Infraestructura responsiva con Zero Trust para procesos automatizados orientados a ciencia de datos.

*Responsive infrastructure with Zero Trust for automated processes oriented to data science.*

Oswaldo Díaz

Laboratorio de Ciencia de Datos, Instituto Nacional de Estadística y Geografía (INEGI)

Av. Héroe de Nacozari no 2301, Aguascalientes, México

oswaldo.diaz@inegi.org.mx

Mirna Muñoz, Jezreel Mejia

Centro de Investigación en Matemáticas (CIMAT), Unidad Zacatecas

Calle Lasec y Andador Galileo Galilei, Quantum, Ciudad del Conocimiento, C.P. 98160, Zacatecas, Zac.

{mirna.munoz, jmejia}@cimat.mx

Resumen — Este artículo describe cómo la implementación de una Infraestructura Responsiva con la estrategia de Zero Trust [3] puede reducir riesgos en los procesos automatizados orientados en ciencia de datos estadísticos y geoespaciales con niveles de seguridad y privacidad con tecnologías de información y comunicaciones.

Palabras Clave – Zero Trust, Procesos en ciencia de datos automatizados, Plataforma de servicios.

Abstract — This article describes how the implementation of a Responsive Infrastructure with the Zero Trust [3] strategy can reduce risks in automated processes oriented towards statistical and geospatial data science with levels of security and privacy using information and communication technologies.

Keywords – Zero Trust; Automated data science processes; Platform as a services .

1. Introducción

En el mundo actual, donde la ciencia de datos se ha convertido en un componente crítico para la toma de decisiones estratégicas y la innovación, la infraestructura tecnológica que soporta estos procesos debe ser robusta, flexible y segura. La creciente complejidad y volumen de los datos, junto con la necesidad de procesamiento automatizado, requiere una arquitectura de infraestructura que no solo sea eficiente, sino que también responda dinámicamente a las demandas cambiantes del entorno digital. Aquí es donde entra el concepto de Infraestructura Responsiva, diseñada para adaptarse y escalar según las necesidades de los procesos automatizados.

Sin embargo, con el aumento de la conectividad y la interdependencia digital, también crece el riesgo de ciberamenazas [1]. Es en este contexto que el enfoque de seguridad conocido como “Zero Trust” [3], se vuelve indispensable. Este paradigma de seguridad parte de la premisa de que ninguna entidad, ya sea dentro o fuera de la red organizacional, debe ser confiada de manera implícita. La combinación de Infraestructura Responsiva con el modelo Zero Trust [3] crea un entorno donde los datos y los procesos automatizados no solo operan con máxima eficiencia, sino también con la seguridad necesaria para proteger la integridad, disponibilidad y confidencialidad de la información, utilizada como insumo para procesos orientados a ciencia de datos.

Después de la introducción, el artículo se estructura como sigue: en la sección 2, se muestran los antecedentes; en la sección 3, se muestra la implementación de la plataforma, en la sección 4, se muestra las conclusiones.

1. ANTECEDENTES

La Arquitectura Zero Trust (Confianza Cero) [3] es un enfoque de seguridad informática que se basa en la premisa de no confiar en nada ni en nadie por defecto, asume que las amenazas pueden surgir tanto desde el interior como desde el exterior.

Los tres pilares principales de Zero Trust [3] son:

* Verificar explícitamente: autenticar y autorizar siempre en función de todos los puntos de controles disponibles, incluida la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.
* Utilizar el acceso con privilegios mínimos: limitar el acceso de los usuarios con limitaciones de tiempo suficientes para generar las actividades, generar políticas orientadas a reducir riesgos, protección de datos generando valor agregado a la productividad.
* Asumir la infracción: verificar el cifrado de extremo a extremo, utilizar la analítica para obtener visibilidad, detectar amenazas y mejorar las defensas.

¿Por qué implementar Zero Trust [3]?

* Permite tener un control del crecimiento de personas, procesos, tecnología, con soluciones ágiles para el control en reducir riesgos internos y externos.
* Permite proteger un volumen creciente de datos en un entorno multiplataforma + multinube hibrida, aporta a simplificar la seguridad con una estrategia, procesos, herramientas automatizadas que verifican cada transacción, aplican el acceso con privilegios mínimos, aplican detección, respuestas avanzadas a las amenazas internas y externas.
* Permite autenticar, autorizar y cifrar completamente todas las solicitudes de acceso, aplica principios de microsegmentación, acceso con privilegios mínimos para minimizar el movimiento lateral, utiliza inteligencia, análisis para detectar y responder a anomalías en tiempo real.

En la siguiente figura muestra los componentes involucrados en el enfoque Zero Trust [3].

Diagrama, Esquemático

Descripción generada automáticamente

Figura 1. Enfoque Zero Trust [3].

Considerando los procesos automatizados orientados a ciencia de grandes volúmenes de datos estadísticos y geoespaciales en el Laboratorio de Ciencia de Datos del Instituto Nacional de Estadística y Geografía, fue implementada una infraestructura computacional que permite transferir, recolectar, almacenar, procesar, transformar, integrar, visualizar información digital con niveles de seguridad y protección de datos como lo muestra la siguiente figura.

Diagrama

Descripción generada automáticamente

Figura 2. Infraestructura tecnológica implementada en laboratorio de ciencia de datos en INEGI [2].

A continuación, son descritos brevemente los componentes implementados en la infraestructura tecnológica en el Laboratorio de Ciencia de Datos del INEGI.

* Plataforma de cómputo On-premises y/o Nube hibrida: en el centro de cómputo está instalada una infraestructura local y remota con capacidades de almacenamiento, procesamiento y transferencia de datos estadísticos y geoespaciales que son recolectados de fuentes de información internas y externas.
* Acceso a datos (autenticación - autorización): para tener acceso a los datos, metadatos, microdatos, almacenados fueron generados perfiles de acceso con mecanismos para control de identidades.
* Interoperabilidad Grupo de trabajo especializado: dentro del Instituto hay personal (Analistas, Científicos, Investigadores) que tiene las habilidades y funciones para acceder a la tecnología computacional implementada para realizar procesos especializados en analítica y ciencia de datos estadísticos y geoespaciales.
* Ingeniería de procesos DevSecOps: grupos de trabajo especializados orientados a operar estrategias de desarrollo en ingeniería de procesos con estrategias de seguridad y privacidad de datos.
* Ingeniería de datos DataSecOps: grupos de trabajo especializados orientados a operar estrategias en relación con los datos, metadatos, microdatos utilizados para procesos de analítica y ciencia de datos.
* Procesos basados en Pipeline CI\CD: los grupos especializados en DevSecOps y DataSecOps, utilizan herramientas para generar una serie de pasos o etapas interconectadas que se utilizan para procesar y transformar grandes volúmenes de datos estadísticos y geoespaciales.
* Extracción, validación, carga de datos: proceso de recolección de información por medio de mecanismos como “web crawling descubre y mapea la web”, “web scraping extrae datos específicos de páginas web”, “web mining analiza los datos extraídos para obtener conocimiento”, por medio de Interfaz de Programación de Aplicaciones (API`s).
* Almacenamiento – Resguardo de datos: proceso que permite depositar datos digitales en tecnología de NAS – Almacenamiento conectado a Red, mediante protocolos especializados de comunicación.
* Homologación, Transformación de datos: la homologación de datos se refiere al proceso de unificar y estandarizar los datos provenientes de diversas fuentes o sistemas. Esto es crucial cuando los datos se recopilan de múltiples orígenes con formatos, unidades o nomenclaturas diferentes. El objetivo es crear un conjunto de datos coherente y comparable. La transformación de datos implica modificar los datos para prepararlos adecuadamente para el análisis. Este proceso puede involucrar una variedad de operaciones dependiendo de las necesidades específicas del proyecto.
* Integración de datos: proceso de combinar datos de diferentes fuentes para proporcionar una vista unificada y coherente. Este proceso es crucial cuando los datos provienen de múltiples sistemas, bases de datos, o formatos y se requiere un análisis conjunto para extraer información valiosa.
* Analítica y ciencia de datos: proceso de examinar conjuntos de datos para extraer conclusiones útiles y significativas. Este proceso incluye técnicas y métodos aplicados a diferentes datos para descubrir patrones, relaciones y tendencias mediante metodologías para hacer descripciones, diagnósticos, prescripciones, predicciones.
* Visualización de datos: proceso que permite generar la representación gráfica de la información y los datos mediante el uso de gráficos, diagramas y mapas para facilitar su comprensión y análisis.

Nota: para tener el contexto a detalle de los anteriores componentes están descritos en el artículo [2].

La estrategia de implementar Zero Trust [3] en la plataforma de procesos del Laboratorio de Ciencia de Datos se describe en la siguiente sección.

1. Estrategia de Implementación.

Esta sección, muestra la descripción de los componentes implementados en la plataforma tecnológica utilizada en el laboratorio de ciencia de datos.

La estrategia de implementar Zero Trust [3] hay que considerar los siguientes componentes.

Componente Identidades

Las identidades, ya sea que representen personas, servicios o dispositivos de IoT (internet de las cosas), definen el plano de control de Confianza Cero. Cuando una identidad intenta acceder a un recurso, debe verificarse con una autenticación sólida. Las directivas deben garantizar que el acceso cumpla con las normas, establecidas por las áreas involucradas considerando los principios de acceso con privilegios mínimos.

* Autenticación Multifactor (MFA): Implementar la autenticación multifactor para agregar una capa adicional de seguridad más allá de las contraseñas. Combinar factores como contraseñas, tokens físicos o virtuales, huellas dactilares y reconocimiento facial para autenticar usuarios.
* Gestión de Acceso Basada en Políticas (PAM): Utilizar soluciones de Gestión de Acceso Privilegiado (PAM) para controlar el acceso a recursos críticos. Implementar políticas granulares que limiten el acceso a lo estrictamente necesario.
* Control de acceso basado en roles (RBAC): Controlar el acceso que otorga privilegios a los usuarios en función de sus roles o responsabilidades internas - externas. Esto ayuda a que los usuarios solo tengan acceso a los recursos que necesitan para realizar sus actividades.
* Administración de identidades y acceso (IAM): Administrar las identidades y los privilegios de acceso de los usuarios, permitiendo que las identidades estén administradas, que los privilegios de acceso se otorguen con un ciclo de vida adecuado.
* Segmentación de red: Dividir la red en segmentos lógicos, lo que permite limitar el daño en caso de una brecha de seguridad. Los segmentos de red pueden basarse en factores como el rol del usuario, el área o la ubicación física.
* Control de Acceso Contextual: Utilizar información contextual, como la ubicación del usuario, dispositivo utilizado y hora del día, para evaluar el riesgo, determinando los niveles de acceso en relación con las actividades del usuario.
* Federación de Identidades: Permitir que los usuarios utilicen sus credenciales de inicio de sesión habituales en múltiples sistemas, servicios, microservicios. Esto reduce la necesidad de gestionar múltiples conjuntos de credenciales y simplifica la administración de identidades.
* Visibilidad y Monitorización Continua: Utilizar herramientas de monitoreo continuo para detectar comportamientos anómalos o actividades sospechosas en tiempo real. Implementar sistemas de información y eventos de seguridad (SIEM) para recopilar, analizar datos de registros de toda la red.
* Gestión de Identidades Privilegiadas: Aplicar una gestión estricta de identidades privilegiadas, verificando que solo las personas autorizadas tengan acceso a cuentas y recursos pertinentes. Utilizar soluciones de administración de identidades privilegiadas (PIM) para controlar, auditar este tipo de accesos.
* Automatización de Provisionamiento y Desprovisionamiento: Implementar procesos automáticos para el ciclo de vida de identidades generadas.
* Capacitación y Concientización: Instruir a los usuarios sobre la importancia de la seguridad de la identidad y la responsabilidad que conlleva. Promover el fortalecimiento de actividades para reducir riesgos en amenazas como la ingeniería social.
* Actualizaciones físicas y lógicas: Mantener los sistemas y aplicaciones para mitigar vulnerabilidades conocidas que podrían ser explotadas para comprometer la identidad de un usuario.
* Pruebas de Penetración y Evaluaciones de Seguridad: Realiza pruebas regulares de penetración y evaluaciones de seguridad para identificar posibles debilidades en la gestión de identidades y corregirlas antes de que puedan ser explotadas.

Componente Dispositivos

Conocer la identidad el acceso a un recurso, dispositivos IoT, smartphones, BYOD [BYOD, o Bring Your Own Device, significa "Trae tu propio dispositivo" en español], a dispositivos gestionados por terceros, así como también cargas de trabajo locales o en la nube. Esta diversidad de puntos de conexión, otros dispositivos crean una superficie en riesgos de ataque, a lo cual es pertinente tener herramientas, procesos para supervisar el estado del dispositivo y el cumplimiento para el acceso seguro.

* Inventario de Dispositivos: Mantener un inventario actualizado de todos los dispositivos conectados a la red. Utilizar herramientas de descubrimiento de activos para identificar automáticamente nuevos dispositivos lo cual permitirá mantener el inventario al día.
* Monitoreo Continuo: Establecer un monitoreo continuo del comportamiento en los dispositivos para detectar anomalías. Utilizar herramientas de análisis de comportamiento para identificar patrones sospechosos que podrían indicar una amenaza.
* Cifrado de Datos: Implementar el cifrado de datos en reposo y en tránsito para proteger la confidencialidad de la información, especialmente en dispositivos móviles y portátiles.
* Gestión de Incidentes: Desarrollar y practicar planes de respuesta a incidentes para abordar posibles violaciones de seguridad de manera ágil. Definir roles y responsabilidades para responder a incidentes que involucren dispositivos comprometidos.
* Acceso Basado en Políticas: Establecer políticas de acceso granulares basadas en roles para garantizar que cada dispositivo tenga acceso solo a los recursos necesarios para sus funciones. Evaluar y ajustar regularmente estas políticas según las necesidades operativas y de seguridad.
* Actualización de software y firmware: Los dispositivos deben actualizarse con las últimas correcciones de seguridad disponibles. Las actualizaciones de software y firmware pueden corregir vulnerabilidades que pueden ser explotadas por los atacantes.
* Control de acceso a dispositivos (DAC): Controlar quién puede acceder y usar dispositivos específicos.
  + Soluciones de seguridad móvil: Proteger los dispositivos móviles contra malware, ransomware y otras amenazas.
  + Soluciones de seguridad de end-points: Proteger los dispositivos de escritorio y portátiles contra malware, ransomware y otras amenazas.
  + Soluciones de seguridad de IoT: Proteger los dispositivos IoT contra malware, ransomware y otras amenazas.

Componente Datos

Los datos deben permanecer seguros, dentro/fuera de los dispositivos, aplicaciones, infraestructura y redes, esta protección comienza con la capacidad de identificar, clasificar y etiquetar datos confidenciales para que se puedan aplicar las directivas correspondientes de forma automatizada.

* Identificación y Clasificación: Realizar una evaluación exhaustiva de los datos para comprender su naturaleza y sensibilidad. Clasificar los datos según su importancia y riesgo.
* Políticas de Acceso Granulares: Implementar políticas de acceso detalladas basadas en la clasificación de datos y las funciones del usuario. Asignar permisos mínimos necesarios para realizar tareas específicas.
* Encriptación End-to-End: Utilizar la encriptación para proteger los datos tanto en reposo como en tránsito. Implementar soluciones de encriptación robustas y actualizadas
* Análisis de Comportamiento: Implementar herramientas de análisis de comportamiento para detectar patrones anómalos en el acceso y uso de datos. Realizar monitoreo continuo de actividades relacionadas con datos sensibles.
* Registros Detallados: Mantener registros detallados de todas las interacciones con datos sensibles. Realizar auditorías regulares para garantizar el cumplimiento de las políticas de seguridad.
* Detección de Amenazas Internas: Utilizar tecnologías avanzadas para detectar y mitigar amenazas internas. Realizar evaluaciones periódicas de riesgos internos. Nota: Usar la inteligencia artificial (IA) y el aprendizaje automático (ML) para detectar y responder a amenazas potenciales, identificando actividad sospechosa que podría indicar una violación de seguridad.
* Controles de Acceso en la Nube: Implementar controles de acceso sólidos para los datos almacenados en entornos de nube hibrida. Utilizar herramientas de cifrado y gestión de claves en la nube.
* Soluciones Unificadas: Implementar soluciones integradas que aborden la seguridad de datos desde múltiples frentes. Integrar sistemas de prevención de pérdida de datos (DLP), firewalls, y sistemas de gestión de identidades.

Componente Aplicaciones

Las aplicaciones de tipo SaaS [Software como servicio], deberán aplicar controles y tecnologías para descubrir “Shadow IT", garantizar los permisos correspondientes en la aplicación, limitar el acceso en función de análisis en tiempo real, supervisar el comportamiento anormal, controlar las acciones de los usuarios y validar las opciones de configuración seguras.

* Segregación de Aplicaciones: Dividir las aplicaciones en categorías según su sensibilidad y función. Aplicar políticas de acceso más estrictas a las aplicaciones críticas o sensibles.
* Evaluación de Riesgos Continua: Realizar evaluaciones de riesgos continuas para identificar y abordar posibles brechas de seguridad en las aplicaciones. Ajustar las políticas de seguridad según las cambiantes condiciones y amenazas.
* Control de acceso basado en riesgos: El acceso a las aplicaciones debe controlarse en función del riesgo asociado a cada usuario, dispositivo o aplicación. El tráfico de las aplicaciones debe inspeccionarse para detectar amenazas, como malware o intrusiones.
* Inspección de tráfico de aplicaciones: El tráfico de las aplicaciones debe inspeccionarse para detectar amenazas, como malware o intrusiones, utilizando firewalls de aplicaciones web (WAF) para inspeccionar el tráfico de las aplicaciones en busca de amenazas conocidas. Los WAF también pueden bloquear el tráfico malicioso antes de que llegue a las aplicaciones. Nota: La autenticación y autorización estrictas son esenciales para proteger las aplicaciones en un entorno Zero Trust [3]. Utilizar MFA para autenticar a los usuarios que intentan acceder a las aplicaciones. MFA agrega una capa adicional de seguridad al requerir que los usuarios proporcionen dos o más factores de autenticación, como una contraseña, una huella digital o un código de verificación enviado por correo electrónico. Implementar una política de privilegios mínimos para las aplicaciones. Esto significa que las aplicaciones solo deben tener los privilegios que necesitan para funcionar. Los privilegios excesivos pueden dar a los atacantes una oportunidad de comprometer las aplicaciones.

Componente Infraestructura

Los servidores locales/remotos, máquinas virtuales, contenedores hospedados en los centros de datos es pertinente implementar herramientas para evaluar las versiones, la configuración, el acceso "Just-In-Time", la telemetría es clave para detectar ataques, anomalías, bloquear, marcar automáticamente el comportamiento de riesgo y tomar medidas de protección.

* Políticas de Menor Privilegio (PoLP): Limitar los privilegios de acceso a lo estrictamente necesario para realizar las funciones asignadas. Minimiza el riesgo de movimientos laterales en caso de compromiso.
* Respuesta Automatizada a Amenazas: Implementar soluciones de respuesta automática para mitigar amenazas en tiempo real. Responder de manera automática a comportamientos maliciosos según las políticas establecidas.
* Implemente el acceso Just-in-time (JIT) y el acceso con Privilegios mínimos (PMM). Permite que los usuarios solo tengan acceso a los recursos que necesitan para realizar las actividades pertinentes.

Componente Redes

Las redes deben estar segmentadas (incluida la microsegmentación más profunda en la red), contar con protección contra amenazas en tiempo real, cifrado de extremo a extremo, supervisión y análisis.

* Control de acceso a red (NAC): Controlar quién puede acceder a una red. Autenticación explícita; todo lo que intente conectarse debe verificarse para que se le conceda acceso. Uso del acceso con privilegios mínimos; se debe asumir que existe una brecha de seguridad y tomar medidas para mitigar los riesgos.
* Aislamiento de Recursos Sensibles: Aislar, proteger los recursos críticos, sensibles mediante la implementación de capas adicionales de seguridad.
* Análisis Forense y Respuesta a Incidentes: Desarrollar un plan de respuesta a incidentes que incluya la capacidad de realizar análisis forenses para comprender y mitigar los incidentes de seguridad de manera ágil, eficaz y eficiente.
* Pruebas de Penetración Continuas: Identificar posibles vulnerabilidades y evaluar la eficacia de las medidas de seguridad implementadas.
* Considerar los métodos en segmentación
  + Segmentación basada en VLAN: dividir la red en función del tráfico de red.
  + Segmentación basada en Políticas: dividir la red en función de las reglas de seguridad.
  + Segmentación basada en Dispositivos: dividir la red en función de los tipos de dispositivos que se conectan a ella.

Nota: Cada segmento tiene reglas de seguridad específicas que determinan qué tipo de tráfico está permitido y qué tipo está bloqueado. La técnica reduce la superficie de ataque y mejora la seguridad al limitar el movimiento lateral de los atacantes si logran infiltrarse en la red.

Ejemplos de segmentación

* Aplicaciones: Se pueden crear segmentos específicos para aplicaciones críticas. Por ejemplo, una base de datos puede estar en un segmento separado de la aplicación web que accede a esa base de datos. Esto asegura que solo el tráfico necesario se permita entre estos componentes.
* Usuarios: Los usuarios dentro de la red pueden ser agrupados en segmentos según sus roles y responsabilidades. Cada segmento puede tener reglas específicas que limitan el acceso a recursos sensibles, reduciendo así el riesgo de acceso no autorizado.
* Entornos de desarrollo, prueba y producción: Cada entorno puede tener su propio segmento, asegurando que el tráfico entre ellos esté estrictamente controlado. Esto evita que eventualidades en entornos menos seguros afecten a entornos más críticos.
* Niveles de sensibilidad de datos: La información sensible puede estar en segmentos separados con reglas estrictas para que solo los sistemas y usuarios autorizados puedan acceder a esos datos.
* Basada en la ubicación geográfica: Considerar sucursales o ubicaciones geográficas diversas, se pueden implementar segmentos específicos para cada ubicación, con reglas que controlan la comunicación entre ellas.
* Activar el control de acceso basado en roles (RBAC) es una forma de otorgar acceso a los recursos de la red en función del rol del usuario o dispositivo.
  + La autenticación de usuarios proporciona una forma de identificar a los usuarios que intentan acceder a la red.
  + La asignación de roles asocia los usuarios con roles específicos, que determinan los privilegios de acceso que tienen.
  + La autenticación de dos factores (2FA) agrega una capa adicional de seguridad al requerir dos factores de autenticación para acceder a la red. El primer factor suele ser una contraseña o token, y el segundo factor puede ser un código enviado a un dispositivo móvil o una huella digital.

CONCLUSIONES

En el panorama actual de la ciencia de datos, la necesidad de una infraestructura responsiva y segura es más crítica que nunca. La adopción del modelo de Zero Trust (Confianza Cero) [3], en la gestión de procesos automatizados representa un avance significativo hacia la protección de datos y la mitigación de riesgos. Este enfoque asegura que cada acceso, movimiento y cambio dentro del sistema esté rigurosamente controlado y verificado, eliminando las suposiciones de confianza implícitas.

La infraestructura responsiva habilitada por Zero Trust [3] no solo mejora la seguridad, sino que también optimiza la eficiencia operacional. Al integrar políticas de seguridad directamente en la automatización de procesos, las organizaciones pueden reaccionar de manera ágil a las amenazas emergentes y a las cambiantes necesidades del negocio. Este enfoque es especialmente beneficioso en la ciencia de datos, donde la integridad y la disponibilidad de la información son esenciales para el éxito de los proyectos.

La combinación de infraestructuras responsivas con principios de Zero Trust [3] proporciona un marco robusto y adaptable que aborda los desafíos de seguridad y eficiencia en la ciencia de datos. Esta sinergia no solo fortalece la postura de seguridad de las organizaciones, sino que también impulsa la innovación y la competitividad en un entorno global cada vez más digitalizado. Adopción de estas prácticas se traduce en una ventaja estratégica, asegurando que las operaciones de ciencia de datos se mantengan seguras, eficientes y resilientes frente a las amenazas del futuro.

Las herramientas especializadas de tipo “open source”, están documentadas en el siguiente repositorio.

<https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Cumplimientos/zero-trust.md>

Agradecimientos

Al equipo de trabajo conformado por CIMAT A.C. Unidad Zacatecas, México e INEGI, por el compromiso de generar conocimiento para enriquecer a las organizaciones, empresas y la experiencia académica.

Referências Bibliográfica

1. Diaz, E. O. & Muñoz, M. (2020). Strategy for Performing Critical Projects in a Data Center Using DevSecOps Approach and Risk Management. International Journal of Information Technologies and Systems Approach (IJITSA), 13(1), 61-73. DOI:10.4018/IJITSA.2020010104.
2. E. A. Villaseñor García et al., "Data Lake Strategy for Data Science Workflows," 2022 11th International Conference On Software Process Improvement (CIMPS), Acapulco, Guerrero, Mexico, 2022, pp. 219-223, DOI: 10.1109/CIMPS57786.2022.10035694.
3. Zero Trust Architecture (ZTA): Aunque no es una norma internacional, el Grupo de Trabajo de Zero Trust del Instituto de Estándares de Internet (IETF) está trabajando en un conjunto de documentos y estándares relacionados con la arquitectura Zero Trust.
4. Liu, C., Tan, R., Wu, Y. et al. Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity 7, 20 (2024). <https://doi.org/10.1186/s42400-024-00212-0>
5. Seaman, Jim. (2023). Zero Trust Security Strategies and Guideline. 10.1007/978-3-031-09691-4\_9.
6. Garbis, Jason & Chapman, Jerry. (2021). Zero Trust Security: An Enterprise Guide. 10.1007/978-1-4842-6702-8.
7. Sarkar, Sirshak & Choudhary, Gaurav & Shandilya, Shishir K & Hussain, Azath & Kim, Hwankuk. (2022). Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability. 14. 11213. 10.3390/su141811213.
8. Alawneh, Muntaha & Abbadi, Imad. (2023). Approaches for Zero Trust Adoption Based upon Organization Security Level. 10.1007/978-981-99-0272-9\_36.
9. Cheng, Ruizhi & Chen, Songqing & Han, Bo. (2023). Towards Zero-trust Security for the Metaverse.
10. Rose, S. , Borchert, O. , Mitchell, S. and Connelly, S. (2020), Zero Trust Architecture, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], 10.6028/NIST.SP.800-207