



TALLER DESCRIPTIVO EN SEGURIDAD Y PRIVACIDAD DE DATOS ESTADÍSTICOS Y GEOESPACIALES

Temario

- Panorama general.
- Arquitectura Zero Trust.
- Estrategia de ciberseguridad basada en IA y ML.



Panorama general

La magnitud y la sensibilidad de la información utilizada para procesos relacionados con analítica y ciencia de datos permite generar indicadores cualitativos – cuantitativos para la toma de decisiones, de tal forma la confianza en la integridad, disponibilidad, confidencialidad de los datos que se recopilan, almacenan, procesan, visualizan.

La globalización de las amenazas ciberneticas y la creciente sofisticación de los ataques informáticos han elevado el nivel de atención que se debe prestar a la seguridad de los datos. La gestión eficiente de estos riesgos se convierte así en un componente esencial para preservar la integridad de las estadísticas producidas y, por ende, la credibilidad de las instituciones estadísticas internacionales.

En este contexto, en el taller exploraremos los desafíos, las estrategias claves relacionadas con la seguridad y privacidad de datos, examinando las mejores prácticas, normativas, tecnologías emergentes que permiten fortalecer la protección de la información, garantizando al mismo tiempo el acceso oportuno, eficiente para la elaboración de análisis de grandes volúmenes de datos estadísticos y geoespaciales.

El **JTF** [Joint Task Force, o Fuerza de Tarea Conjunta], define la ciberseguridad como una "disciplina basada en la informática que involucra tecnología, personas, información y procesos para permitir operaciones seguras. Implica la creación, operación, análisis y prueba de sistemas informáticos seguros. Es un estudio interdisciplinario, que incluye aspectos del derecho, las políticas, los factores humanos, la ética y la gestión de riesgos en el contexto de los adversarios". (Definición de trabajo de la JTF, establecida el 7 de diciembre de 2015).

Puntos a considerar:

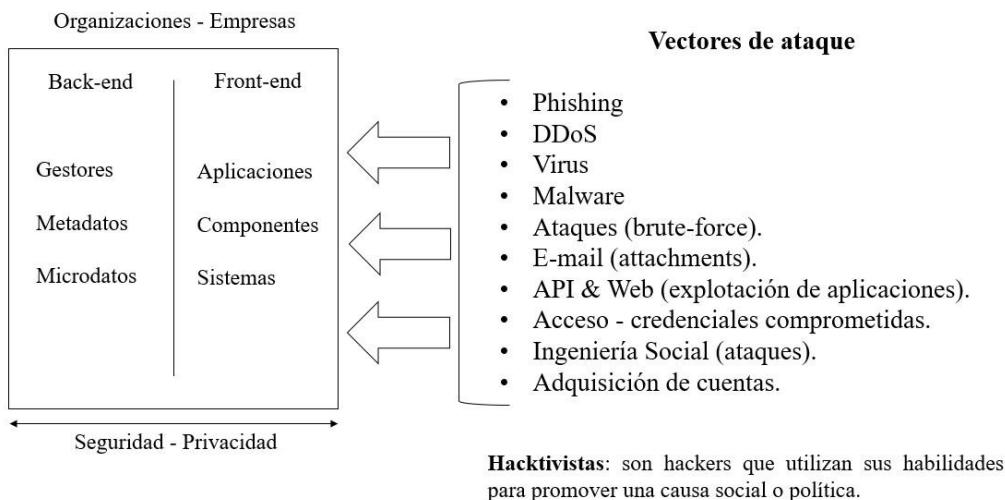
- | | |
|--|---|
| <ul style="list-style-type: none">• Personas [Entrenamiento, Conocimiento, Hábitos]• Procesos [Ágiles, Documentados]• Tecnologías [Eficaz, Autoadministrado] | <p>Seguridad en:</p> <ul style="list-style-type: none">• Datos• Software• Componentes• Conexión• Sistemas• Humanos• Organizaciones• Sociedad |
|--|---|



Estadísticas

- El volumen mundial de ataques de malware aumentó un 20% en 2023, con un total de 2,5 billones de ataques. Los tipos de malware más comunes fueron los programas espía (35 %), los troyanos (23 %) y los ransomware (17 %).
- El ransomware es un tipo de malware que cifra los datos de una víctima y exige un rescate a cambio de la clave de descifrado. Los ataques de ransomware aumentaron un 83 % en 2023, con un total de 154,9 millones de ataques. Las industrias más afectadas por los ataques de ransomware fueron las de servicios financieros (20 %), la atención médica (19 %) y el gobierno (17 %).
- Los ataques cibernéticos dirigidos a dispositivos de Internet de las cosas (IoT), aumentó un 87 % en 2023, con un total de 112 millones de ataques. Los tipos de ataques de IoT más comunes fueron los ataques de denegación de servicio (DoS & DDoS - múltiples) (42 %), los ataques de escaneo de puertos (36 %) y los ataques de fuerza bruta (22 %).

Symantec Corporation. (2023). recuperado de <https://www.symantec.com/>





Malware es una abreviatura de "software malicioso" (del inglés "malicious software"). Se refiere a cualquier tipo de software o programa informático diseñado con la intención de dañar, robar información, controlar o acceder de manera no autorizada a sistemas informáticos, dispositivos o redes.

Algunos ejemplos comunes de malware incluyen:

- **Virus:** Programas que se adjuntan a archivos legítimos y se propagan cuando estos archivos se ejecutan. Los virus pueden dañar archivos y programas en el sistema.
- **Gusanos (Worms):** Son programas que se replican a sí mismos y se propagan a través de redes, a menudo explotando vulnerabilidades en sistemas sin necesidad de intervención del usuario.
- **Troyanos (Trojans):** Se disfrazan como programas legítimos para engañar a los usuarios y permiten a los atacantes obtener acceso no autorizado al sistema o robar información.
- **Spyware:** Se utiliza para recopilar información personal del usuario, como contraseñas, historial de navegación o datos bancarios, sin su conocimiento o consentimiento.
- **Ransomware:** Cifra los archivos del usuario y exige un rescate para descifrarlos y recuperar los datos. Un ejemplo famoso es WannaCry.Adware: Muestra anuncios no deseados en el sistema del usuario y, a menudo, se instala junto con aplicaciones gratuitas.

https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Conceptos/Malware_vectores_ataque.md

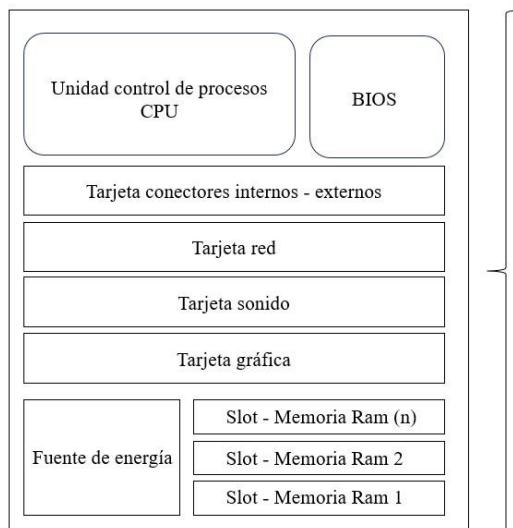
La **ingeniería social** es un conjunto de técnicas que utilizan los cibercriminales para engañar a las personas para que revelen información confidencial o realicen acciones que les permitan acceder a sistemas informáticos o redes.

- **Robo de Identidad:** Un atacante puede hacerse pasar por una entidad de confianza, como un banco o una agencia gubernamental, para obtener información personal de una persona, como números de seguridad social, números de tarjetas de crédito y contraseñas. Posteriormente, esta información se utiliza para cometer fraude financiero o robo de identidad.
- **Phishing:** Los correos electrónicos o sitios web falsos se utilizan para engañar a las personas y hacer que revelen sus credenciales de inicio de sesión. Por ejemplo, un correo electrónico que parece ser de una empresa de renombre podría pedir a los destinatarios que ingresen sus nombres de usuario y contraseñas, que luego se utilizan para acceder a cuentas en línea.
- **Ataques de Ingeniería Social en Redes Sociales:** Los atacantes pueden crear perfiles falsos en redes sociales y establecer relaciones de confianza con personas. Luego, pueden utilizar esta relación para engañar a las víctimas y obtener información confidencial o extorsionarlas.
- **Suplantación de Identidad en Llamadas Telefónicas:** Los delincuentes pueden hacerse pasar por empleados de servicio al cliente, técnicos de soporte o incluso parientes en llamadas telefónicas. Pueden solicitar información personal o financiera, o incluso persuadir a las personas para que realicen transacciones financieras.
- **Acceso no autorizado a edificios e instalaciones:** En entornos físicos, los ingenieros sociales pueden hacerse pasar por empleados, contratistas o visitantes legítimos para ganar acceso a edificios o instalaciones seguras. Esto puede facilitar robos, espionaje o sabotaje.
- **Secuestro de cuentas de redes sociales:** Los atacantes pueden engañar a las víctimas para que revelen contraseñas o información de recuperación de cuentas de redes sociales. Luego, pueden asumir el control de esas cuentas, lo que puede tener un impacto significativo en la privacidad y la reputación de la víctima.
- **Obtención de información confidencial de empleados:** Los ingenieros sociales pueden apuntar a empleados de una organización para obtener acceso a información sensible o sistemas internos. Esto podría incluir persuadir a un empleado para que revele credenciales de acceso o detalles sobre la infraestructura de la empresa.
- **Manipulación en el lugar de trabajo:** Los atacantes pueden hacerse pasar por colegas o supervisores para obtener información privilegiada o lograr que los empleados realicen acciones que no están autorizados a hacer, como transferir fondos o proporcionar datos confidenciales de la empresa.
- **Obtención de información de celebridades o figuras públicas:** Los ingenieros sociales a menudo apuntan a figuras públicas o celebridades para obtener acceso a sus cuentas de redes sociales o información personal. Esto puede llevar a la difusión de información comprometedora o el chantaje.

https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Conceptos/ingenier%C3%ADA_social.md



Componentes físicos



Modelo OSI capas:

- 1 Física.
- 2 de Enlace de Datos.
- 3 de Red.
- 4 de Transporte.
- 5 de Sesión.
- 6 de Presentación.
- 7 de Aplicación.

https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Conceptos/OSI_model.md

El **Modelo de Referencia OSI (Open Systems Interconnection)** es un marco conceptual que se utiliza para comprender y estandarizar cómo se comunican los dispositivos en una red de computadoras.

Capa 1 Física: la capa más baja del modelo y se encarga de la transmisión de datos en forma de señales eléctricas, ópticas o electromagnéticas a través del medio físico, como cables de cobre, fibra óptica o transmisiones inalámbricas. En esta capa, se determina cómo se transmiten los bits, la topología de la red y los voltajes requeridos para la transmisión. En esencia, esta capa se ocupa de la conexión física entre dispositivos.

Capa 2 de Enlace de Datos: se encarga de la transferencia confiable de datos entre dos dispositivos directamente conectados. Controla el flujo de datos, detecta y corrige errores, y maneja la dirección MAC (Media Access Control). También divide los datos en tramas para su transmisión.

Capa 3 de Red: responsable de la gestión del enruteamiento de datos a través de la red. Aquí se determinan las rutas óptimas para el tráfico de datos y se utilizan protocolos como el IP (Internet Protocol) para direccionar y enrutar los paquetes de datos a través de la red.

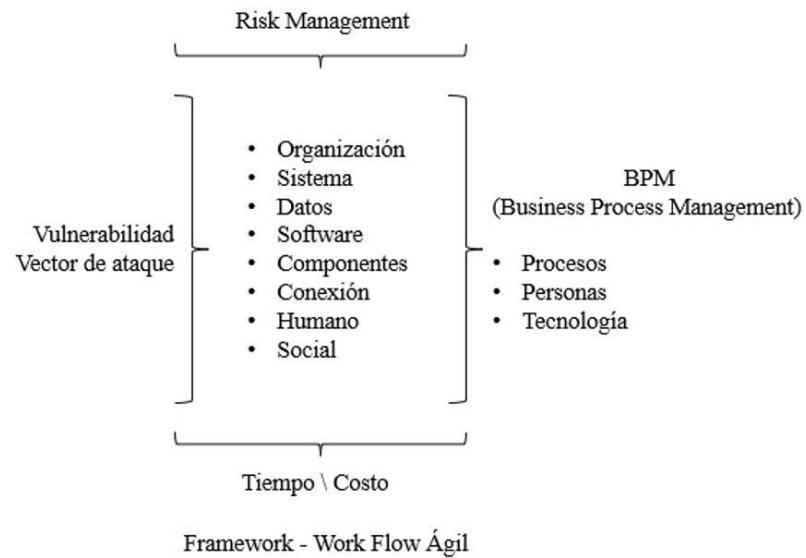
Capa 4 de Transporte: garantiza la entrega de datos extremo a extremo, administrando la segmentación y reensamblaje de los datos, y proporcionando control de flujo y detección de errores. Los protocolos comunes en esta capa incluyen TCP (Transmission Control Protocol) y UDP (User Datagram Protocol).

Capa 5 de Sesión: establece, administra y finaliza las sesiones de comunicación entre dos dispositivos. Se encarga de la sincronización y el control del diálogo entre las aplicaciones, lo que permite la comunicación eficiente.

Capa 6 de Presentación: se encarga de la representación de datos, lo que incluye la codificación y decodificación, la compresión y el cifrado de datos. Esta capa asegura que los datos sean legibles y comprensibles entre dispositivos con diferentes formatos de datos.

Capa 7 de Aplicación: es la capa superior del Modelo OSI y se encarga de proporcionar interfaces a las aplicaciones y servicios de red. Aquí se ejecutan programas y aplicaciones que utilizan la red para la comunicación, como navegadores web, clientes de correo electrónico y transferencia de archivos. Los protocolos de aplicación, como HTTP, SMTP y FTP, operan en esta capa.

https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Conceptos/OSI_model.md



Arquitectura Zero Trust



La Arquitectura Zero Trust (Confianza Cero) 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 son:

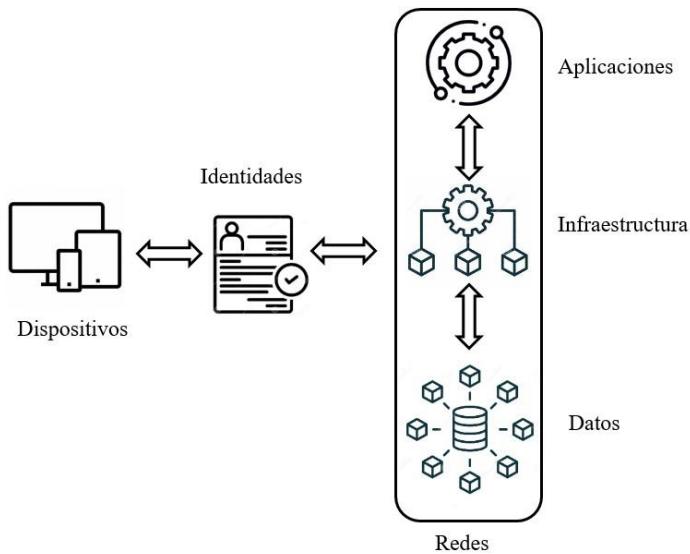
- **Verificar explícitamente:** autenticar y autorizar siempre en función de todos los puntos de controles disponibles, incluida la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.
- **Utilizar el acceso con 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?

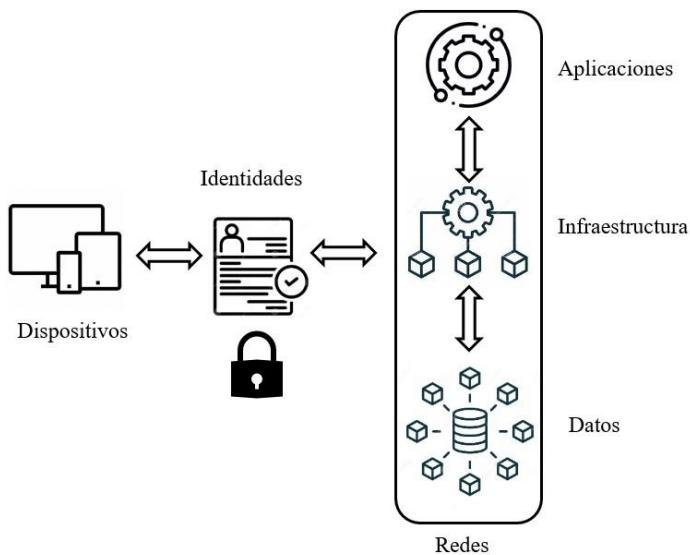
- Permite tener un control del crecimiento de personas, procesos, tecnología, con soluciones ágiles para el control en reducir riesgos internos y externos.
- Permite proteger un volumen creciente de datos en un entorno multiplataforma + multinube híbrida, aporta a simplificar la seguridad con una estrategia, 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.



Arquitectura Zero Trust



Arquitectura Zero Trust





Identidades

Las identidades, ya sea que representen personas, servicios o dispositivos de IoT, 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.

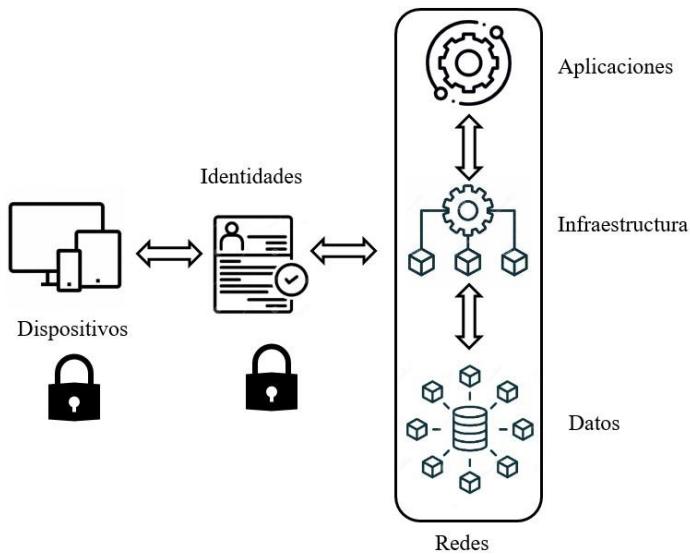
- **Autenticación Multifactor (MFA):** Implementar la autenticación multifactor para agregar una capa adicional de seguridad más allá de las contraseñas. Combinar factores como contraseñas, tokens físicos o virtuales, huellas dactilares y reconocimiento facial para autenticar usuarios.
- **Gestión de 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 a 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.



Arquitectura Zero Trust



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.



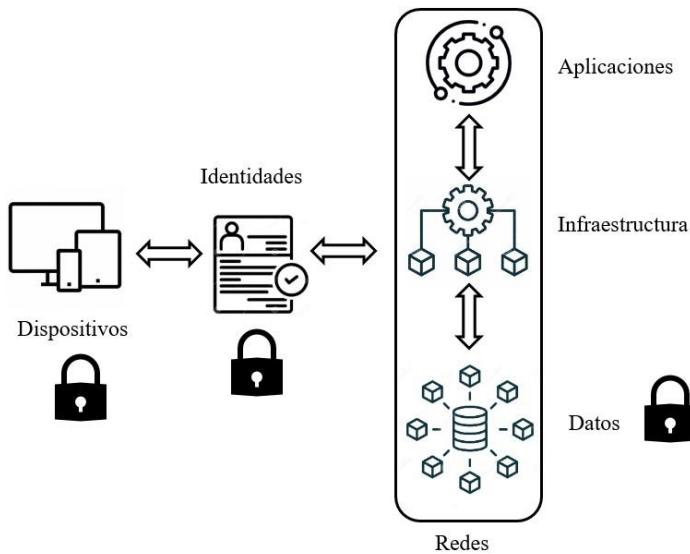
- **Gestión de Incidentes:** Desarrollar y practicar planes de respuesta a incidentes para abordar posibles violaciones de seguridad de manera ágil. Definir roles y responsabilidades para responder a incidentes que involucren dispositivos comprometidos.
- **Acceso Basado en Políticas:** Establecer políticas 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.



Arquitectura Zero Trust



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.

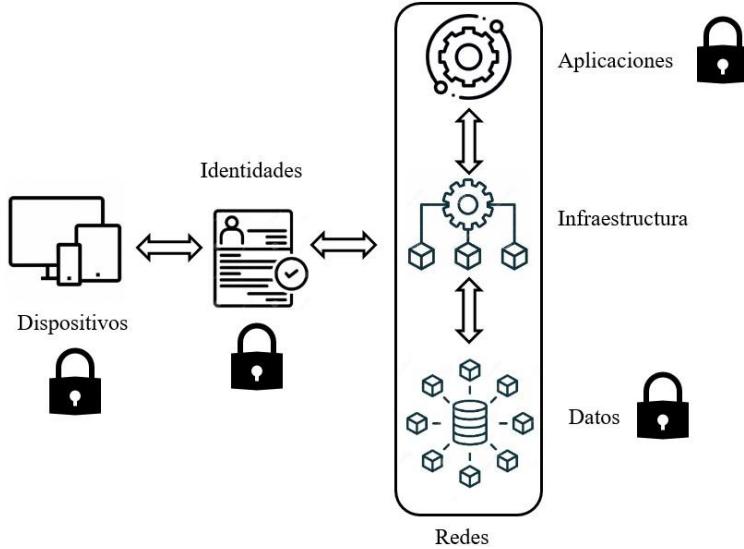


- **Análisis de Comportamiento:** Implementar herramientas de análisis de comportamiento para detectar patrones anómalos en el acceso y uso de datos. Realizar monitoreo continuo de actividades relacionadas con datos sensibles.
- **Registros Detallados:** Mantener registros detallados de todas las interacciones 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 híbrida. 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.

Arquitectura Zero Trust





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.

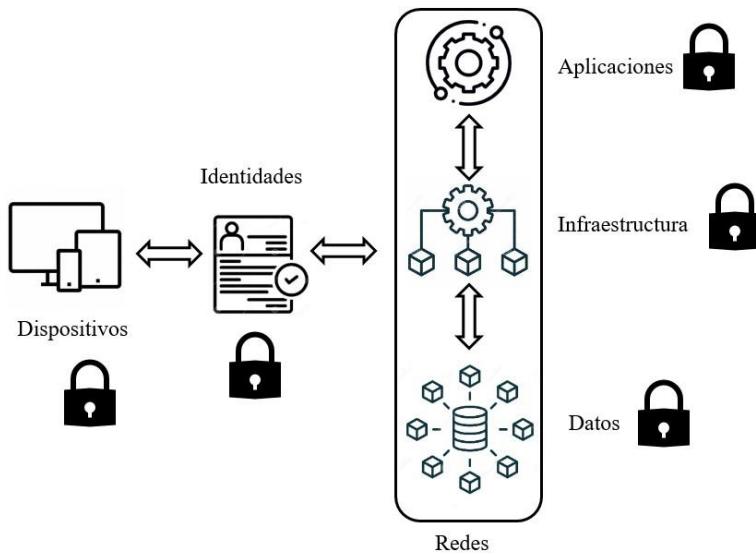
Control de acceso basado en riesgos: El acceso a las aplicaciones debe controlarse en función del riesgo asociado a cada usuario, dispositivo o aplicación. El tráfico de las aplicaciones debe inspeccionarse para detectar amenazas, como malware o intrusiones.

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. 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.



Arquitectura Zero Trust



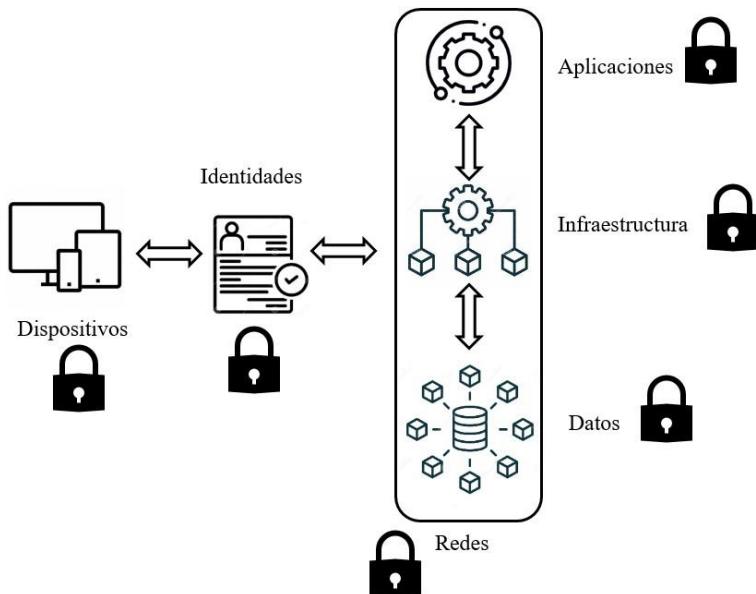
Infraestructura

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.



Arquitectura Zero Trust



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. Esta técnica reduce la superficie de ataque y mejora la seguridad al limitar el movimiento lateral de los atacantes en caso de que logren infiltrarse en la red.

Ejemplos de segmentación

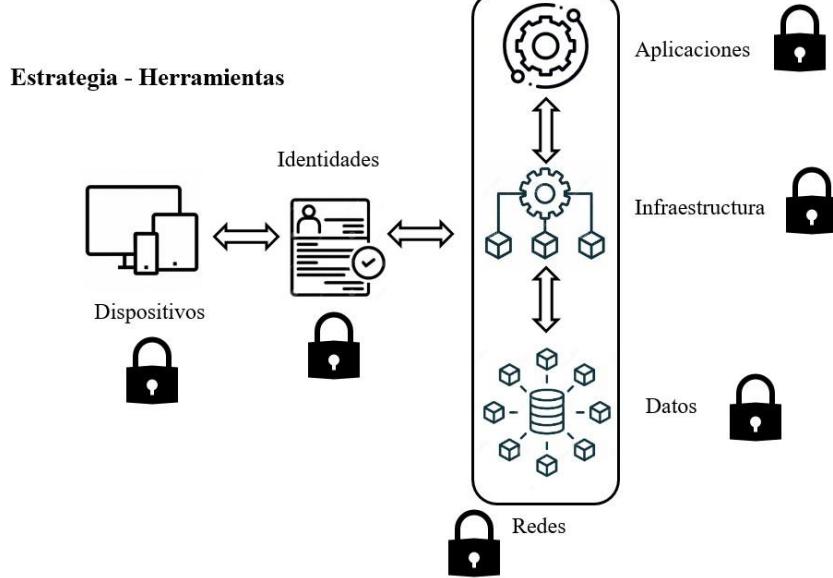
- **Aplicaciones:** Se pueden crear segmentos específicos para aplicaciones críticas. Por ejemplo, una base de datos puede estar en un segmento separado de la aplicación web que accede a esa base de datos. Esto asegura que solo el tráfico necesario se permita entre estos componentes.
- **Usuarios:** 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.

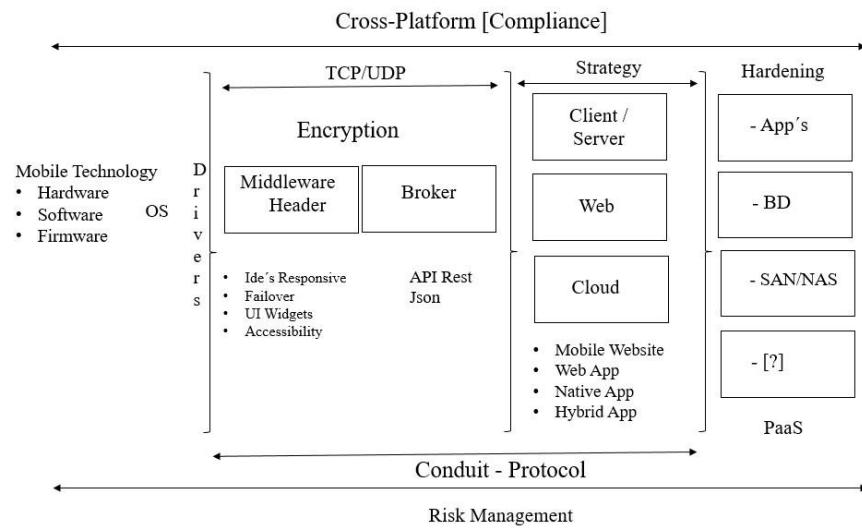
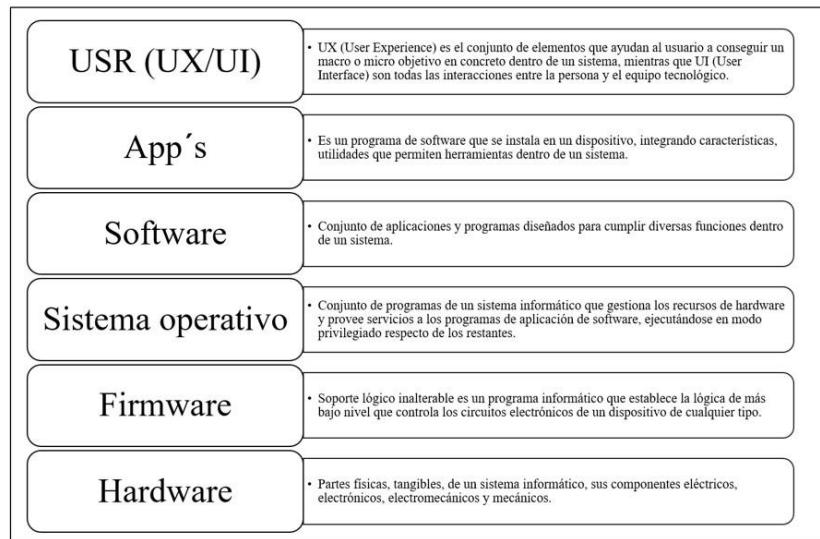
- ✓ La autenticación de usuarios proporciona una forma de identificar a los usuarios que intentan acceder a la red.
- ✓ La asignación de roles asocia los usuarios con roles específicos, que determinan los privilegios de acceso que tienen.
- ✓ La autenticación de dos factores (2FA) agrega una capa adicional 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.

Arquitectura Zero Trust



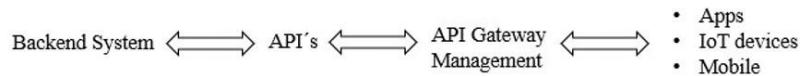


Host





Application Programming Interface - API



Transferencia de Estado Representacional (REST)

- GET: Recupera un recurso.
- POST: Crea un nuevo recurso.
- PUT: Actualiza un recurso existente.
- PATCH: Actualiza un recurso existente de forma parcial.
- DELETE: Elimina un recurso existente.
- HEAD: Recupera el encabezado de respuesta de un recurso, pero no el contenido del recurso.
- OPTIONS: Obtiene información sobre los métodos HTTP que se admiten para un recurso.
- CONNECT: Establece una conexión entre dos hosts.
- TRACE: Devuelve una copia de la solicitud original.

Un API gateway es una herramienta de gestión de API que se encuentra entre un cliente y una colección de servicios de back-end. El API gateway actúa como un proxy inverso para aceptar todas las llamadas API, agrupar los diversos servicios necesarios para cumplirlas y devolver el resultado apropiado.

https://git.inegi.org.mx/oswaldo.diaz/ciberseguridad/-/blob/master/Cumplimientos/API_s.md

Normas internacionales

- Zero Trust Architecture (ZTA): el Grupo de Trabajo del Instituto de Estándares de Internet (IETF) está trabajando en un conjunto documentos y estándares relacionados con la arquitectura.
- ISO 27001: Estándar internacional para la gestión de la seguridad de la información, proporciona un marco sólido para establecer políticas y procedimientos de seguridad que pueden ser integrados en un enfoque Zero Trust.
- NIST Cybersecurity Framework: El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ofrece pautas y mejores prácticas para la gestión de la seguridad cibernética. Principios de confianza cero.
- GDPR (Reglamento General de Protección de Datos): Unión Europea, establece requisitos específicos de protección de datos y privacidad.
- PCI DSS (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago): estándares de seguridad para implementarse en el uso de Información de tarjetas de pago.



Modelo OWASP SAMM

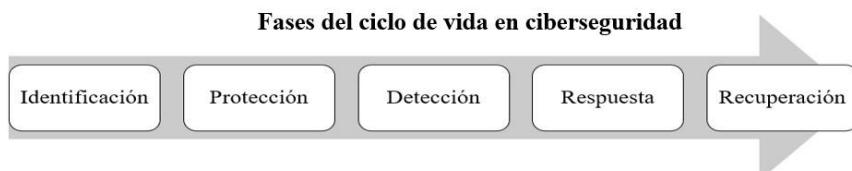
Políticas, procedimientos, educación y conciencia en seguridad

Gobernanza	Diseño	Implementación	Verificación	Operaciones
• <u>Estrategia y Métricas</u>	• <u>Evaluación de amenazas</u>	• <u>Construcción segura</u>	• <u>Evaluación de Arquitectura</u>	• <u>Gestión de incidencias</u>
• <u>Política y cumplimiento</u>	• <u>Requisitos de seguridad</u>	• <u>Implementación segura</u>	• <u>Pruebas basadas en requisitos</u>	• <u>Gestión del Medio Ambiente</u>
• <u>Educación y Orientación</u>	• <u>Arquitectura de seguridad</u>	• <u>Gestión de defectos</u>	• <u>Pruebas de seguridad</u>	• <u>Gestión Operativa</u>

Estrategia de ciberseguridad basada en IA y ML.



Estrategia de ciberseguridad basada en IA y ML.



Identificación: se refiere al proceso de reconocer y clasificar activos, vulnerabilidades y amenazas en un entorno digital, crear un inventario detallado de todos los activos de información, incluyendo hardware, software, datos, usuarios, posibles vulnerabilidades, amenazas que podrían afectar la seguridad de estos activos.

Protección: se refiere a la implementación de medidas para salvaguardar los activos de información identificados, incluye controles de seguridad, como firewalls, antivirus, sistemas de prevención de intrusiones, políticas de acceso y cifrado de datos, entre otros.

Detección: implica la identificación temprana de eventos o actividades sospechosas que podrían indicar una amenaza de seguridad utilizando sistemas de monitoreo y análisis de registros (logs - bitácoras) para detectar patrones anómalos, implementando análisis de comportamiento, inteligencia artificial y aprendizaje automático para identificar actividades maliciosas de forma ágil.

Respuesta: se activa cuando se confirma un incidente de seguridad. Implica la ejecución de planes de acción predefinidos para contener y mitigar la amenaza. Esto puede incluir la desconexión de sistemas comprometidos, la aplicación de procesos sistematizados de seguridad, la restauración de datos desde copias de seguridad y la colaboración con organismos de aplicación de la ley regulatoria establecida en el entorno geográfico.

Recuperación: se centra en restaurar la operatividad normal después de un incidente de seguridad. Esto incluye la restauración de sistemas, datos desde copias de seguridad, la revisión, mejora de las políticas, procedimientos de seguridad, la implementación de lecciones aprendidas para fortalecer la postura de ciberseguridad en el futuro.



Ventajas

- Mejora en la velocidad de detección y respuesta.
- Reducción de falsos positivos y negativos.
- Análisis predictivo para anticipar amenazas potenciales.
- Automatización de tareas rutinarias, liberando recursos humanos para tareas más estratégicas.

Implementación de una estrategia de ciberseguridad basada en Inteligencia Artificial (IA) y Aprendizaje Automático (ML).

- Recolectar datos relevantes de eventos de seguridad, registros de actividad, amenazas y cualquier otra información relacionada con la seguridad.
- Integrar datos externos, como feeds de amenazas, bases de datos de vulnerabilidades y otros recursos de inteligencia de amenazas.
- Validar que los datos estén en un formato consistente y normalizarlos para facilitar el análisis.
- Identificar y eliminar datos irrelevantes o ruido que pueda afectar la calidad del modelo.



- Determinar si se utilizarán algoritmos supervisados o no supervisados según la naturaleza de los datos y los objetivos de seguridad.
 - Seleccionar algoritmos de ML, como máquinas de soporte vectorial (SVM), bosques aleatorios, redes neuronales, entre otros., según los requisitos específicos del entorno de ciberseguridad.
 - Utilizar un conjunto diverso y representativo de datos para entrenar el modelo.
 - Verificar la precisión y eficacia del modelo utilizando datos de validación y técnicas de validación cruzada.
-
- Integrar el modelo en tiempo real con sistemas de detección de intrusiones, firewalls y otros componentes de seguridad para tomar decisiones en tiempo real.
 - Implementar mecanismos que permitan que el modelo aprenda y se adapte continuamente a medida que evolucionan las amenazas.
 - Mantener actualizados los modelos y las reglas de seguridad para abordar nuevas amenazas y vulnerabilidades.
 - Comprender cómo toma decisiones el modelo y poder explicar esas decisiones de manera transparente.
 - Verificar que la estrategia cumpla con los requisitos regulatorios y de cumplimiento.



- Desarrollar modelos que puedan identificar patrones anómalos en el comportamiento del sistema y de los usuarios.
- Integrar la inteligencia humana para validar y contextualizar las alertas generadas por los modelos de IA.
- Establecer mecanismos para recopilar retroalimentación humana y mejorar constantemente los modelos.
- Implementar medidas para proteger los modelos de posibles ataques adversarios y manipulaciones maliciosas.
- Fortalecer la privacidad y la seguridad de los datos utilizados para el entrenamiento y la operación del modelo.

Caso de uso Sistemas de “Detección de Intrusiones (IDS) inteligentes”.

- Definir las amenazas y tipos de intrusiones que se buscan detectar.
- Determinar qué partes del sistema o red estarán bajo vigilancia.
- Recolectar datos de logs de red, registros de sistemas, tráfico de red, y cualquier otra fuente relevante.
- Utilizar datos históricos para entrenar modelos de ML en situaciones normales y anómalas.
- Asegurar que los datos estén en un formato consistente y limpio de ruido.
- Identificar y crear características (features) relevantes para el modelo.
- Evaluar si es más adecuado un enfoque supervisado (si hay etiquetas de intrusiones) o no supervisado.
- Utilizar algoritmos como Random Forests, Support Vector Machines (SVM), Redes Neuronales, o algoritmos de clustering para la detección de anomalías.
- Utilizar datos etiquetados y no etiquetados para entrenar el modelo.
- Realizar validación cruzada y ajustar parámetros para mejorar la precisión del modelo.
- Implementar el modelo en la infraestructura de seguridad para analizar el tráfico en tiempo real.
- Configurar el sistema para generar alertas cuando se detecten patrones sospechosos.
- Actualizar el modelo periódicamente con nuevos datos para adaptarse a las amenazas emergentes.



- Incorporar la retroalimentación humana para mejorar la precisión y relevancia de las alertas.
- Integrar el IDS con sistemas de respuesta automatizada para mitigar amenazas en tiempo real.
- Facilitar la comunicación entre el IDS y los equipos de respuesta a incidentes.
- Establecer métricas para evaluar la eficacia del IDS, como la tasa de falsos positivos y negativos.
- Analizar incidentes para mejorar la capacidad de detección y respuesta.
- Implementar medidas para proteger el modelo contra intentos de evasión o manipulación.
- Asegurarse de que la implementación del IDS cumple con las normativas de privacidad y protección de datos.

Nota: La estrategia deberá ser flexible y adaptarse a medida que evolucionan las amenazas ciberneticas. Además, la transparencia en la toma de decisiones del modelo y la capacidad de explicar las alertas generadas son aspectos cruciales en el contexto de la seguridad cibernetica.

Métricas Cuantitativas

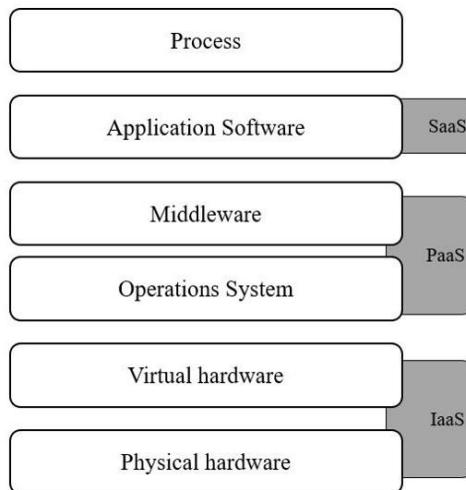
- **Tasa de Falsos Positivos (FP):** Reducir la generación de alertas falsas para evitar la sobrecarga del personal de seguridad. Número de alertas incorrectas generadas por el IDS.
- **Tasa de Falsos Negativos (FN):** Reducir los casos en los que el IDS no identifica amenazas reales. Número de amenazas reales no detectadas por el IDS.
- **Precisión:** Asegurar que las alertas generadas sean altamente precisas y relevantes. Proporción de alertas correctas sobre el total de alertas generadas.
- **Recall (Sensibilidad):** Maximizar la capacidad del IDS para detectar todas las amenazas reales. Proporción de amenazas detectadas sobre el total de amenazas reales.
- **Tiempo de Respuesta:** Reducir el tiempo de respuesta para mitigar los impactos de un incidente. Tiempo que tarda el IDS en identificar y responder a una amenaza.
- **Cobertura de Anomalías:** Verificar que el IDS sea capaz de identificar una amplia gama de comportamientos anómalos. Porcentaje de tipos de anomalías detectadas por el IDS.



Métricas Cualitativas.

- **Relevancia de la Alerta:** Clasificar la criticidad de las alertas para priorizar la respuesta. Evaluación de la importancia y gravedad de una alerta generada.
- **Complejidad de la Detección:** Evaluar la madurez del IDS frente a técnicas evasivas. Evaluación de la complejidad técnica para evadir la detección del IDS.
- **Capacidad de Adaptación:** Validar que el IDS sea capaz de evolucionar con las tácticas cambiantes de los atacantes. Evaluación de la capacidad del IDS para adaptarse a nuevas amenazas.
- **Facilidad de Integración:** Promover la adopción del IDS sin interrupciones significativas en la operación. Evaluación de la facilidad para integrar el IDS en la infraestructura existente.
- **Interfaz de Usuario:** Facilitar la interpretación de alertas por parte del personal de seguridad. Evaluación de la usabilidad y accesibilidad de la interfaz del IDS.
- **Capacidad de Reporte y Registro:** Facilitar la auditoría y el análisis post-incidente. Evaluación de la capacidad del IDS para generar informes detallados y mantener registros históricos.

Nube de servicios





Vulnerabilidades con tecnología web

- Inyección SQL: Inserción de código SQL malicioso a través de entradas no validadas para manipular bases de datos.
- Cross-Site Scripting (XSS): Inyección de scripts maliciosos en contenido web visible por otros usuarios.
- Cross-Site Request Forgery (CSRF): Engañar a un usuario autenticado para que ejecute acciones no deseadas en una aplicación web.
- Deserialización Insegura: Ejecución de datos deserializados no confiables que pueden conducir a la ejecución de código arbitrario.
- Inyección de Código: Inserción de código arbitrario que se ejecuta en el servidor debido a entradas no validadas.

Vulnerabilidades con tecnología web

- Configuraciones de Seguridad Incorrectas: Configuraciones predeterminadas inseguras o inapropiadas que exponen la aplicación a ataques.
- Falta de Control de Acceso: Omisión o implementación incorrecta de mecanismos para verificar los permisos de acceso a recursos.
- Exposición de Datos Sensibles: Almacenamiento o transmisión insegura de datos sensibles, como contraseñas o información personal.
- Vulnerabilidades en Dependencias: Uso de librerías y paquetes de terceros con vulnerabilidades conocidas sin actualizaciones.
- Manejo Inseguro de Archivos: Acceso y manipulación no controlada de archivos en el servidor, lo que puede permitir ataques como Directory Traversal.



Vulnerabilidades con tecnología móvil.

- Inyección SQL: Uso inadecuado de consultas SQL que permite la manipulación de bases de datos.
- Inyección de Comandos del Sistema: Ejecución de comandos del sistema a través de entradas no validadas.
- Fuga de Datos Sensibles: Almacenamiento y transmisión de datos sensibles sin cifrado adecuado.
- Autenticación Débil: Implementación deficiente de mecanismos de autenticación y gestión de sesiones.
- Control de Acceso Inadecuado: Falta de validación de permisos para acceder a recursos y funcionalidades.

Vulnerabilidades con tecnología móvil.

- Deserialización Insegura: Deserialización de datos no confiables que permite la ejecución de código arbitrario.
- Gestión Deficiente de Dependencias: Uso de bibliotecas y paquetes desactualizados con vulnerabilidades conocidas.
- Almacenamiento Inseguro de Credenciales: Guardado de contraseñas y tokens en texto plano o en lugares no seguros.
- Exposición de API Insegura: Falta de medidas de seguridad en las API que permite accesos no autorizados.
- Validación Insuficiente de Entradas: Falta de sanitización y validación de entradas del usuario que pueden llevar a ataques como XSS y CSRF.



Mejores prácticas de seguridad en API's

- Autenticación Robusta: Utilizar métodos de autenticación fuertes, como tokens de acceso o certificados, para verificar la identidad de los usuarios y servicios que acceden a la API.
- Autorización Granular: Implementar un control de acceso preciso y basado en roles para asegurarse de que los usuarios y servicios solo tengan acceso a los recursos y operaciones que necesitan.
- Protección contra Ataques CSRF: Implementar medidas para prevenir ataques de falsificación de solicitudes entre sitios (CSRF) mediante el uso de tokens anti-CSRF y asegurándose de que las solicitudes requieran autenticación.
- Validación de Entradas: Validar y sanitizar todas las entradas de usuario y datos recibidos a través de la API para prevenir ataques de inyección, como SQL injection o ataques de scripting entre sitios (XSS).
- Control de Errores Seguro: Configurar y manejar los errores de manera segura, evitando revelar información sensible sobre la estructura interna del sistema. Los mensajes de error deberían ser genéricos y no proporcionar detalles específicos.

Mejores prácticas de seguridad en API's

- Seguridad en la Capa de Transporte: Utilizar conexiones seguras mediante el protocolo HTTPS para proteger la confidencialidad e integridad de los datos transmitidos entre el cliente y el servidor.
- Límites de Tasa y Cuotas: Implementar límites de tasa y cuotas para prevenir ataques de denegación de servicio (DoS) y ataques de fuerza bruta. Esto ayuda a controlar la cantidad de solicitudes que pueden realizarse en un período de tiempo determinado.
- Registro y Monitoreo: Implementar un sistema de registro y monitoreo robusto para detectar y responder rápidamente a posibles amenazas o comportamientos anómalos. Registrar eventos de seguridad es esencial para realizar un análisis forense en caso de incidentes.
- Gestión de Sesiones Segura: Si la API maneja sesiones, asegurarse de que las credenciales y tokens de sesión se gestionen de manera segura, utilizando medidas como la expiración automática y la renovación de tokens.
- Seguridad en la Gestión de Configuraciones: Proteger la configuración de la API y los secretos almacenados, evitando su exposición accidental o malintencionada. Utilizar mecanismos seguros para la gestión de secretos.



Decálogo de riesgos en Machine Learning (ML)

- Alterar la entrada de datos a un modelo para obtener resultados apócrifos.
- Introducir datos maliciosos o erróneos en el conjunto de datos de entrenamiento o de validación de un modelo para degradar su rendimiento o sesgarlo.
- Utilizar las salidas de un modelo para inferir información sobre los datos de entrenamiento o los parámetros internos del modelo.
- Alterar un dato específico utilizado para entrenar un modelo basándose en las salidas y resultados.
- Robo de modelo, obtener una copia o una aproximación de un modelo sin autorización, ya sea mediante consultas al modelo o mediante el acceso al código o a los artefactos del modelo en algún repositorio.
- Afectar uno o más componentes de la cadena de suministro como los proveedores de (datos, infraestructura, servicios).
- Suplantar un modelo pre-entrenado redirigiendo a un dominio diferente con el fin de realizar un ataque, como la generación de contenido falso o la suplantación de identidad.
- Producir resultados injustos o discriminatorios debido a la presencia de sesgos en los datos, en los algoritmos o en los procesos para el entrenamiento del modelo.
- Alterar la salida de un modelo para engañar o perjudicar, modificando directamente el canal de comunicación entre el modelo.
- Modificar un modelo en tiempo de ejecución para cambiar su comportamiento o degradar su rendimiento, ya sea mediante la inyección de código malicioso o mediante la explotación de vulnerabilidades del entorno.

Decálogo de riesgos en Large Language Models (LLM)

- Manipulación a través de entradas "prompts" para provocar acceso no autorizado, filtraciones de datos y comprometer la toma de decisiones.
- No validar los resultados puede dar lugar a vulnerabilidades de seguridad posteriores, incluida la ejecución de código que comprometa los sistemas y exponga los datos.
- Reducción gradual de los datos de entrenamiento para afectar los modelos y generar respuestas que pueden comprometer la seguridad, la precisión o el comportamiento ético.
- Sobrecarga de peticiones utilizando "prompts" afectando los recursos computacionales provocando interrupciones en el servicio y mayores costos de operación.
- Afectación en componentes, servicios o conjuntos de datos comprometidos, poniendo en riesgo la integridad, disponibilidad, de los datos dentro del sistema.
- Eventualidades en la divulgación de datos confidenciales en los resultados del LLM, provocando consecuencias legales o una pérdida de credibilidad y ventaja competitiva.
- Procesamiento de entradas "prompts" que no son de confianza y que tienen un control de acceso insuficiente, permitiendo la ejecución de código malicioso.
- Otorgar a los LLM autonomía sin control para tomar medidas puede tener consecuencias no deseadas, poniendo en riesgo la confiabilidad, integridad, disponibilidad y privacidad de los datos.
- No evaluar críticamente los resultados del LLM, puede comprometer la toma de decisiones, y responsabilidades legales.
- Acceso no autorizado a modelos propietarios corre el riesgo de robo, ventaja competitiva y difusión de información confidencial.



Referencias bibliográficas

- Rose, S. , Borchart, 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
- Cusick, James. (2018). *The General Data Protection Regulation (GDPR): What Organizations Need to Know*. CT Corporation Resource Center.
- Seaman, Jim. (2023). *Zero Trust Security Strategies and Guideline*. 10.1007/978-3-031-09691-4_9.
- Garbis, Jason & Chapman, Jerry. (2021). *Zero Trust Security: An Enterprise Guide*. 10.1007/978-1-4842-6702-8.
- 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.
- Alawneh, Muntaha & Abbadi, Imad. (2023). *Approaches for Zero Trust Adoption Based upon Organization Security Level*. 10.1007/978-981-99-0272-9_36.
- Cheng, Ruizhi & Chen, Songqing & Han, Bo. (2023). *Towards Zero-trust Security for the Metaverse*.