provocado pérdidas financieras de poca cuantía y ha dañado la reputación de muchas empresas. Lamentablemente, varios ejemplos de la vida real (Figura 1) demuestran la gravedad de estas amenazas.

Los ataques a la cadena de suministro, una sofisticada forma de guerra cibernética, implican comprometer a terceros proveedores para obtener acceso no autorizado a los sistemas de un objetivo. Este método permite a los atacantes explotar la confianza establecida entre

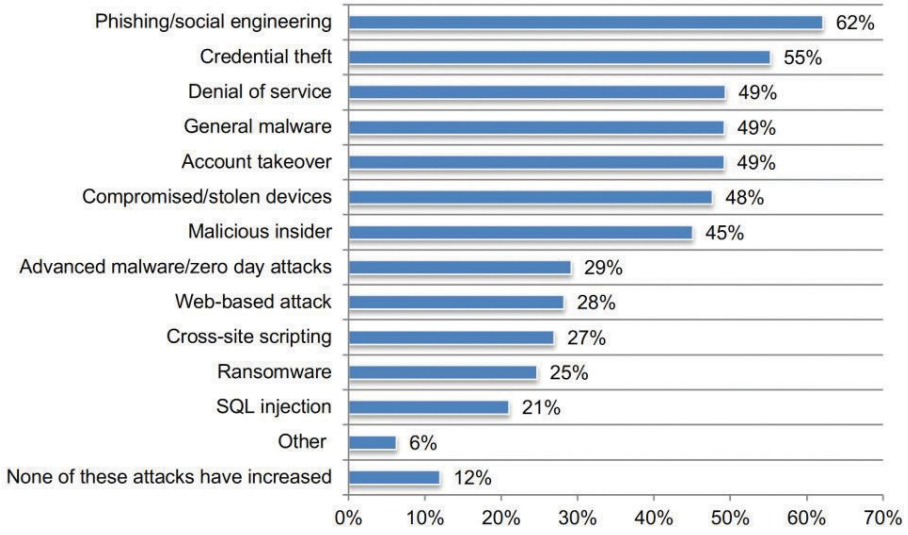

Fig. 1. Informe de una encuesta sobre el aumento de los distintos tipos de ciberamenazas desde COVID-19. SQL: lenguaje de consulta estructurado

Citación: Blockchain en la sanidad hoy 2024, 7: 302 - https://doi.org/10.30953/bhty.v7.302

organizaciones y sus proveedores. El ataque a SolarWinds en 2020 es un claro ejemplo de esta estrategia, en la que piratas informáticos rusos utilizaron vulnerabilidades en el proceso de actualización de SolarWinds para infiltrarse en las redes de miles de organizaciones.[5]

Explotar las vulnerabilidades de los dispositivos de Internet de las Cosas (IoT) es otra faceta de las ciberamenazas. El ataque de la red de bots Mirai de 2016 a Dyn es un ejemplo notable en el que se utilizaron dispositivos IoT compr-misos para lanzar un ataque masivo de denegación de servicio distribuido (DDoS), que abruma cualquier servidor o red con una avalancha de tráfico, causando importantes interrupciones de sitios web en todo el este de Estados Unidos y provocando daños estimados en 110 millones de dólares.[6]

Las amenazas persistentes avanzadas (APT) consisten en el acceso prolongado y no detectado a sistemas por parte de usuarios no autorizados. En 2015, piratas informáticos chinos ejecutaron una APT a gran escala contra la Oficina de Administración de Personal de Estados Unidos (OPM), comprometiendo los datos personales de más de 21 millones de personas[7]. Las APT se caracterizan por su naturaleza sigilosa, a menudo impulsadas por agentes de estados-nación con la intención de robar datos confidenciales o perpetrar otros ataques. La filtración de la OPM puso de manifiesto los importantes retos a los que se enfrentan las organizaciones a la hora de detectar y mitigar las APT.

Los ataques de ransomware cifran los datos de la víctima y exigen un pago por la clave de descifrado. El ataque WannaCry de 2017 afectó a más de 300.000 ordenadores en todo el mundo, aprovechando una vulnerabilidad de Microsoft Windows[8].Otro incidente notable fue el ataque Colonial Pipeline de 2021, en el que un ransomware interrumpió el suministro de combustible en el este de Estados Unidos, poniendo de relieve el papel fundamental que desempeña la ciberseguridad en la protección de infraestructuras esenciales[9]. La ingeniería social es una táctica empleada por los ciberdelincuentes para manipular a las personas para que revelen información sensible o realicen acciones que comprometan la seguridad. En 2023, MGM Resorts fue víctima de un sofisticado ataque de ingeniería social, en el que los piratas informáticos se hicieron pasar por un proveedor legítimo para acceder y robar guiones cinematográficos inéditos, documentos financieros confidenciales e información de los empleados(10). información de los empleados.[10]

Los deepfakes, vídeos o grabaciones de audio manipulados e hiperrealistas, añaden una capa de sofisticación tecnológica a la ingeniería social. Estas herramientas de "medios sintéticos" suponen una amenaza creciente, ya que permiten a los atacantes hacerse pasar por ejecutivos, difundir información errónea o llevar a cabo sofisticados planes de chantaje. Un estudio realizado en 2020 por la RAND Corporation advertía del uso potencial de los deepfakes para alterar las elecciones, manipular los mercados financieros y erosionar la confianza pública[11].El caso de deepfake de 2023 en el que se vio implicada la actriz Rashmika Mandanna muestra la amenaza en evolución que supone esta tecnología, causando angustia y daños reputacionales[12].

Las apropiaciones de cuentas van en aumento, afectando tanto a in-dividuos como a grandes organizaciones. En 2019, Capital One sufrió un importante ataque de apropiación de cuentas en el que un hacker obtuvo acceso a los datos personales de millones de usuarios. Las consecuencias fueron graves, ya que el hacker pudo acceder a números de la seguridad social, puntuaciones de crédito y números de cuentas bancarias, lo que condujo a una multa de 80 millones de dólares para Cap-ital One.[13]

El robo de credenciales es una táctica común utilizada por los atacantes para obtener acceso a información o sistemas sensibles. La violación de datos de Marriott International en 2018 expuso la información personal de aproximadamente 500 millones de huéspedes, ya que el hacker robó credenciales de inicio de sesión de un proveedor externo. En consecuencia, Marriott se enfrentó a una multa de 123 millones de dólares.[14]

Los insiders maliciosos, individuos con acceso autorizado a los sistemas de una organización, pueden representar una amenaza significativa cuando hacen un uso indebido de ese acceso. En 2019, un antiguo empleado de Tesla fue acusado de robar información confidencial y propiedad intelectual del sistema de la empresa. El empleado tenía acceso a los sistemas de la empresa y copió más de 300.000 archivos a su cuenta personal.[15]La filtración en 2023 de documentos clasificados del Pentágono a un grupo de chat de videojuegos subraya también la naturaleza insidiosa de las amenazas internas.[16]

El gusano Stuxnet es un ejemplo notable de ataque de día cero, en el que un atacante aprovecha una vulnerabilidad desconocida hasta entonces en el software[17].Su objetivo eran los sistemas de control industrial, aprovechando varias vulnerabilidades de día cero en Windows y en el software de Siemens para modificar los controladores lógicos programables y causar posibles daños físicos. Se cree que el ataque fue llevado a cabo por un Estado-nación y ha tenido importantes implicaciones para el desarrollo de armas cibernéticas y el uso de exploits de día cero en la guerra.

Estos ejemplos muestran las devastadoras consecuencias financieras y de reputación que pueden tener los ataques a la ciberseguridad. Las empresas pueden enfrentarse a sanciones legales, pérdida de clientes y daños significativos a la reputación de su marca. Además, la sociedad en su conjunto puede sufrir la pérdida de información sensible, la interrupción de infraestructuras críticas y un mayor riesgo de robo de identidad y fraude. A la luz de estos riesgos, las organizaciones deben tomarse en serio la ciberseguridad e invertir en medidas de seguridad sólidas para proteger sus sistemas y datos.

Medidas actuales de protección contra las ciberamenazas

En el dinámico ámbito de la ciberseguridad, es primordial adelantarse a las amenazas en constante evolución. Para lograrlo, las organizaciones deben aprovechar las soluciones más avanzadas. Esta explotación profundiza en seis avances clave, desentrañando sus funcionalidades, beneficios y aplicaciones en el mundo real.

Un avance fundamental es la integración de la IA y el aprendizaje automático (ML) como centinelas digitales (Tabla 1). Su destreza reside en el análisis en tiempo real de grandes flujos de datos, descifrando el tráfico de red, el comportamiento de los usuarios y los registros del sistema. Esto les permite aprender de las vulnerabilidades existentes y predecir futuros patrones de ataque. La IA y el ML actúan

Tabla 1. Opciones de uso del aprendizaje automático en el ámbito de la ciberseguridad[19]

Caso de uso	Descripción
Gestión de vulnerabilidades	Proporciona una priorización de vulnerabilidades recomendada basada en la criticidad para los equipos de TI y de seguridad.
Análisis estático de archivos	Permite la prevención de amenazas mediante la predicción de la malicia de un archivo basándose en sus características.
Análisis de comportamiento	Analiza el comportamiento de los adversarios en tiempo de ejecución para modelar y predecir patrones de ataque en toda la cadena cibernética.
Análisis híbrido estático y de comportamiento	Combina el análisis estático de archivos y el análisis de comportamiento para proporcionar una detección avanzada de amenazas.
Detección de anomalías	Identifica anomalías en los datos para informar sobre la puntuación de riesgos y dirigir las investigaciones de amenazas.
Análisis forense	Ejecuta contrainteligencias para analizar la progresión de los ataques e identificar las vulnerabilidades del sistema.
Análisis de malware en entornos aislados	Analiza muestras de código en entornos aislados y seguros para identificar y clasificar comportamientos maliciosos, así como relacionarlos con adversarios conocidos.

TI: tecnología de la información.

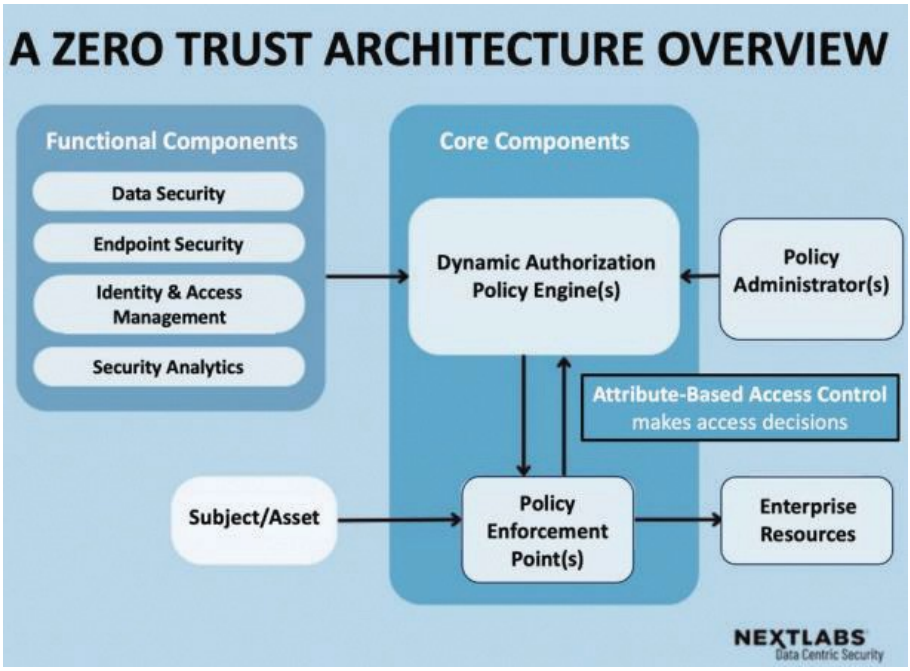

Fig. 2. Creación de una solución ZTA para empresas. ZTA: arquitectura de confianza cero.[21]

como sistemas de vigilancia sobrehumanos, que identifican en tiempo real anomalías sutiles en la actividad de la red, intentos inusuales de inicio de sesión y modificaciones sospechosas de archivos. Esto facilita la reducción de los tiempos de respuesta, permitiendo a las organizaciones prevenir las violaciones de datos mediante la detección temprana de las amenazas. Además, estas tecnologías destacan en la identificación de ataques de día cero, proporcionando una capa crucial de defensa contra nuevas amenazas. La belleza de la respuesta a incidentes impulsada por IA reside en su rápida actuación. Estos sistemas pueden aislar automáticamente los sistemas infectados, corregir vulnerabilidades e incluso recopilar pruebas y generar informes. Esto no sólo evita la propagación de amenazas, sino que también agiliza el proceso de análisis, proporcionando información valiosa para mejorar las defensas futuras.[18]

Los enfoques de seguridad tradicionales, parecidos a un "castillo y una cabaña", se están quedando obsoletos en el mundo interconectado de hoy. La arquitectura de confianza cero (ZTA) ofrece un cambio de para-digma a través de la micro-segmentación, el control de acceso, autenticación y autorización continuas. Entornos ZTA que dividen una red en minifortalezas, cada una de las cuales alberga datos o aplicaciones específicos. La implementación del acceso con menos privilegios impide el movimiento lateral no autorizado dentro de la red (Figura 2). La verificación dinámica de la confianza garantiza que ésta se verifique continuamente a lo largo de una sesión, adaptándose a la evolución del panorama de riesgos. ZTA emplea un sistema de seguridad multifactor con "esteroides". Más allá de las palabras clave, aprovecha factores como las huellas dactilares, los escáneres biométricos o los códigos de un solo uso para la verificación del usuario. La autenticación basada en el riesgo tiene en cuenta factores contextuales como la lo-cación del usuario y el tipo de dispositivo, ajustando los requisitos de autenticación en función del riesgo evaluado.[20]

Además de las criptomonedas, el libro mayor distribuido y a prueba de manipulaciones de blockchain ofrece ventajas únicas para la ciberseguridad, como la procedencia segura de los datos, la protección contra manipulaciones, la gestión segura de identidades y la descentralización.

Citación: Blockchain en la sanidad hoy 2024, 7: 302 - https://doi.org/10.30953/bhty.v7.302

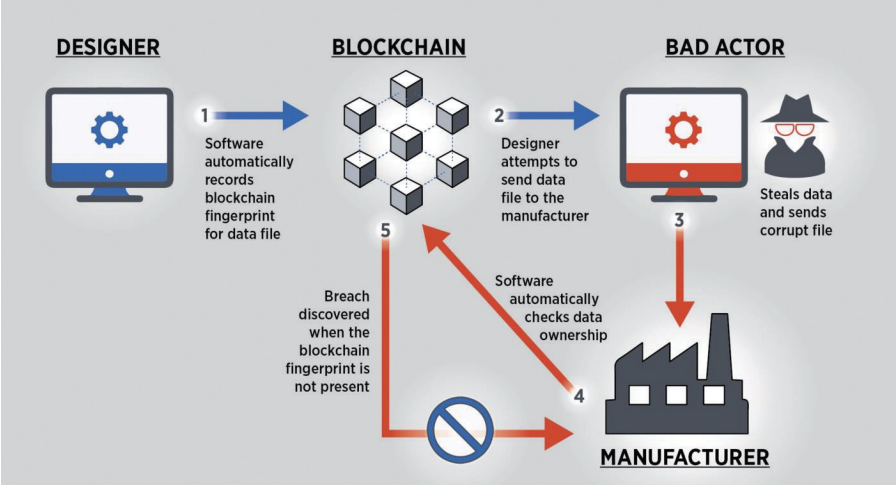

Fig. 3. Concepto generalizado de blockchain para la protección de activos[22].

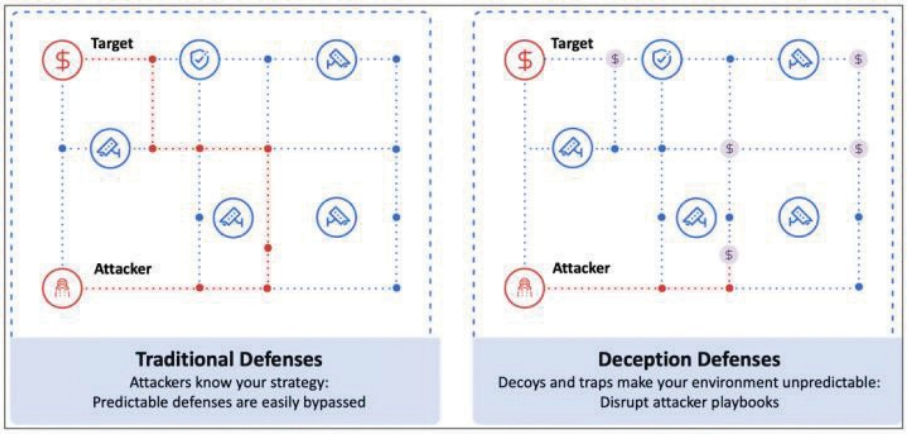

Fig. 4. Un ejemplo del concepto de engaño al estilo de Pac-Man[24]

identidad. Blockchain emplea hash criptográfico y un libro de contabilidad distribuido para asegurar los bloques de datos. Cada bloque se asegura con una huella digital única, lo que hace que cualquier alteración sea inmediatamente detectable. La naturaleza distribuida del libro de contabilidad a través de una red hace que la manipulación sea prácticamente imposible. Blockchain introduce la identidad descentralizada (DID) y las credenciales verificables (VC). La DID permite a los usuarios controlar sus datos de identidad, eliminando los puntos únicos de fallo. Las VC permiten a los usuarios emitir y compartir cre-denciales sin depender de intermediarios, reduciendo el riesgo de fraude (Figura 3).[23]

Las tecnologías de engaño crean una falsa realidad digital, utilizando trampas, honeypots, emulación de amenazas y simulación para engañar e inutilizar a los ciberdelincuentes. Las trampas y los honeypots actúan como señuelos y trampas digitales. Las trampas se asemejan a los sistemas reales, engañando a los atacantes para que pierdan el tiempo. Los honeypots capturan las tácticas y técnicas de los atacantes, proporcionando valiosa información a los equipos de seguridad. La emulación y simulación de amenazas reproducen vectores de ataque reales, lo que permite a las organizaciones poner a prueba sus defensas e identificar vulnerabilidades. Estas simulaciones revelan los puntos débiles de los controles de seguridad existentes, lo que ayuda a priorizar el parcheado de vulnerabilidades y a reforzar las defensas (Figura 4).[25]

Unos marcos jurídicos sólidos son fundamentales para la mitigación de riesgos y la rendición de cuentas. Estas medidas legales, junto con los avances tecnológicos, ofrecen una defensa integral contra los agentes maliciosos. El Reglamento General de Protección de Datos, la Ley de Intercambio de Información sobre Ciberseguridad (CCPA) y otras leyes regionales establecen normas de seguridad de los datos, elevando la ciberseguridad en todo el sector. La Protección de Infraestructuras Críticas impone controles de seguridad específicos para salvaguardar los sistemas vitales de las ciberamenazas. La CISA fomenta la colaboración público-privada y la respuesta rápida mediante el intercambio de información sobre amenazas[26]. Los acuerdos mundiales, como el Convenio de Budapest, fomentan los esfuerzos de colaboración contra la ciberdelincuencia. Leyes como la Computer Fraud and Abuse Act de Estados Unidos penalizan varios delitos relacionados con la ciberdelincuencia, sirviendo de disuasión legal contra la ciberdelincuencia.

actividad maliciosa. Reglamentos como la Ley de Ciberseguridad de la UE responsabilizan a las organizaciones de las violaciones de datos en determinadas circunstancias, incentivando prácticas de seguridad sólidas y promoviendo la responsabilidad[27]. Iniciativas como el Regulatory Sandbox del Reino Unido permiten probar tecnologías emergentes de ciberseguridad en entornos controlados, acelerando el desarrollo y fomentando la innovación en respuesta a las nuevas amenazas. La revisión y actualización periódicas de las leyes y marcos son cruciales para seguir el ritmo de la evolución del panorama de amenazas. Los diálogos abiertos entre los responsables políticos, los expertos en seguridad y las partes interesadas del sector garantizan que los marcos sigan siendo pertinentes.

La biometría del comportamiento añade una nueva dimensión a la seguridad al reconocer a los usuarios basándose en características únicas como la dinámica de pulsación de teclas, los movimientos del ratón y los hábitos de inicio de sesión. La biometría del comportamiento supervisa continuamente la actividad del usuario, incluida la dinámica de pulsación de teclas, los movimientos del ratón y los hábitos de inicio de sesión. Así se crea una guardia digital que vigila cada movimiento, mejorando la seguridad al reconocer las desviaciones de los perfiles de usuario establecidos. Esta forma de biometría ajusta las defensas en función del perfil de riesgo del usuario. Los escenarios de alto riesgo desencadenan pasos adicionales de verificación biométrica, mientras que las actividades de menor riesgo permanecen simplificadas, proporcionando una experiencia fácil de usar. La biometría del comportamiento también ayuda a detectar el fraude al identificar cambios inusuales en el comportamiento del usuario (Figura 5).[29]

Aunque estos seis avances marcan un progreso significativo en ciberseguridad, el panorama sigue evolucionando. Tecnologías como la computación cuántica, la computación segura multipartita (SMPC) y el cifrado h o m o m ó r f i c o prometen reforzar aún más las defensas. Sin embargo, para lograr un entorno digital resistente y seguro, es imprescindible una estrategia de ciberseguridad holística. Esto implica combinar tecnología avanzada, prácticas de seguridad tradicionales y fomentar la colaboración global para combatir el cambiante panorama de las amenazas. Reconocer las variaciones de las distintas regiones es vital para la eficacia de dicha estrategia.

Análisis de las medidas actuales de ciberresiliencia frente a las amenazas del mundo real

Un examen en profundidad de las estrategias defensivas contra las polifacéticas amenazas digitales revela una compleja interacción de tecnologías avanzadas y marcos integrales. Esta intrincada danza implica una relación simbiótica entre IA, ML, ZTA, blockchain, marcos legales y sólidas prácticas de ciberseguridad, formando un mecanismo de defensa multifacético.

Tanto la IA como el ML actúan como centinelas vigilantes, aprovechando amplios análisis de datos para identificar componentes comprometidos y detectar actividades IoT sospechosas. Esto complementa a la perfección los sólidos marcos de ciberseguridad que establecen las mejores prácticas del sector. La ZTA refuerza aún más la seguridad limitando el movimiento lateral, incluso después de una posible infiltración. La utilización de la cadena de bloques, un libro de contabilidad inmutable, garantiza el seguimiento de la procedencia de los componentes, abordando los problemas de autenticidad en la cadena de suministro. La incorporación de directrices de marcos de ciberseguridad reconocidos, como el Cybersecurity Frame-work del National Institute of Standards and Technology, mejora la implementación segura de blockchain. Es esencial reconocer el potencial de sesgo de la IA, subrayando la importancia de las consideraciones éticas y los diversos conjuntos de datos de formación. Además, aunque la complejidad de la ZTA requiere conocimientos especializados, la aplicación de marcos de ciberseguridad como modelos de implementación puede mitigar los retos. Abordar las limitaciones de escalabilidad en las implementaciones actuales de blockchain exige esfuerzos de colaboración y claridad normativa.

En el ámbito de los ataques DDoS, la IA y el ML desempeñan un papel crucial en la respuesta rápida a patrones de tráfico anómalos, mitigando su impacto. Incidentes coordinados

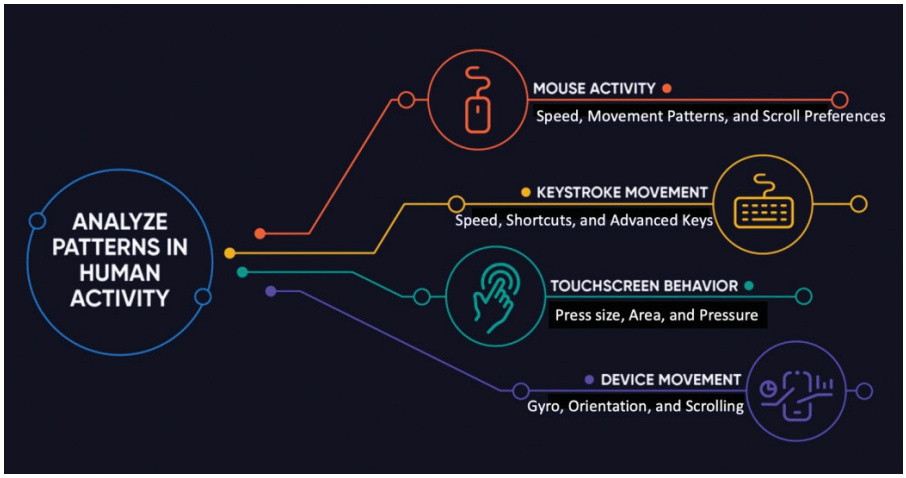

Fig. 5. Tipos de singularidad en el patrón de comportamiento[28]

Citación: Blockchain en la sanidad hoy 2024, 7: 302 - https://doi.org/10.30953/bhty.v7.302

Los planes de respuesta, tal y como se describen en los marcos de ciberseguridad establecidos, garantizan un tiempo de inactividad mínimo. Los servicios especializados de mitigación DDoS actúan como un baluarte contra los ataques digitales, con marcos legales que responsabilizan a los proveedores de servicios de las infracciones. La ZTA, mediante la verificación de la identidad y las restricciones de acceso, refuerza las defensas contra los ataques DDoS originados en cuentas comprometidas. Sin embargo, es esencial reconocer que los sistemas de mitigación DDoS basados en IA pueden interrumpir inadvertidamente el tráfico legítimo, causando interrupciones del servicio. Los costes asociados a los servicios especializados de mitigación de DDoS presentan barreras financieras, especialmente para las organizaciones más pequeñas. Los retos de coordinación durante la respuesta a incidentes, influidos por los retrasos en las comunicaciones y las complejidades jurisdiccionales, subrayan las complejidades de la defensa DDoS.

En la lucha contra las APT, la IA y el ML actúan como analistas vigilantes, discerniendo sutiles anomalías indicativas de amenazas potenciales. Los marcos legales facilitan el intercambio de inteligencia sobre amenazas, fomentando una defensa colectiva contra las tácticas conocidas de las APT. La ZTA, mediante el acceso restringido y la verificación continua de la identidad, dificulta el movimiento de las APT y la exfiltración de datos. La presencia de leyes de notificación de violaciones de datos incentiva la divulgación rápida, mitigando los daños relacionados con las APT. Sin embargo, los sistemas de detección de APT basados en IA pueden generar falsos positivos, lo que requiere investigaciones que consumen muchos recursos. Las sofisticadas técnicas empleadas por las APT para ocultar su actividad ponen de manifiesto las limitaciones de las herramientas de vigilancia avanzadas. La preocupación por la privacidad y la necesidad de confianza pueden obstaculizar el intercambio colaborativo de información confidencial sobre amenazas.

Al cambiar el enfoque hacia la ingeniería social, la formación para la concienciación sobre la seguridad prepara a las personas para reconocer y resistir la manipulación, con el apoyo de marcos de ciberseguridad que guían la aplicación eficaz del programa. La autenticación multifac-tor añade una capa adicional de seguridad, con marcos legales que incentivan su adopción. Fomentar un entorno de comunicación abierta favorece la detección precoz de los esquemas de ingeniería social. Sin embargo, la eficacia de la formación para la concienciación sobre la seguridad puede variar entre los empleados, especialmente entre aquellos con conocimientos técnicos limitados. La constante evolución de los atacantes requiere una adaptación continua de las estrategias para contrarrestar las nuevas técnicas. Establecer una cultura de comunicación abierta puede ser difícil, especialmente en organizaciones jerárquicas.

La biometría del comportamiento entra en juego cuando se supervisa el comportamiento del usuario para descubrir posibles intentos de acceso no autorizado. Las contraseñas seguras y la autenticación multifactor proporcionan una sólida defensa guiada por marcos de ciberseguridad. La prevención de la pérdida de datos minimiza el riesgo de filtración de datos sensibles, y las leyes de notificación de violaciones de datos incentivan respuestas rápidas. No obstante, pueden surgir problemas de privacidad en la recopilación de datos biométricos de los empleados, y la fatiga de los usuarios con la autenticación multifactor puede afectar a su adopción. La implantación y el mantenimiento de soluciones eficaces de prevención de pérdida de datos (DLP) plantean retos financieros.

A la hora de salvaguardar la propiedad intelectual, el cifrado de datos garantiza la confidencialidad, y los marcos jurídicos penalizan la protección inadecuada de datos sensibles. La gestión de derechos digitales controla el acceso, impidiendo la copia y distribución no autorizadas. La planificación de la respuesta a incidentes, tal y como se describe en los marcos de ciberseguridad, facilita una actuación rápida en caso de sospecha de robo de propiedad intelectual. Sin embargo, la gestión segura de las claves de cifrado es primordial para garantizar la eficacia del cifrado. Los problemas de interoperabilidad entre distintos sistemas DRM pueden dificultar la distribución de contenidos. La rapidez de la respuesta a los incidentes de robo de propiedad intelectual requiere una amplia coordinación y consideraciones jurídicas.

Al mejorar la vigilancia de los ataques de día cero, la IA y el ML buscan continuamente anomalías, abordando los ataques de día cero antes de su difusión generalizada. Las tecnologías de engaño, como los honeypots y los señuelos, revelan los exploits de día cero, con marcos legales que ofrecen protección. La modelización de amenazas, facilitada por metodologías estructuradas, permite adoptar medidas de mitigación proactivas. Sin embargo, los problemas de explicabilidad de la IA pueden dar lugar a falsos positivos o al descuido de las amenazas. Las consideraciones legales en el despliegue de tecnologías de engaño subrayan las posibles perturbaciones y requieren una planificación cuidadosa. Las lagunas en las metodologías de modelado de amenazas dificultan la planificación eficaz y la mitigación de las amenazas de día cero.

Para hacer frente a las amenazas internas es necesario supervisar el comportamiento inusual de los usuarios mediante la biometría del comportamiento y llevar a cabo revisiones periódicas del acceso, siguiendo las directrices de los marcos de ciberseguridad. Los mecanismos de denuncia anónima permiten a los empleados informar de actividades sospechosas sin temor a represalias. Equilibrar las necesidades de seguridad con las preocupaciones de privacidad de los empleados es crucial en la supervisión de la actividad de los empleados. La eficacia de las revisiones periódicas de acceso puede verse comprometida por la naturaleza intensiva en recursos del proceso. A pesar de las protecciones legales, el miedo a las represalias puede dificultar la notificación oportuna de amenazas internas.

En el contexto de la reducción de los ataques de ransomware, las copias de seguridad de los datos garantizan una restauración rápida, mitigando el impacto de tales ataques. La rápida gestión de vulnerabilidades reduce la superficie de ataque, con marcos legales que incentivan la divulgación de vulnerabilidades. La formación en materia de seguridad informa a los empleados sobre los riesgos del ransomware y las tácticas de phishing. Sin embargo, los ataques de ransomware pueden tener como objetivo las copias de seguridad, con la consiguiente pérdida de datos incluso después de la restauración primaria del sistema. Parchear vulnerabilidades con prontitud puede ser un reto, especialmente en entornos informáticos complejos. Las frecuentes sesiones de formación sobre concienciación en materia de seguridad pueden contribuir al cansancio de los empleados.

Los ataques de ingeniería social pueden mitigarse mediante la supervisión de medios sociales , guiada por datos privacidad

normativa. Las campañas de concienciación sobre el phishing y la autenticación multifactor reducen la tasa de éxito de estos ataques. Los marcos jurídicos incentivan las prácticas de autenticación sólidas. Sin embargo, la supervisión de la actividad de los empleados en las redes sociales plantea problemas de privacidad y requiere políticas trans-parentes. Desarrollar simulaciones de phishing eficaces puede requerir muchos recursos. Aunque eficaces, los sistemas de autenticación multifactor introducen vulnerabilidades potenciales. La clasificación de datos prioriza y etiqueta los datos sensibles, tal y como exige la normativa de protección de datos. El control de acceso a los datos limita el acceso, minimizando el riesgo de filtración no autorizada. Las herramientas de DLP detectan y evitan la transferencia no autorizada de datos, guiándose por los marcos de ciberseguridad. Sin embargo, una clasificación de datos demasiado granular puede aumentar los costes operativos y obstaculizar el acceso legítimo a los datos. La implantación de sistemas sólidos de control de acceso requiere experiencia en gestión de identidades y autorización. Las herramientas de DLP pueden gener-
de falsos positivos, lo que requiere una gestión cuidadosa.

La supervisión continua de los usuarios, aplicada a través de medidas técnicas y organizativas, ayuda a prevenir la apropiación no autorizada de cuentas. Las herramientas analíticas avanzadas detectan patrones sospechosos en los inicios de sesión de los usuarios. Las prácticas de autenticación sólidas, como la autenticación multifactor y las políticas de contraseñas seguras, reducen significativamente el riesgo de que se produzcan robos de cuentas. Los marcos jurídicos pueden incentivar a las organizaciones a adoptar y mantener prácticas de autenticación sólidas. Sin embargo, la implantación y el mantenimiento de sistemas de supervisión continua de usuarios pueden resultar caros, sobre todo para organizaciones con grandes bases de usuarios. Un alto volumen de alertas de actividad sospechosa puede abrumar a los equipos de seguridad, provocando la fatiga de las alertas y el descuido potencial de amenazas genuinas. Convencer a los usuarios para que adopten y utilicen de forma coherente métodos de autenticación fuertes plantea un reto, especialmente entre los usuarios no técnicos. Para navegar por el intrincado panorama de la ciberseguridad, es imperativo reconocer tanto los puntos fuertes como las limitaciones de las distintas estrategias. La integración colaborativa de IA, ML, ZTA, blockchain, marcos legales y prácticas integrales de ciberseguridad contribuye a una defensa multicapa contra las diversas y cambiantes amenazas que ensombrecen el ámbito digital. A medida que avanzan las tecnologías y evolucionan las amenazas, un enfoque holístico que abarque las innovaciones tecnológicas, las consideraciones éticas, el cumplimiento de la normativa y la mejora continua sigue siendo fundamental para salvaguardar la integridad, confidencialidad y disponibilidad de los activos digitales.

Soluciones propuestas para salvaguardar la integridad digital

Hemos abordado varias soluciones centradas en la prevención de las amenazas a la ciberseguridad, reconociendo que no existe una solución única. Ahora vamos a centrarnos en un aspecto diferente de la cuestión. ¿Cómo podemos minimizar la difusión de información confidencial filtrada? ¿Qué medidas medidas pueden aplicarse para que las violaciones de datos sean menos gratificantes, disuadiendo a los posibles atacantes de iniciar tales acciones? Exploremos las soluciones en torno a estas preguntas.

Concepto de eliminación de filtraciones

Siguiendo la filosofía de que un enfoque proactivo es clave para una defensa eficaz, he desarrollado un concepto que se ajusta a este principio. Antes de profundizar en los detalles, familiaricémonos con algunos términos esenciales que resultarán beneficiosos en nuestra exploración.

Para empezar, los datos hexadecimales son una representación de la información en un sistema numérico de base 16. Sirve como formato fundamental para la codificación de datos. Se trata de un formato fundamental para la codificación de datos binarios, empleado habitualmente en programación e informática.

La huella digital basada en el contenido es una técnica que examina el contenido visual o sonoro de un archivo para crear una huella digital única, una especie de "hash" digital que capta la esencia del medio sin necesidad de reproducirlo. Los algoritmos extraen características como colores, texturas, formas o frecuencias de audio para componer esta huella digital. Y lo que es más importante, este método sigue siendo eficaz para identificar el contenido original, aunque el formato del archivo sufra cambios o compresión.[30]El hash perceptual desplaza el foco de atención a cómo perciben los humanos el contenido. A pesar del ruido, los artefactos de compresión o la edición, el hashing perceptual sigue siendo sólido a la hora de identificar medios de forma única.[31]

Por otra parte, un gusano es un tipo de software malicioso capaz de replicarse de forma independiente y propagarse por redes y sistemas. Los gusanos aprovechan las vulnerabilidades, lo que representa una amenaza significativa para la seguridad de los entornos interconectados.

Del mismo modo, el malware troyano se disfraza de software legítimo, engañando a los usuarios para que lo instalen. Una vez infiltrado, permite el acceso no autorizado y puede comprometer información sensible o facilitar otras actividades maliciosas.

Además, una bomba lógica es un fragmento de código insertado intencionadamente en un sistema de software para ejecutar acciones dañinas cuando se cumplen determinadas condiciones. Estas condiciones pueden ser desencadenadas por varios eventos, causando potencialmente interrupciones o daños al sistema.

En el ámbito de las vulnerabilidades recientes, es crucial destacar la vulnerabilidad crítica de las imágenes WebP (CVE-2023-4863)[32]. Este fallo permitía a los atacantes ejecutar código malicioso a través de archivos .webp manipulados, afectando a numerosas aplicaciones debido al uso generalizado de la biblioteca libwebp para manejar dichas imágenes. Es esencial actualizar inmediatamente el software para solucionar esta vulnerabilidad y garantizar la protección. Si nos centramos en las protecciones integradas, los antivirus y los indexadores de búsqueda integrados en el sistema operativo son herramientas integrales diseñadas para detectar y neutralizar virus y programas maliciosos. Estas utilidades vigilan e identifican activamente las amenazas potenciales, contribuyendo significativamente a la protección general de los sistemas operativos.
seguridad del sistema.

Citación: Blockchain en la sanidad hoy 2024, 7: 302 - https://doi.org/10.30953/bhty.v7.302

Además, una red de distribución de contenidos (CDN) funciona como un sistema distribuido de servidores que colaboran para entregar contenidos web de forma eficiente en función de la ubicación geográfica de los usuarios. Además de mejorar el rendimiento de los sitios web, las CDN proporcionan una capa añadida de seguridad frente a ciberamenazas específicas.

Entender estas terminologías es esencial para comprender los matices del concepto que se centra en una estrategia de defensa proactiva. Ahora, profundicemos en los aspectos específicos de cómo cada uno de estos elementos contribuye a construir mi sólido enfoque de ciberseguridad.

El proceso consiste en tomar los archivos multimedia o de texto deseados para "soltarlos". A continuación, estos archivos se procesan mediante programas como hex dump o Vim para obtener datos hexadecimales de los archivos de texto e información de identificador único de los archivos multimedia, aprovechando las metodologías de huella digital basada en el contenido y hashing perceptual. Posteriormente, se desarrolla un código de gusano, diseñado para propagarse por Internet y conectarse a CDN para descargar troyanos (Figura 6).

Una vez que el gusano está activo en un dispositivo, recupera el paquete del troyano, y éste, a su vez, descarga los metadatos (datos hexadecimales o identificadores únicos) previamente generados y dispersos por diversas CDN públicas o privadas. El siguiente paso consiste en que el troyano se empareja con los escáneres de virus o índices de búsqueda incorporados en el sistema, iniciando un escaneo para encontrar coincidencias con los metadatos almacenados.

En los casos en que el sistema carece de un escáner para el acceso root/administrador, el gusano puede descargar el suyo propio de los precargados en la CDN. Utilizando una estrategia de caballo de Troya, el gusano puede engañar a los usuarios para que concedan privilegios de administrador presentándose como un archivo del sistema. Volviendo al proceso de escaneado, si se detecta una coincidencia, el gusano actúa como una bomba lógica, corrompiendo los archivos al sustituir los datos originales por datos basura. Este método pretende eliminar la información filtrada sin provocar acciones destructivas adicionales.

En situaciones en las que el acceso a la CDN no está disponible, el script del gusano puede adjuntarse a un archivo y enviarse a usuarios no sospechosos, lo que recuerda a técnicas como las macros de Word o la explotación de vulnerabilidades como .webp. Una vez ejecutado, el gusano emprende sus tareas. Además, el gusano está programado para detectar la presencia de cualquier troyano existente con el fin de evitar la sobrecarga del sistema y la posible detección por parte del usuario. Este enfoque integral garantiza un método estratégico y matizado para abordar la filtración de información.

Modelo de privacidad de datos Web3

La transición de la Web 2.0 a la Web 3.0 marca el paso de sistemas centralizados a sistemas descentralizados. El principio básico de la Web 3.0 es la descentralización, que transforma radicalmente el tratamiento de los datos y las aplicaciones. Este cambio mejora la privacidad al reducir la dependencia de las autoridades centrales, lo que permite a los individuos tener un mayor control sobre su información personal. En la Web 3.0, tecnologías como la cadena de bloques, los identificadores descentralizados y las pruebas de conocimiento cero desempeñan un papel clave en el fomento de un entorno digital más privado, seguro y centrado en el usuario. Ahora, adentrándonos en los entresijos de este modelo, se aprovechan conceptos contemporáneos actualmente en desarrollo. Antes de profundizar en los detalles operativos del modelo, es crucial familiarizarse con la terminología asociada.

Los DID son un elemento fundacional de la Web 3.0, ya que desempeñan un papel vital a la hora de proporcionar a los usuarios un mecanismo descentralizado para crear y gestionar identidades únicas en línea. A través de los DID, los usuarios adquieren autonomía para establecer y controlar su personalidad digital de forma independiente, mejorando así su privacidad. Un ejemplo que ilustra esto es la capacidad de los DID para permitir a los individuos crear y gestionar identidades en línea sin depender de una autoridad central, en consonancia con el tema general de la mejora de la privacidad del usuario en el ámbito digital[33].

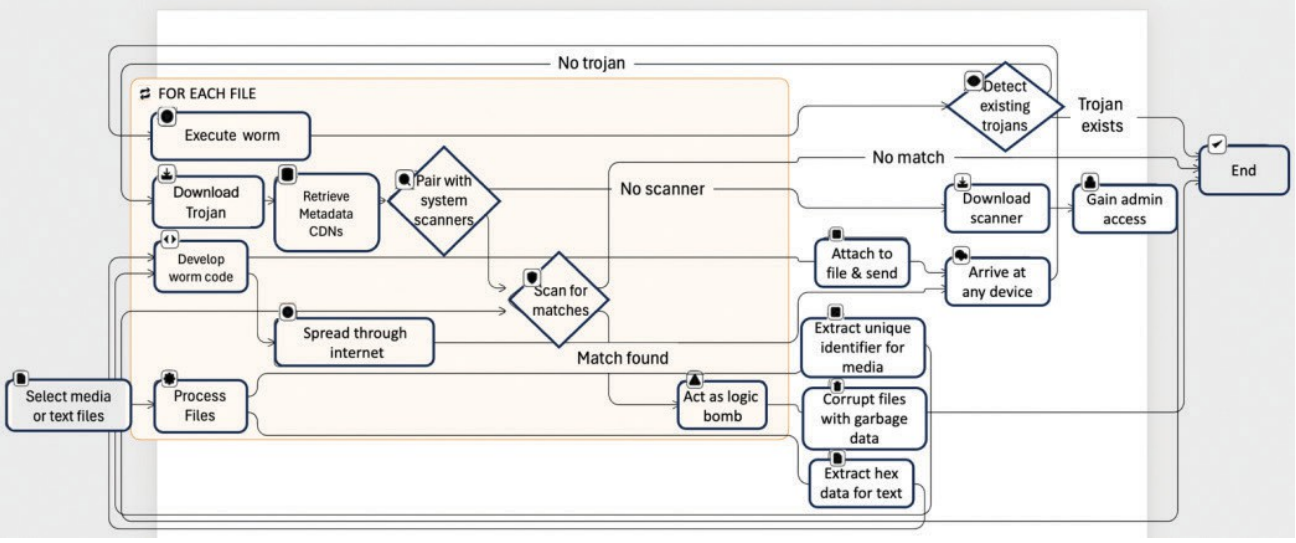

Fig. 6. Diagrama de flujo explicativo del mecanismo de funcionamiento.

Las CV constituyen un aspecto fundamental de la Web 3.0, ya que facilitan la emisión y presentación de credenciales a prueba de manipulaciones y verificables digitalmente. En la práctica, las personas pueden compartir credenciales firmadas digitalmente, como diplomas, sin divulgar información personal innecesaria. Esto ejemplifica el papel de las CV en el refuerzo de la privacidad y la seguridad, proporcionando una ilustración tangible de cómo capacitan a los usuarios en el panorama digital[34].

Las pruebas de conocimiento cero (ZKP) destacan como una técnica criptográfica crucial dentro del paradigma de la Web 3.0, ya que permiten a las partes demostrar la autenticidad de la información sin revelar los datos reales. Los ZKP contribuyen significativamente a la privacidad al verificar la información sin revelar los detalles subyacentes. Un ejemplo que ilustra este concepto es cuando las ZKP permiten a alguien demostrar el conocimiento de un secreto sin revelar el propio secreto, garantizando así la privacidad en las transacciones digitales[35].

El aprendizaje federado (FL) transforma el panorama del ML en la Web 3.0 al facilitar el entrenamiento colaborativo de modelos a través de dispositivos descentralizados. Un ejemplo que ilustra el enfoque de FL respetuoso con la privacidad es su capacidad para permitir que los dispositivos móviles entrenen en colaboración un modelo predictivo sin intercambiar datos brutos. Esto preserva la privacidad del usuario al tiempo que aprovecha el conocimiento agregado en beneficio de todo el sistema[36].

El SMPC desempeña un papel fundamental en la Web 3.0, ya que permite el cálculo seguro entre múltiples partes sin exponer las entradas individuales. Un ejemplo ilustrativo es cuando el SMPC permite a varias partes calcular conjuntamente un resultado sin revelar sus entradas individuales. Esta funcionalidad resulta valiosa para el análisis de datos confidenciales, lo que pone de relieve su importancia para salvaguardar la privacidad[37].

Los almacenes de datos personales (PDS) permiten a los individuos gestionar sus datos personales de forma segura dentro de un repositorio privado. Por ejemplo, los PDS permiten a los usuarios controlar el acceso a su información almacenada, reforzando el control del usuario sobre su identidad digital y mejorando la privacidad en la gestión de los datos personales.[38]

El almacenamiento de datos basado en blockchain (BBDS) es un concepto revolu-cionario de la Web 3.0, que descentraliza el almacenamiento de información en una red de nodos. Este enfoque transparente y a prueba de manipulaciones garantiza la integridad de los datos y minimiza el riesgo de alteraciones no autorizadas. Un ejemplo que ilustra este concepto es la forma en que blockchain almacena los datos, haciéndolos resistentes a la manipulación y garantizando un almacenamiento de datos transparente, seguro y con mayor privacidad.[39]

Los entornos de ejecución de confianza (TEE) contribuyen significativamente a la Web 3.0 proporcionando espacios seguros en los dispositivos para procesar información sensible. Los TEE en acción son su capacidad para salvaguardar las claves de cifrado y proteger la privacidad del usuario garantizando que determinados procesos se produzcan en un espacio de confianza y protegido en un dispositivo.[40])

Actualmente, las terminologías pueden no estar del todo claras (Figura 7). Conozcamos a fondo

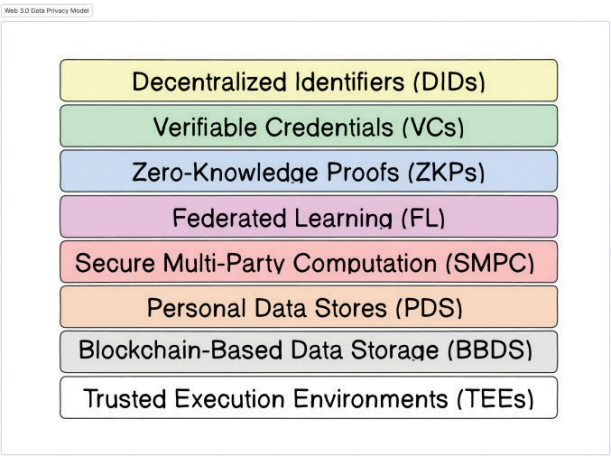

Fig. 7. Modelo de privacidad de datos Web3 (W3DPM).

todos estos conceptos utilizando el modelo y explorando un ejemplo que demuestra la funcionalidad de cada modelo.

En este escenario futurista de votación impulsado por las tecnologías Web 3.0, los individuos experimentan un proceso electoral transformador y centrado en la privacidad. Cada votante dispone de un DID almacenado en su dispositivo móvil, que le otorga la propiedad y el control de su identidad digital con independencia de una autoridad central. En lugar de la identificación física tradicional, los votantes emiten CV seguras a través de sus DID directamente desde las bases de datos gubernamentales, lo que demuestra la elegibilidad sin comprometer los datos personales y, por tanto, mejora la privacidad.

Para garantizar aún más la privacidad, la autoridad electoral emplea ZKP para verificar la elegibilidad de los votantes sin acceder a los registros individuales y confirmar la elegibilidad sin exponer detalles específicos. El modelado predictivo colaborativo se consigue a través de FL, donde los modelos ML se entrenan con datos cifrados de los votantes almacenados de forma segura en dispositivos individuales. Esto no solo mejora la precisión predictiva, sino que también mantiene la privacidad durante todo el proceso.

La integridad de los resultados electorales se salvaguarda aprovechando el SMPC durante el cálculo de los resultados. Los funcionarios electorales y los auditores independientes analizan en colaboración los datos de la votación sin compartir directamente información sensible, preservando así la confidencialidad de los votos individuales. Los votantes conservan el control sobre su historial de voto y sus preferencias a través del PDS, al que la comisión electoral sólo puede acceder con el consentimiento explícito del votante a través de los DID y los CV, lo que minimiza la exposición de los datos y permite a los usuarios gestionar su información de forma segura (Figura 8).

El almacenamiento transparente y a prueba de manipulaciones se logra a través de BBDS, donde los resultados electorales y los registros de votación se almacenan de forma segura en una blockchain autorizada. Esto garantiza la integridad del proceso electoral al tiempo que restringe el acceso a las entidades autorizadas. Además,

Citación: Blockchain en la sanidad hoy 2024, 7: 302 - https://doi.org/10.30953/bhty.v7.302

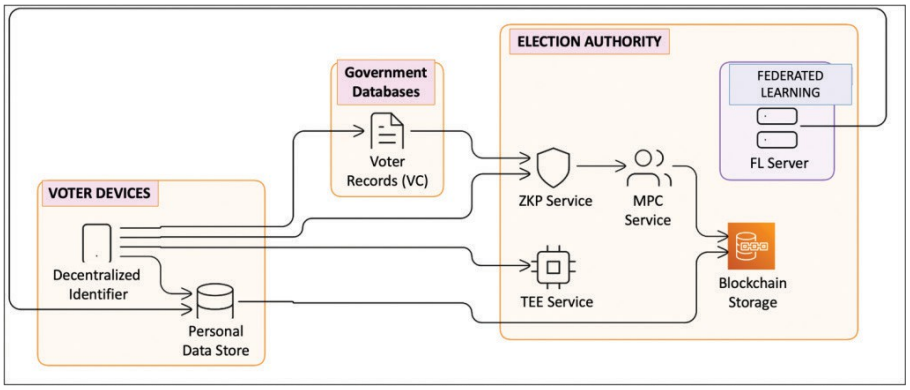

Fig. 8. Ejemplo de escenario de votación. FL: aprendizaje federado; TEE: entornos de ejecución de confianza; ZKP: pruebas de conocimiento cero.

Los TEE aportan una capa adicional de seguridad aislando los cálculos sensibles, como la detección de fraudes y la verificación de resultados, dentro de enclaves de confianza en los dispositivos de los votantes.

Este completo ejemplo demuestra cómo los principios de la Web 3.0 revolucionan las aplicaciones del mundo real. Ofrece una experiencia de voto segura, transparente y centrada en la privacidad, en la que los individuos mantienen el control sobre sus identidades y datos personales a lo largo de todo el proceso electoral.

Análisis comparativo y crítico

Como ya se ha dicho, mis soluciones y mi planteamiento en materia de ciberseguridad se apartan considerablemente de las prácticas dominantes en este campo. En consecuencia, una comparación directa con las metodologías existentes plantea distintos retos. Si centramos nuestra atención en el concepto de deleakificación, éste resulta controvertido y potencialmente peligroso, ya que encierra tanto ventajas como inconvenientes.

Un virus bien diseñado, parte integrante del concepto de borrado, tiene el potencial de escanear y eliminar eficazmente los datos seleccionados, superando a los métodos manuales o tradicionales, lo que resulta especialmente beneficioso cuando se trata de conjuntos de datos extensos. Esta ventaja resulta especialmente crucial en situaciones en las que el tiempo apremia y la rápida mitigación de la información filtrada es primordial.

Otra ventaja es la capacidad del virus para acceder y eliminar datos de sistemas infectados a los que podría resultar difícil llegar por medios convencionales, como dispositivos desconectados o ubicaciones de almacenamiento ocultas. Aunque es ventajoso en determinados casos, las consecuencias imprevistas y las posibles violaciones de la privacidad son motivo de preocupación.

La visión de un virus autorreplicante dentro de este concepto introduce la perspectiva de automatizar el proceso de eliminación de datos, reduciendo la dependencia de la intervención humana y minimizando potencialmente el riesgo de error humano. Sin embargo, esta automatización suscita preocupaciones válidas relacionadas con la controlabilidad y el potencial de propagación o daños no intencionados.

Es imperativo reconocer que la aplicación práctica de un virus de este tipo se enfrentaría a retos considerables. Conseguir un objetivo preciso para eliminar los datos filtrados sin afectar a los contenidos legítimos en línea resulta ser una tarea complicada. Dada la rápida e incontrolable propagación de los virus, existe un riesgo considerable de afectar a datos no relacionados, lo que podría causar daños colaterales. Para complicar aún más las cosas, los datos filtrados suelen existir fragmentados en múltiples sitios y plataformas. El virus requeriría un diseño excepcionalmente sofisticado para localizar y eliminar todas las instancias de la información filtrada, lo que resulta prácticamente imposible.
información filtrada, lo que resulta prácticamente imposible en la mayoría de los casos. Además, la tecnología subyacente de un virus de este tipo,
si bien se diseñó con fines éticos dentro de la deleakificación, podría ser susceptible de uso indebido con objetivos maliciosos. Esto sienta un precedente preocupante para posibles ciberataques en el futuro y pone de relieve importantes problemas éticos y de seguridad.

Las soluciones de privacidad de datos de la Web 3.0 suponen un cambio de paradigma en la forma en que los individuos gestionan sus identidades y, entre ellas, los DID desempeñan un papel crucial. Al permitir a los individuos poseer y gestionar sus identidades, los DID reducen la influencia de las autoridades centrales, minimizando así la vulnerabilidad de los datos. Sin embargo, la complejidad de la gestión de los DID y las CV podría impedir su adopción generalizada, especialmente entre los usuarios no técnicos. La necesidad de perfeccionar continuamente las normas y la interoperabilidad es primordial para garantizar una colaboración fluida entre diversas plataformas.

Las CV ofrecen una forma segura de compartir atri-butos de datos específicos, mitigando los riesgos de manipulación de datos y usurpación de identidad. Sin embargo, la integración de las CV en diversos sectores exige una adopción generalizada y formatos coherentes para facilitar su verificación y utilización sin fisuras. La aplicación ética es crucial para evitar un posible uso discriminatorio de las CV.

Las ZKP ofrecen una solución innovadora al demostrar la posesión de información sin revelar detalles, lo que reduce la exposición de los datos. Sin embargo, la aplicación y comprensión de las

las ZKP plantean retos tanto para los desarrolladores como para los usuarios, ya que exigen conocimientos técnicos. El coste computacional de las ZKP complejas podría repercutir en los recursos de procesamiento, por lo que es necesario tenerlo muy en cuenta durante la integración.

El FL minimiza el intercambio de datos al entrenar los modelos en dispositivos locales, lo que mejora la privacidad. Sin embargo, la agregación y gestión de datos descentralizados puede ralentizar los procesos. Unos protocolos de seguridad sólidos son esenciales para garantizar la seguridad de los datos en diversos dispositivos y redes, y unos incentivos bien diseñados son cruciales para fomentar la participación de los usuarios.

El SMPC permite el análisis conjunto de datos sin revelar las contribuciones individuales, lo que fomenta una colaboración segura. Sin embargo, el coste computacional de los protocolos complejos y las dificultades de ampliación a grandes conjuntos de datos exigen un hardware potente. Su aplicación efectiva requiere conocimientos técnicos especializados.

Los PDS permiten a los individuos poseer y gestionar sus datos, reduciendo la vulnerabilidad a las violaciones centralizadas. Sin embargo, es vital que los formatos de los datos y los protocolos de acceso sean coherentes para poder compartirlos sin problemas. Los mecanismos de copia de seguridad y recuperación son esenciales para evitar la pérdida de datos, y la formación de los usuarios es clave para su adopción generalizada.

La BBDS garantiza la inmutabilidad y la transparencia de los datos, pero algunos mecanismos de consenso plantean problemas de escalabilidad para grandes volúmenes y de entorno. Las técnicas de preservación de la privacidad son cruciales para equilibrar las ventajas de la transparencia con la privacidad del usuario.

Las TEE proporcionan enclaves seguros para cálculos sensibles, mejorando la seguridad de los datos. Sin embargo, hay que tener en cuenta su limitada disponibilidad en todos los dispositivos y su posible sobrecarga de ejecución. La investigación continua es esencial para abordar las posibles vulnerabilidades y garantizar una seguridad sólida.

En general, el concepto de deleakificación y las soluciones de privacidad de datos de la Web 3.0 ofrecen un gran potencial para dotar a las personas de un mayor control sobre sus datos y garantizar la privacidad en el mundo digital. Sin embargo, cada tecnología tiene sus propias ventajas e inconvenientes, y su aplicación con éxito requiere una cuidadosa consideración de estos factores, así como la colaboración de las distintas partes interesadas para abordar los retos existentes y garantizar un desarrollo ético y responsable.

Conclusión y alcance futuro

El panorama actual de los modelos de unleakification y Web3 para la privacidad de los datos se enfrenta a limitaciones, ya que estas tecnologías se encuentran aún en sus primeras fases. Sin embargo, esta fase incipiente ofrece una importante oportunidad de mejora, haciéndolas más viables, fáciles de usar y ampliamente adoptables, lo que en última instancia aumentará su estabilidad. Es necesario abordar retos como la complejidad técnica, la adopción por parte de los usuarios y la escalabilidad, pero las oportunidades que ofrecen la descentralización y los datos propiedad de los usuarios son prometedoras para un futuro más seguro y centrado en el usuario.

En el ámbito de la IA y la ciberseguridad, el aumento de las superficies de ataque resultantes de la integración de la IA es preocupante. Marcos y normativas como la ISO 42001 y la legislación europea sobre IA son pasos en la dirección correcta para un desarrollo responsable y una seguridad sólida. Aunque las soluciones emergentes, como la criptografía cuántica, son prometedoras, la vigilancia frente a posibles amenazas, especialmente de la Inteligencia Artificial General (IAG), es crucial. Más allá de las consideraciones técnicas, es crucial abordar las implicaciones sociales y éticas de la IA y la privacidad de los datos. Los debates abiertos sobre la propiedad de los datos, los sesgos algorítmicos y la manipulación impulsada por la IA son necesarios para un desarrollo responsable. Hacer hincapié en la colaboración entre el ser humano y la IA, considerándola como una herramienta de capacitación y no como un sustituto, puede contribuir a un desarrollo ético y beneficioso. A medida que avanza la revolución de la IA, se producen avances y desafíos. La aplicación generalizada de la IA en diversos sectores amplía la superficie de ataque, lo que plantea retos para los profesionales de la ciberseguridad, que deben mejorar su juego. A pesar de los marcos existentes, aún queda mucho por proteger. El poder computacional de la IA podría dejar obsoletas las tecnologías actualmente seguras. Aunque las soluciones emergentes, como la criptografía cuántica, son prometedoras, las amenazas potenciales de la inteligencia artificial general subrayan la necesidad de una investigación cautelosa, medidas de seguridad sólidas y consideraciones éticas[41]La investigación continua, la colaboración y la consideración cuidadosa de los retos y las implicaciones éticas pueden ayudar a aprovechar el potencial de estas tecnologías para un futuro seguro, equitativo y enriquecedor.

Financiación

No se proporcionó financiación para la elaboración de este artículo.

Relaciones y actividades financieras y no financieras

Los autores no han informado de ninguna.

Colaboradores

Todos los autores de este artículo de investigación han participado directamente en la planificación, ejecución o análisis de este estudio. Todos los autores de este trabajo han leído y aprobado la versión final presentada.

Declaración de disponibilidad de datos (Das), intercambio de datos, reproducibilidad y repositorios de datos

Los datos originales no se utilizaron en la elaboración del artículo.

Aplicación de texto generado por IA o tecnología relacionada

En la elaboración de este artículo no se ha utilizado IA ni tecnologías relacionadas.

Agradecimientos

Ninguno.

Referencias

1. Enigma. Bletchley Park. [citado 2024 Ene 13]. Disponible en: https://bletchleypark.org.uk/our-story/enigma/
2. Cronología de virus y gusanos informáticos. Wikipedia; 2024 [citado 2024 Ene 13]. Disponible en: https://en.wikipedia.org/w/index.php?title=Timeline_of_computer_viruses_and_worms&ol-did=1194773804
3. cybercrimemag. Se prevé que el gasto mundial en ciberseguridad supere el billón de dólares entre 2017 y 2021. Revista Cybercrime. 2024 [citado 2024 Ene 13]. Disponible en: https://cybersecurityven-tures.com/cybersecurity-market-report/
4. Principales amenazas a la ciberseguridad en 2023. Cisco. [citado 2024 Ene 13]. Disponible en: https://www.cisco.com/c/en/us/products/secu-rity/top-cybersecurity-threats-2023.html
5. M. C. D. O. C. (CDOC) Intelligence Microsoft Threat. Inmersión profunda en la activación de la segunda fase de Solorigate: de SUNBURST a TEARDROP y raindrop. Blog de seguridad de Microsoft. [citado 2024 Ene 15]. Disponible en: https://www.microsoft.com/en-us/ security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
6. ¿Qué es la red de bots Mirai? Cloudflare. [citado 2024 Ene 12]. Disponible en: https://www.cloudflare.com/learning/ddos/glossary/ mirai-botnet/
7. El hackeo de OPM explicado: las malas prácticas de seguridad se encuentran con el Capitán América chino. CSO Online. [citado el 12 de enero de 2024]. Disponible en: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america. html
8. ¿Qué es el ataque ransomware WannaCry? | UpGuard. [citado 2024 Ene 12]. Disponible en: https://www.upguard.com/blog/ wannacry
9. Ataque de ransomware Colonial Pipeline. Wikipedia; 2023 [citado 2024 Ene 12]. Disponible en: https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&ol-did=1189897140
10. Times F. A phone call to helpdesk was likely all it took to hack MGM. Ars Technica. [citado 2024 Ene 12]. Disponible en: https://arstechnica.com/security/2023/09/a-phone-call-to-help-desk-was-likely-all-it-took-to-hack-mgm/
11. Helmus TC. Artificial intelligence, deepfakes, and disinfor-mation: a primer. RAND Corporation; 2022 [citado 2024 Ene 12]. Disponible en: https://www.rand.org/pubs/perspectives/ PEA1043-1.html
12. Rashmika Mandanna caso deepfake : Delhi Police track down 4 suspects, hunt for key conspirator on. Hindustan Times. [citado 2024 enero 12]. Disponible en: https://www. hindustantimes.com/india-news/rashmika-mandanna-deepfake-case-delhi-police-track-down-4-suspects-hunt-for-key-conspirator-on-101703043714888.html
13. 2019 capital one cyber incident | Qué pasó. Capital One. [citado 2024 Ene 12]. Disponible: https://www.capitalone.com/ digital/facts2019/
14. Preguntas frecuentes sobre la violación de datos de Marriott: ¿qué ocurrió realmente? Hotel Tech Report. [citado 2024 Ene 12]. Disponible en: https://hoteltechre-port.com/news/marriott-data-breach
15. Page C. Tesla dice que la filtración de datos que afectó a 75.000 empleados fue un trabajo desde dentro. TechCrunch. [citado el 12 de enero de 2024]. Disponible en: https:// techcrunch.com/2023/08/21/tesla-breach-employee-insider/
16. Hern A, A. H. U. editor de tecnología. Pentagon leak traced to video game chat group users arguing over war in Ukraine. *The Guardian*; 2023 abr 11 [citado 2024 ene 12]. Disponible en: https://www.theguardian.com/world/2023/apr/11/pentagon-leak-traced-to-video-game-chat-group-users-arguing-over-war-in-ukraine
17. Stuxnet. *Wikipedia*; 2024 Ene 10 [citado 2024 Ene 12]. Disponible en: https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=119468 7512
18. IA en ciberseguridad: defienda su reino digital. [citado 2024 Ene 13]. Disponible en: https://www.veritis.com/blog/ai-in-cy-bersecurity-defending-against-evolving-threats/
19. Machine Learning (ML) in cybersecurity: use cases-Crowd-Strike.crowdstrike.com;[citado2024enero15]. Disponible en: https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity/
20. Chandramouli R, Butcher Z. A zero trust architecture model for access control in cloud-native applications in multi-cloud environments. National Institute of Standards and Technology, NIST Special Publication (SP) 800-207A; 2023.
21. Zhou L. ¿Qué es la arquitectura de confianza cero (ZTA)? | NextLabs Data-CentricSecurity.NextLabs.[citado2024enero13].Disponibleen: https://www.nextlabs.com/what-is-zero-trust-architecture-zta/
22. NIST: blockchain provides security, traceability for smart man-ufacturing. NIST; 2019 [citado 2024 Jan 13]. Disponible en: https://www.nist.gov/news-events/news/2019/02/nist-block-chain-provides-security-traceability-smart-manufacturing
23. Perspectiva de innovación para identidad descentralizada y reclamaciones verificables. Gartner. [citado 2024 ene 13]. Disponible en: https:// www.gartner.com/en/documents/4004851
24. ¿Qué es la tecnología de engaño? Importancia y ventajas| Zscaler. [citado 2024 Ene 13]. Disponible en: https://www.zscaler.com/ resources/security-terms-glossary/what-is-deception-technology
25. Han X, Kheir N, Balzarotti D. Deception techniques in com-puter security: a research perspective. ACM Comput. Surv. 2018;51(4):80:1–36. https://doi.org/10.1145/3214305
26. Página de inicio| CISA. [citado 2024 ene 13]. Disponible en: https:// www.cisa.gov/
27. El Consejo de Europa: Guardián de los Derechos Humanos, la Democracia y el Estado de Derecho para 700 millones de ciudadanos-Portal-www.coe.int. Portal. [citado 2024 Ene 13]. Disponible en: https:// www.coe.int/en/web/portal
28. ¿Qué es la biometría del comportamiento? [citado 2024 Ene 13]. Disponible en: https://www.biocatch.com/blog/what-is-behavioral-biometrics
29. Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective. IEEE Internet Things J. 2020;7(9):9128-43. https://doi.org/10.1109/JIOT.2020.3004077
30. Du L, Shang Q, Wang Z, Wang X. Robust image hashing based on multi-view dimension reduction. J Inf Secur Appl. 2023;77:103578. https://doi.org/10.1016/j.jisa.2023.103578
31. Qin C, Liu E, Feng G, Zhang X. Perceptual image hashing for content authentication based on convolutional neural network with multiple constraints. IEEE Trans Circuits Syst Video Technol. 2021;31(11):4523–37. https://doi.org/10.1109/ TCSVT.2020.3047142
32. Uncovering the Hidden WebP vulnerability: a tale of a CVE with muchbiggerimplicationsthanitoriginallyseemed. El blog de Cloudflare. [citado 2024 Ene 14]. Disponible en: https://blog.cloudflare. com/uncovering-the-hidden-webp-vulnerability-cve-2023-4863
33. Identificadores descentralizados (DID) v1.0. [citado 2024 Ene 14]. Disponible en: https://www.w3.org/TR/did-core/

34. Barker E. Recommendation for key management: part 1-gen-eral. Gaithersburg, MD: National Institute of Standards and Technology; 2020.
35. Fenzi G. Zero knowledge proofs theory and applications. Uni-versidad de St. Andrews. Andrews. September 2019. [citado sin fecha]. Disponible en: https://info.cs.st-andrews.ac.uk/student-handbook/files/ project-library/cs4796/gf45-Final_Report.pdf
36. Mahlool DH, Abed MH. A comprehensive survey on federated learning: concept and applications. arXiv. 2022. https://doi.org/10.48550/arXiv.2201.09384
37. Merino L-H, Cabrero-Holgueras J. Secure multi-party compu-tation. En: V Mulder, A Mermoud, V Lenders, B Tellenbach, editors. Trends in data protection and encryption technologies. Cham: Springer Nature Switzerland, 2023; p. 89-92.
38. Arewa O. Data Collection, Privacy, and Children in the Digital Economy. George Mason Legal Studies Research Paper No. LS 23-22, Capítulo en FAMILIES AND NEW MEDIA (Springer Link 2023). 2023. [citado sin fecha]. Disponible en: https://ssrn.com/ abstract=4617953 o https://doi.org/10.2139/ssrn.4617953
39. Foro Económico Mundial. [citado 2024 Ene 14]. Disponible en: https://www.weforum.org/publications/realizing-the-potent ial-of-blockchain/
40. Lee D, Kohlbrenner D, Shinde S, Asanovi K, Song D. Key-stone: an open framework for architecting trusted execution environments. En Proceedings of the fifteenth European con-ference on computer systems, en EuroSys '20. Nueva York: NY. Nueva York, NY: Association for Computing Machinery, 2020; p. 1-16.
41. Kaur R, GabrijelčD, Klobučar T. Artificial intelligence for cyber-security: literature review and future research directions. Inf Fusion. 2023;97:101804. https://doi.org/10.1016/j.inffus.2023.101804