

CIBERSEGURIDAD

MANUAL

Proyecto Aula 3IM12





FUSIÓN DE TECNOLOGÍAS "(CIBERSEGURIDAD)"



Proyecto Aula
Instituto Politécnico nacional
Centro de Estudios Científicos y Tecnológicos
No.8 "Narciso Bassols García"
Grupo 3IM12



Índice

1----- Capítulo 1: Teoría de la Ciberseguridad

1----1.1Teoría de la Ciberseguridad

5----1.2¿Qué alcance tiene la ciberseguridad?

9----1.3Áreas generales de aplicación de la ciberseguridad

13-----Capítulo 2: Ciberseguridad aplicada y sus conflictos

13----2.1Retos de ciberseguridad

19----2.2Aplicaciones prácticas de alumnos y docentes para protección de información
consejos

22---2.3Consejos necesarios sobre la identificación y la lucha contra riesgos digitales.

27-----Capítulo 3: IA con ciberseguridad.

27----3.1Concepto básico sobre IA, uso en nuestra vida diaria, ciberseguridad y que

. esperamos de ellas . Manejo, usos, peligros que representan en nuestro día a día



Capítulo 1. Teoría de la ciberseguridad

1.1 Ciberseguridad

La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.



La función de la ciberseguridad es evitar que nuestra información de distintos aspectos sea expuesta principalmente ante algún “ciberdelincuente” (persona que comete los delitos utilizando las tecnologías informáticas y de comunicación). Por esto desde la perspectiva técnica es la práctica de proteger sistemas informáticos, redes y datos contra amenazas electrónicas como:



Tipos de amenazas

Amenazas internas:

Las amenazas internas provienen de personas dentro de una organización que tienen acceso legítimo a los sistemas y recursos, pero que los utilizan de manera malintencionada o negligente

Ejemplos:

- Acciones malintencionadas: empleados que roban datos confidenciales o realizan sabotajes, ya sea por beneficio personal, venganza o espionaje corporativo.
- Errores humanos: errores involuntarios como enviar información confidencial a destinatarios incorrectos, instalar software malicioso accidentalmente o configurar mal un sistema.
- Uso indebido de privilegios: abuso de derechos de acceso para obtener información no autorizada o causar daño.

Amenazas externas:

Las amenazas externas provienen de actores que no tienen acceso legítimo a los sistemas de una organización y buscan vulnerar la seguridad desde fuera.

Tipos:

· Malware:

Software malicioso como virus, gusanos, ransomware, y spyware diseñado para dañar sistemas o extraer datos.

Phishing:

Intentos de engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios, mediante correos electrónicos o sitios web fraudulentos.

Ataques de denegación de servicio (DDOS):

Saturación de redes y servidores para interrumpir su funcionamiento.

Exploits:

Aprovechamiento de vulnerabilidades en software o hardware para obtener acceso no autorizado.

Ciberguerra:

Ataques organizados por gobiernos o grupos asociados para espiar o desestabilizar a otros estados.



Cultura de ciberseguridad

La formación continua de los empleados sobre las mejores prácticas de seguridad y la importancia de la protección de datos es clave para prevenir errores humanos que podrían comprometer la seguridad.

Implementar tecnologías de protección avanzadas:

- Las organizaciones deben adoptar tecnologías como firewalls, sistemas de detección de intrusiones, y software de antivirus. Además, el cifrado de datos es esencial para garantizar que la información sensible esté protegida.

Planes de respuesta ante incidentes:

- Es crucial que las organizaciones cuenten con un plan detallado para responder rápidamente a los ciberataques, con procedimientos claros para mitigar el daño y restaurar las operaciones.

Recomendaciones para gobiernos

- Los gobiernos tienen un papel fundamental en la creación de marcos regulatorios y en la implementación de políticas para proteger a sus ciudadanos y a sus infraestructuras críticas de los riesgos cibernéticos.





¿Por qué es importante la ciberseguridad hoy en día?

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en un aspecto crucial de nuestra vida diaria. A medida que los dispositivos conectados y los servicios en línea se han integrado en casi todos los aspectos de la sociedad, la protección contra amenazas cibernéticas se ha convertido en una prioridad tanto para individuos como para organizaciones y gobiernos. Desde la protección de datos personales hasta la seguridad de las infraestructuras críticas y la defensa de la economía global, la ciberseguridad es esencial para mantener el orden y la seguridad en el entorno digital.



¿Por qué es importante la ciberseguridad para tu empresa?

- El principal motivo de las empresas para invertir en ciberseguridad es para evitar pérdidas a gran escala de todo tipo siendo fundamental en la actualidad para el futuro cercano digital que nos aguarda siendo esta lista de motivos de su relevancia:
- Preservación de datos
- Autentificar disponibilidad y datos
- Evitar ingreso externo a datos confidenciales o importantes
- Proteger la operatividad de los sistemas.
- Evitar manipulaciones
- Evitar que se suplanten identidades para la toma de datos
- Evitar el robo de información, datos, imágenes, etc.
- Asegurar un cambio seguro a la digitalización
- Proteger los dispositivos personales.

1.2 ¿Qué alcance tiene la ciberseguridad?

El concepto de trabajo decente promovido por la Organización Internacional del Trabajo (OIT), se refiere a oportunidades laborales que respeten los derechos fundamentales, ofrezcan una remuneración justa y fomenten la seguridad social.

El Trabajo Decente en el Contexto Digital:

La digitalización ha transformado la naturaleza del trabajo, pues en la última década, el auge de la tecnología ha creado nuevas oportunidades laborales, especialmente en el sector de la ciberseguridad.

-Oportunidades Laborales: La ciberseguridad genera empleo en roles como analistas de seguridad, ingenieros de redes y expertos en respuesta a incidentes, según el foro económico mundial, se proyecta que esta industria generará millones de empleos en los próximos años.

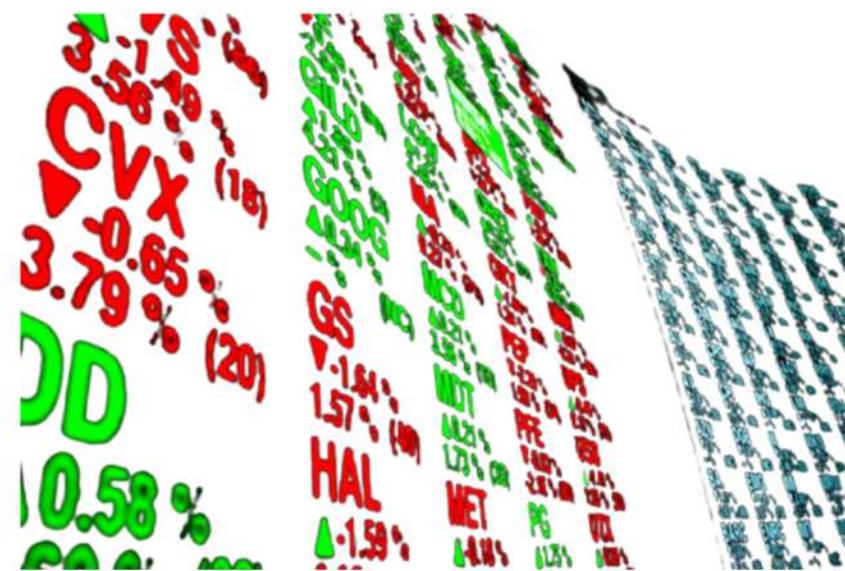
-Condiciones de Trabajo: Los empleos en ciberseguridad tienden a ofrecer salarios competitivos y condiciones estables, cumpliendo con los principios del trabajo decente, sin embargo, también enfrentan desafíos como el estrés laboral debido a la naturaleza crítica de las funciones



Ciberseguridad y Crecimiento Económico

La ciberseguridad no solo protege a las empresas, sino que también actúa como un motor del crecimiento económico al garantizar la confianza en los sistemas digitales...

- -Impacto Económico Directo: Empresas de todo el mundo invierten en soluciones de ciberseguridad impulsando la innovación tecnológica y fortaleciendo la economía digital
- -Reducción de Pérdidas: Los ataques cibernéticos cuestan billones de dólares anuales a nivel mundial. Invertir en ciberseguridad reduce estas pérdidas, permitiendo que las empresas reinvertan en expansión y creación de empleos.
- -Impulso al Emprendimiento: Las pequeñas y medianas empresas (PYMES), al adoptar medidas de ciberseguridad, ganan confianza de sus clientes y socios, lo que les permite competir en mercados globales.



Las estrategias de mitigación en el sector industrial incluyen:

- Uso de redes segregadas: Limitar la conectividad entre sistemas críticos y redes externas.
- Actualización constante: Aplicar parches de seguridad y actualizaciones para evitar vulnerabilidades.
- Redundancia y backups: Implementar sistemas de respaldo para minimizar el impacto de los ataques.
- Monitoreo continuo: Utilizar herramientas de análisis en tiempo real para identificar actividades sospechosas.

Tecnologías de Protección

- Blockchain: Garantiza la integridad de los datos mediante registros inmutables.
- IA en ciberseguridad: Detecta y responde a amenazas de manera automática y proactiva.
- Cifrado de datos: Protege la información sensible, incluso si es interceptada.

Medidas de Protección



Las estrategias para proteger infraestructuras críticas incluyen:

- Colaboración intersectorial: Involucrar a gobiernos, empresas y organismos internacionales en la protección de infraestructuras.
- Normativas y estándares: Implementar regulaciones que obliguen a cumplir con estándares de ciberseguridad.
- Simulacros y planes de contingencia: Preparar a las organizaciones para responder de manera efectiva ante incidentes.

Impacto que se tiene en la economía por la desigualdad en la ciberseguridad

La delincuencia por medio de la ciberseguridad, contribuye a la pobreza y desigualdad socioeconómica. Una de estas formas es cuando ocurre a través del fraude financiero y las estafas en línea, lo que provocan significativas perdidas para empresas y personas.

Para quienes viven en condiciones de pobreza, estas perdidas pueden agravar más su situación económica; Asimismo, los ataques hacia las infraestructuras, como energía, salud y transporte, afectan a los servicios esenciales y obstaculizan el desarrollo económico en regiones vulnerables.

La desigualdad en ciberseguridad no solo refleja las brechas socioeconómicas existentes, sino que también contribuye a agravarlas, continuando ciclos de pobreza y exclusión.

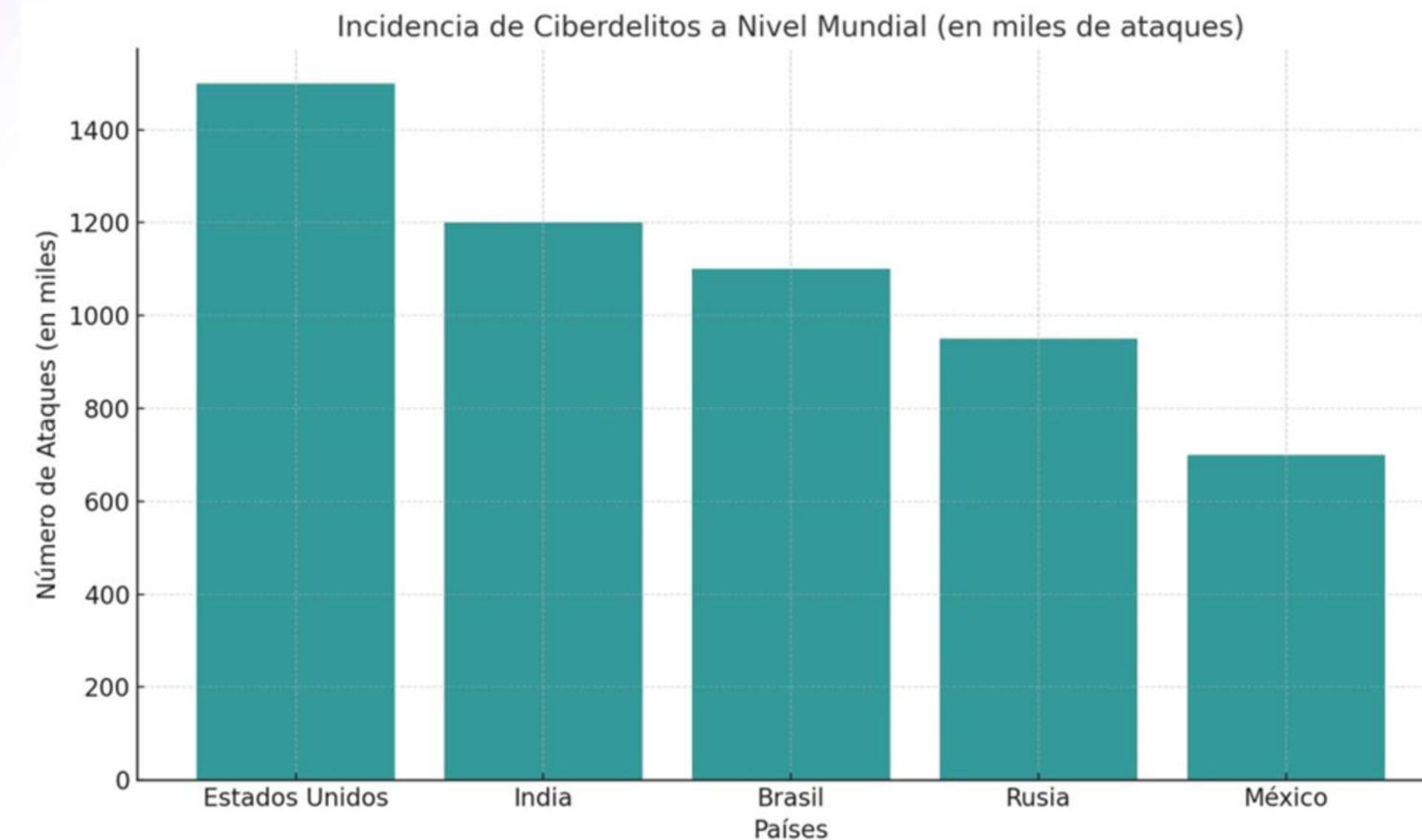
La ciberseguridad se ha convertido en un campo estratégico esencial para proteger los datos digitales y garantizar la continuidad de sistemas críticos en un mundo cada vez más interconectado. Este ámbito no solo exige conocimientos técnicos, sino que también requiere colaboraciones internacionales dado que las amenazas ciberneticas no tienen fronteras, se han creado alianzas en diferentes regiones del mundo para enfrentarlas de manera conjunta y coordinada.





Los gobiernos de todo el mundo consideran que proteger a los activos disponibles a través del internet y las redes informáticas de los hackers, es vital para el funcionamiento, la estabilidad de una nación y el sustento de la gente.

Hoy en día, vivimos rodeados de tecnología, pero con eso también han aumentado los riesgos digitales y las vulnerabilidades en nuestros sistemas. La ciberseguridad se ha vuelto super importante para proteger nuestra información y mantener todo funcionando sin problemas. Además, como las amenazas en internet no tienen fronteras, muchos países y organizaciones han empezado a trabajar juntos. Estas alianzas globales son clave para enfrentar los problemas de manera más efectiva y hacer que el mundo digital sea un lugar más seguro para todos.





1.3 Áreas Generales de Aplicación y Tipos de Ciberseguridad



Las Áreas Generales de Aplicación de la Ciberseguridad abarcan una amplia gama de sectores donde la protección de sistemas informáticos, datos y redes es muy importante para asegurar la integridad, confidencialidad y disponibilidad de la información. Estas áreas son fundamentales para mitigar los riesgos asociados con el cibercrimen, el espionaje, el fraude y otras amenazas.

1. Seguridad Empresarial

Protección de datos sensibles: Implementación de cifrado de extremo a extremo y políticas de gestión de identidades (IAM).

2. Gobierno y Defensa Nacional:

Infraestructuras críticas: Requieren monitoreo continuo y respuesta rápida ante incidentes

3. Sector Financiero

Seguridad de transacciones: Uso de cifrado TLS y machine learning para detectar fraudes.





¿Qué alcances tiene la ciberseguridad?

La ciberseguridad abarca la **protección de sistemas**, redes y datos frente a ataques, accesos no autorizados y fallos. A nivel personal, **protege** la privacidad y evita fraudes como el robo de identidad. En las empresas, garantiza la continuidad de las operaciones, el cumplimiento de regulaciones y la **seguridad** de los datos sensibles.

En el ámbito gubernamental, es esencial para **resguardar** infraestructuras críticas como energía, salud y transporte. También **enfrenta desafíos globales** como el ciberterrorismo y el espionaje digital, ayudando a mantener la estabilidad económica y social.

Además, la ciberseguridad se adapta a **proteger tecnologías emergentes** como el Internet de las cosas (IoT), la inteligencia artificial y las redes 5G, que introducen nuevos riesgos y oportunidades.



Bases de la ciberseguridad

La ciberseguridad se basa en tres principios fundamentales: **confidencialidad**, para que los datos solo sean accesibles por quienes estén autorizados; **integridad**, para garantizar que la información no sea alterada o manipulada; y **disponibilidad**, asegurando el acceso a los sistemas cuando sea necesario. Incluye medidas técnicas como firewalls, cifrado, antivirus y autenticación multifactor, además de fomentar hábitos seguros en los usuarios, como evitar enlaces sospechosos y usar contraseñas robustas. También se actualiza constantemente para afrontar amenazas modernas, combinando tecnología, procesos y educación para crear un entorno digital seguro y confiable.





4. Salud

Historia clínica electrónica (HCE): Información médica de los pacientes. Los hospitales aseguran que solo el personal autorizado tenga acceso a información médica sensible mediante encriptación.



5. Educación

Protección de datos estudiantiles: Evitar filtraciones de información personal y académica. Se cuida la privacidad de los estudiantes en plataformas digitales, resguardando sus datos personales.

6. Telecomunicaciones y Redes

Protección frente a espionaje: Evitar que terceros accedan a llamadas, mensajes y datos. Se evitan accesos no autorizados a llamadas y mensajes, asegurando la privacidad de las comunicaciones.

6. Telecomunicaciones y Redes

Protección frente a espionaje: Evitar que terceros accedan a llamadas, mensajes y datos. Se evitan accesos no autorizados a llamadas y mensajes, asegurando la privacidad de las comunicaciones.

7. Industria del Entretenimiento:

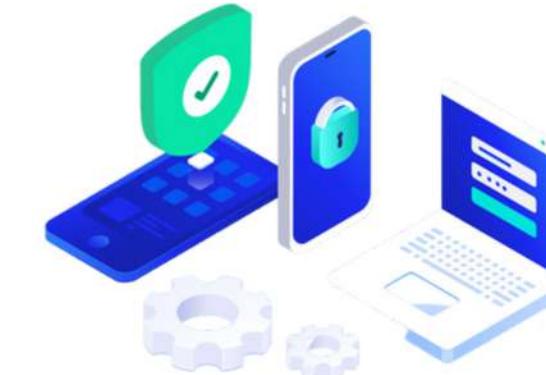
Protección de cuentas: Evitar el robo de credenciales de usuarios. Las plataformas de entretenimiento implementan medidas de seguridad para proteger el acceso a las cuentas de sus usuarios.





Seguridad de redes:

Es como poner puertas y alarmas en tu casa, pero en internet. Protege las conexiones entre computadoras para que nadie pueda espiar o colarse. Por ejemplo, se usan cosas como firewalls y VPNs.



Seguridad de información:

Aquí se cuidan tus datos, como si fueran secretos importantes. Se trata de mantenerlos a salvo, que nadie los robe ni los cambie. Se usan claves, contraseñas y métodos para protegerlos.

TIPOS DE CIBERSEGURIDAD



Seguridad en la nube:

Es como proteger las cosas que guardas en una caja fuerte digital (como Google Drive o Dropbox). Asegura que tus datos en la nube estén seguros y no se pierdan o los roben.

Seguridad de aplicaciones:

Imagina que las apps de tu celular o computadora tienen una armadura. Esto se trata de asegurarse de que las aplicaciones sean seguras, desde que se crean hasta cuando las usas. Así se evitan hackers y problemas.



Capítulo 2. Ciberseguridad aplicada y sus conflictos

2.1 Retos Ciberseguridad

Los problemas de ciberseguridad ponen en peligro la información confidencial de una empresa y supone un impacto negativo cualquier negocio. La protección de la infraestructura crítica en ciberseguridad enfrenta desafíos constantes debido a la evolución de las amenazas. La ciberseguridad no es solo una prioridad, sino que es esencial para salvaguardar la sociedad digital.

La infraestructura crítica enfrenta diversas amenazas ciberneticas que comprometen su estabilidad y seguridad. Entre las principales amenazas se encuentran:

- **Ciberespionaje:** Actores estatales y no estatales recopilan información confidencial para obtener ventajas geopolíticas, económicas o militares.
- **Ransomware:** Los ciberdelincuentes cifran sistemas esenciales y exigen pagos para restaurar el acceso
- **Ataques DDoS:** Saturan recursos, interrumpeando operaciones mediante la sobrecarga de redes
- **Manipulación de Datos:** Alteran la integridad de información crucial, afectando sectores como salud o finanzas.
- **Ingeniería Social:** Utilizan tácticas como phishing para engañar a empleados





Seguridad de los dispositivos IOT

IoT es una abreviatura de la expresión “Internet de las cosas” y denota todos sus dispositivos y más concursos conectados a la red: cámara de videovigilancia, refrescador inteligente, vehículo con red favorable inalámbrica, entre muchos otros.

Dado que cualquier cosa conectada a la red es vulnerable al ataque, no se hace una excepción de los dispositivos del IoT. Los atacantes pueden comprometerlos para realizar robos de datos, lanzar ataques anarchist distributed del to-region en el servicio y atacar redes más amplias.

Los ataques más comunes a dispositivos IoT (Internet de las Cosas) incluyen:

- **Explotación de vulnerabilidades del firmware:** El firmware de los dispositivos IoT es simplificado y carece de protección adecuada
- **Ataques basados en credenciales débiles:** Muchos dispositivos utilizan contraseñas de fábrica simples y comunes que, en algunos casos, no pueden cambiarse, facilitando ataques como el credential stuffing.
- **Ataques de ruta (man-in-the-middle):** Los atacantes interceptan mensajes entre el dispositivo IoT y su servidor manipulando datos confidenciales.
- **Acceso físico al hardware:** Dispositivos ubicados en espacios públicos, como cámaras son susceptibles a manipulación directa para extraer datos o tomar el control del sistema



Reducción de desigualdad

Promover la equidad en ciberseguridad no solo protege a los más vulnerables, sino que fortalece la cohesión social y fomenta una economía digital inclusiva. Es un paso esencial hacia un futuro más justo y seguro

Estrategias para Reducir Desigualdades en Ciberseguridad

- Educación digital accesible: Ofrecer formación básica en ciberseguridad mediante talleres gratuitos, integrar el tema en la educación formal y adaptarlo para comunidades vulnerables.
- Infraestructura segura y accesible: Garantizar internet de calidad en zonas marginadas y proteger redes públicas con medidas como encriptación.
- Políticas públicas inclusivas: Crear leyes que protejan contra ciberdelitos y lanzar campañas educativas claras.
- Herramientas de seguridad asequibles: Proveer antivirus, firewalls y dispositivos seguros gratuitos o a bajo costo.
- Inclusión de grupos vulnerables: Diseñar soluciones tecnológicas adaptadas y accesibles, apoyadas por centros comunitarios tecnológicos.
- Equidad en el diseño tecnológico: Desarrollar tecnologías seguras, asequibles e inclusivas, considerando las necesidades de todos los usuarios.



Policía cibernética en Mexico



¿Que es la ciberpolicia en Mexico?

Son unidades fuerzas de seguridad especializadas que estan encargados de la persecución de delitos de ámbitos digitales entre los que se incluyen personal de :

- Agentes
- Detectives
- Analistas
- Fiscales
- Jueces con especialidad en delito cibernéticos
- Informáticos



¿Qué hace la ciber policía?

Los objetivos principales de la ciber policía es la prevención y auxilio a los ciudadanos sobre el riesgo de su integridad física y patrimonial en internet

En CDMX se tuvo la necesidad de crear un área gracias a el crecimiento del uso de internet por lo que el 3 de abril de 2013 se creó la unidadcibernética que se encarga de promover el civismo digital dentro del área de CDMX y transmitir conocimientos de prevención, respeto, autocuidado al navegar en internet



Policía cibernética en Mexico

¿Qué son los delitos digitales?

- Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo. Y Como fin, son las dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

DELITOS CIBERNETICOS

Ciber acoso

Tambien conocido como acoso cibernético o acoso virtual es la intimidación por medio de medios digitales ya sean redes sociales ,aplicaciones de mensajeria,chats de voz ,etc.

Estos se caracterizan por que son un comportamiento repetitivo con el afán de humillar, causar miedo o causar enojo en las personas

Grooming

Mediante engaño una persona con mayoría de edad se gana la confianza de una persona menor de edad generando una especie de amistad con el con la finalidad de

conseguir fotos de índole sexual ,estas imágenes se vuelven de consumo de pederastas

Tambien pueden derivar en otros delitos como abuso sexual, acoso o en casos extremos secuestros

Robo de Identidad

Este se da cuando una persona se hace pasar por otra con el fin de hacer estafas ,fraude y extorsión con la finalidad de que no se atrape a la persona real que está cometiendo el delito

Sexting

Este es el intercambio de fotos y videos personales de índole sexual por aplicaciones de mensajería como WhatsApp pero que llevan un riesgo alto ya que una vez que se envió el contenido se pierde el control total sobre el





Violencia Digital

Acciones Dolosas mediante las TIC (Tecnologías de la Información y las Comunicaciones)

Con las reformas de Ley General de Acceso de las Mujeres a una Vida Libre de Violencia la violencia digital se define como una acción dolosa mediante el uso de tecnologías de la información y la comunicación que se use para distribuir, difundir, comercializar o comparten imágenes, videos, audios reales o de edición o creados con inteligencia artificial de contenido íntimo sin el consentimiento de las personas de las imágenes y que les puede generar daño psicológico, emocional o que perjudiquen a su imagen personal y dignidad de las mujeres

Formas de violencia digital

- Cuando se molestan por no recibir respuesta inmediata en línea
- Cuando me obligan a mostrar mis chats con otras personas.
- Cuando me exigen mi geolocalización.
- Cuando controlan el uso de mi dispositivo móvil.
- Cuando me obligan a compartir imágenes íntimas.
- Cuando crean y comparten información falsa con la intención de dañar mi reputación

Recomendaciones para evitar volverse una víctima de violencia digital

- Antes de interactuar en cualquier red social, sitio web o aplicación, investiga un poco sobre estas para identificar posibles riesgos
- Evita compartir información personal
- Conoce y configura las opciones de privacidad y seguridad de todas las redes sociales
- Utiliza contraseñas seguras
- Verifica cuáles y cuántos dispositivos están conectados a tus redes; cierra sesiones de dispositivos que no conozcas



ALGUNAS FORMAS DE VIOLENCIA DIGITAL

2.2 Aplicaciones prácticas de alumnos y docentes para protección de información y consejos útiles para las personas cotidianas

Prosperidad económica

La reducción de las desigualdades en el ámbito de la ciberseguridad es un desafío crítico que requiere atención global debido a las discapacidades en recursos, capacidades técnicas y acceso a la formación.

-Educación:

Iniciativas como programas de formación especializada en ciberseguridad y asociaciones público-privadas han demostrado eficacia para cerrar la brecha de habilidades en países de desarrollo. Por ejemplo, en Israel, la ciberseguridad se enseña desde la escuela secundaria, lo que podría replicarse en otros lugares para capacitar a los jóvenes y grupos subrepresentados.

Un enfoque en la alfabetización digital permite a las personas participar plenamente en las esferas económica y política, fortaleciendo su resiliencia ante riesgos cibernéticos.

Las naciones con baja capacidad cibernética son más vulnerables a ciberataques, lo que afecta tanto a empresas como a infraestructuras críticas.

Invertir en ciberseguridad no solo mejora la resiliencia ante amenazas digitales.



Trabajo docente y crecimiento económico



Trabajo Decente y Crecimiento Económico:

El concepto de trabajo decente brilla como un faro de esperanza en un mundo donde la desigualdad y la precariedad laboral son realidades que todos podemos sentir. Este término, creado por la Organización Internacional del Trabajo (OIT),

La Naturaleza del Trabajo Decente

El trabajo decente se refiere a la creación de empleos que son productivos y que ofrecen condiciones laborales justas y seguras. Esto incluye salarios justos, protección social, y la posibilidad de crecer y aprender en el entorno laboral. En un mundo donde el desempleo y la subcontratación han aumentado, el trabajo decente se convierte en un refugio; un lugar donde cada persona puede contribuir a la sociedad y, al mismo tiempo, encontrar un sentido de pertenencia y propósito.

Cuando las personas trabajan en un ambiente que respeta sus derechos, se sienten valoradas y motivadas. Esto no solo mejora su bienestar individual, sino que también fortalece el tejido social de nuestras comunidades.



Crecimiento Económico:

El crecimiento económico, que se mide a través del aumento del Producto Interno Bruto (PIB), es a menudo visto como el principal indicador del desarrollo de un país.

-Este enfoque puede ser engañoso si no consideramos la calidad del crecimiento. Un crecimiento que no mejora la vida de las personas es un crecimiento vacío.

-Aquí es donde el trabajo decente se vuelve muy importante. Cuando las personas tienen acceso a trabajos dignos, no solo aumentan sus ingresos; también se crea un ambiente de estabilidad social y económica.

-Genera una fuerza laboral más capacitada y productiva. Este ciclo de inversión y retorno es lo que realmente alimenta un crecimiento económico sostenible. Además, cuando los trabajadores tienen acceso a mejores salarios y condiciones laborales, su capacidad de consumo aumenta.

-Por un lado, el crecimiento económico proporciona los recursos necesarios para crear empleos de calidad. Por otro lado, la creación de trabajo decente impulsa la economía al aumentar el consumo y la inversión.





2.3 Consejos necesarios sobre la identificación y la lucha contra riesgos digitales

Anuncios en programas y Ventanas emergentes

Los procesos como abrir aplicaciones, iniciar sesión se tardan en llevar a cabo. Esto es porque el malware se apodera de los recursos del equipo y sobrecargando el sistema operativo haciendo que el equipo se bloquee o que se detengan los programas en segundo plano



Uso de recursos cuando no se ocupan programas

El uso que marca la CPU y memoria RAM es alto a pesar de que no hay programas en uso o ejecución y el sistema llega a alcanzar temperaturas altas.



Identificación de Amenazas

Realentización del Equipo

El dispositivo comienza a mostrar anuncios en navegadores o aplicaciones.

Algunos tipos de malware pueden mostrar anuncios mientras intentamos usar los navegadores ,entre las cosas que pueden saltar sobre la pantalla son:

- Anuncios pornográficos.
- Anuncios sobre regalos por usar algún sitio web.
- Advertir sobre infección de virus en el dispositivo.



Restricción de acceso a software

Se llega a perder el acceso parcial o total a programas o a dispositivos de hardware y memorias de almacenamiento.



Iconos de programas no responden

Al presionar los iconos de los programas estos no se abren o en el caso contrario que cierran.



Antivirus con comportamiento inusual

Los antivirus de programas y navegadores se desactivan de forma inesperada sin que el usuario entre a desactivarlos.





Prever la ciberseguridad

Protección de dispositivos y redes

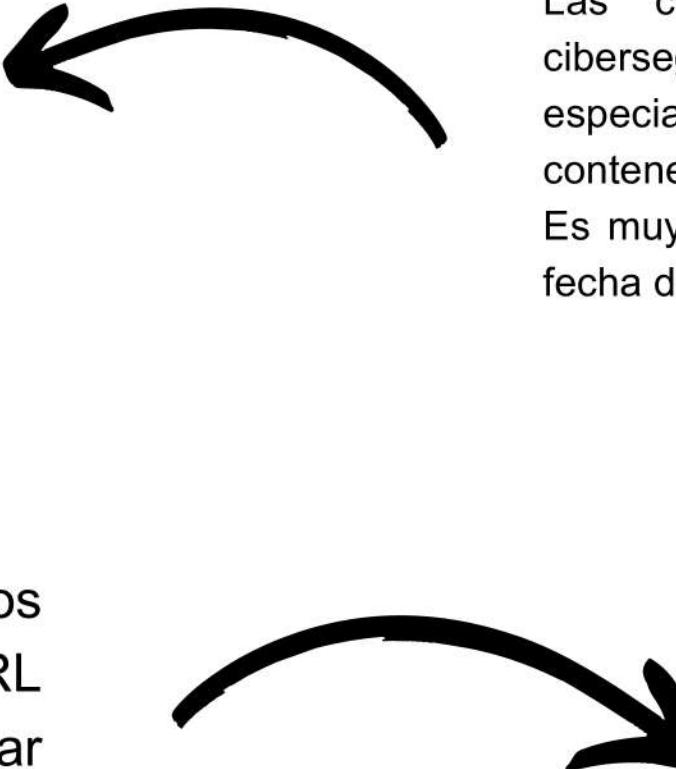
Mantener los sistemas operativos y las aplicaciones actualizadas es una de las formas mas efectivas de evitar vulnerabilidades conocidas que usualmente explotan los cibercrimen.

Una conexión VPN (red privada virtual) cifra el tráfico de Internet haciendo todo más seguro. Los cortafuegos y el software antivirus sin barreras esenciales contra las ciber amenazas.



Evitar abrir archivos, URLs correos electrónicos sospechosos

Las amenazas de phishing, son comunes. Saber identificar los signos de phishing como errores ortográficos y URL sospechosas es fundamental. Es importante siempre comprobar que el remitente de un correo electrónico es verídico antes de realizar cualquier acción.



Gestión de contraseñas seguras

Las contraseñas seguras son un elemento clave en la ciberseguridad. Deber ser medianamente largas, con caracteres especiales ("/", "*", ".", etc.) según la plataforma lo permita, deben contener letras mayúsculas y minúsculas, además de números.

Es muy importante evitar poner información fácil de obtener, como fecha de nacimiento, nombres o apellidos, ciudad de nacimiento, etc.





Prevenir un cibertaque

Verificación en dos pasos

Este es un método de seguridad de administración de identidad. La verificación de dos pasos sirve también como detector de actividad de actividad sospechosa emitiendo alertas si se producen intentos de acceso desde ubicaciones sospechosas.

Con un dispositivo móvil se puede generar tokens o códigos propios para proporcionar un conjunto exclusivo de letras y/o números para verificar la autenticidad del intento de acceso.



Los usuarios deben garantizar que su información personal también está segura. Esto incluye evitar el intercambio excesivo de información en las redes sociales.

En nuestro entorno es más común el uso de códigos de un solo uso que pide el software o aplicación para completar el uso de la aplicación, pueden ser redes sociales, cuentas bancarias, correo electrónico, etc. Lo más común son códigos enviados SMS, correo electrónico, o como se ha comenzado a utilizar, vía WhatsApp.



Protege tus datos personales

Comprende al grupo de medidas tecnológicas organizativas y legales que buscan resguardar, ante cualquier vulnerabilidad, los datos personales del usuario al asegurar que pueda tener control sobre la información que se brinda por internet o cualquier medio físico.





Mensajes de phishing

CORREOS

Estimado cliente: Su paquete esta listo para la entrega confirme el pago de aduanas de (0,99 €) en el siguiente enlace: t.ly/Siguiente

20 min

⊕ Mensaje de tex... 😊 0

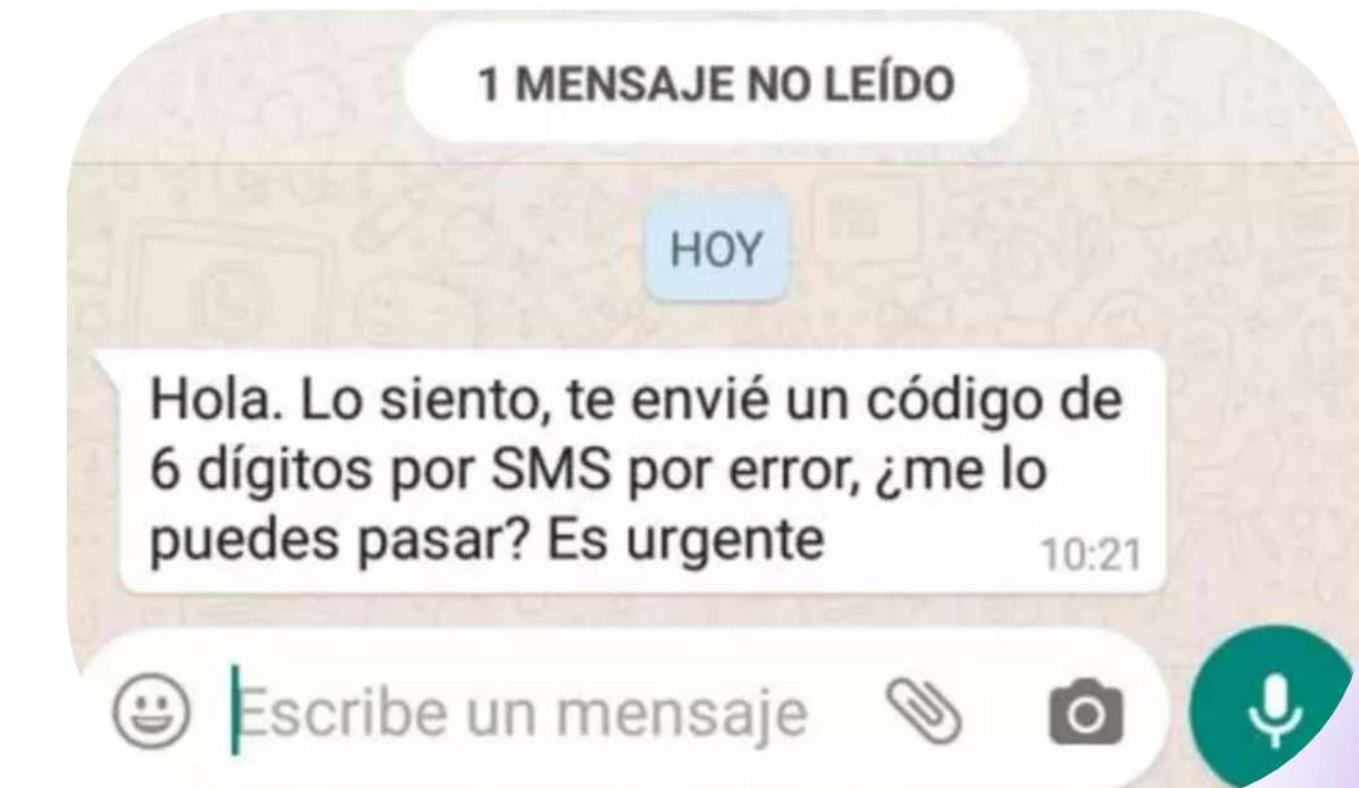


Lun, 16:09

Eres tu que apareces en este Video?..
<https://l2l.li/Fwalk>



Aa



Escribe un mensaje





Puedes utilizar
VPN



Utiliza
verificación en
dos pasos



Números
Caracteres especiales

Estén medianamente largas

Que tengan:

Manten
contraseñas
seguras

Mantén actualizados
el antivirus y el
cortafuegos

Acciones para prevenir un ciber ataque

Ten un correo de
recuperación



Proteger cuentas en caso de
intentos de acceso a correos
personales

Ayuda a:
Recuperar
contraseñas

Evita dar datos
personales muy
importantes.



Nombres
Fecha de
nacimiento

No abras enlaces
sospechosos

Documentos

Correos
electrónicos

URLs



3.1 Concepto básico sobre IA, uso en nuestra vida diaria, ciberseguridad y que esperamos de ellas

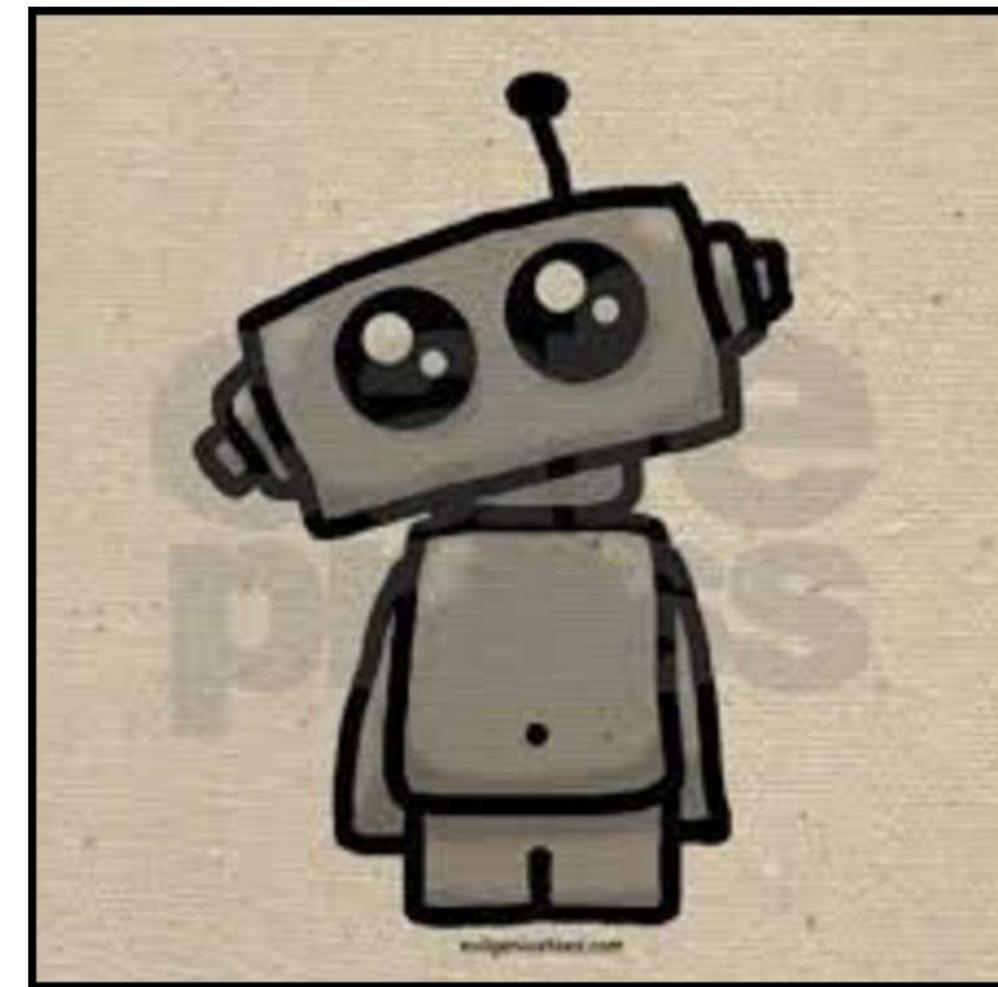
Manejo, usos, peligros que representan en nuestro día a día

Concepto básico

La Inteligencia Artificial es una rama de la informática que busca replicar capacidades humanas un ejemplo es la toma de decisiones, el aprendizaje y la comprensión del lenguaje.

Su origen se remonta a la década de 1950. Desde entonces, la inteligencia artificial ha evolucionado significativamente. Los avances recientes en aprendizaje automático han impulsado su uso en la vida cotidiana, dando lugar a herramientas como los asistentes virtuales, entre los que destacan Siri y Alexa.

¡No soy un
cerebro digital!
¿o sí?



Aunque a veces se considera la IA como “cerebros digitales”, en realidad es son algoritmos que procesan grandes cantidades de datos para automatizar tareas humanas.

Uso de la IA en la vida cotidiana

La IA se ha integrado profundamente en nuestras actividades diarias

Asistentes virtuales

Herramientas como Siri, Alexa y Google Assistant automatizan tareas básicas como recordatorios, encender luces o ajustar la temperatura en hogares inteligentes.



Smartphones

Los dispositivos móviles utilizan IA para asistentes de voz, filtros de fotos y detección de spam en correos electrónicos.



Casas inteligentes

La automatización en el hogar abarca robots de cocina, sistemas de iluminación y dispositivos como Smart TVs.



Uso de la IA en la vida cotidiana

Redes sociales

Personalizan las notificaciones y el contenido que vemos, mejorando la experiencia del usuario.



Compras en línea

El comercio electrónico utiliza IA para recomendar productos personalizados.



GPS

La automatización en el hogar abarca robots de cocina, sistemas de iluminación y dispositivos como Smart TVs.



Ciberseguridad

La IA ayuda a detectar ataques y prevenir amenazas cibernéticas, protegiendo tanto datos personales



El uso cotidiano de la IA responde al deseo de facilitar tareas diarias. Sin embargo, esto puede fomentar la dependencia tecnológica. Es fundamental usar esta tecnología de forma equilibrada y responsable.



Peligros de la IA

A pesar de sus beneficios, la IA presenta riesgos significativos en los ámbitos ético, social, económico y de seguridad:

1. Discriminación algorítmica: Los algoritmos reflejan sesgos presentes en los datos de entrenamiento, resultando en decisiones injustas en áreas como empleo, justicia penal y acceso a servicios.
2. Impacto laboral: Según el Foro Económico Mundial, para 2030 se perderán más de 85 millones de empleos debido a la automatización, afectando principalmente a tareas repetitivas.
3. Ciberseguridad: Facilita la creación de deepfakes y ataques de phishing personalizados, aumentando el riesgo de fraudes digitales.
4. Superinteligencia: Aunque hipotético, el desarrollo de una IA más inteligente que los humanos plantea preguntas filosóficas y existenciales sobre el control de dicha tecnología.

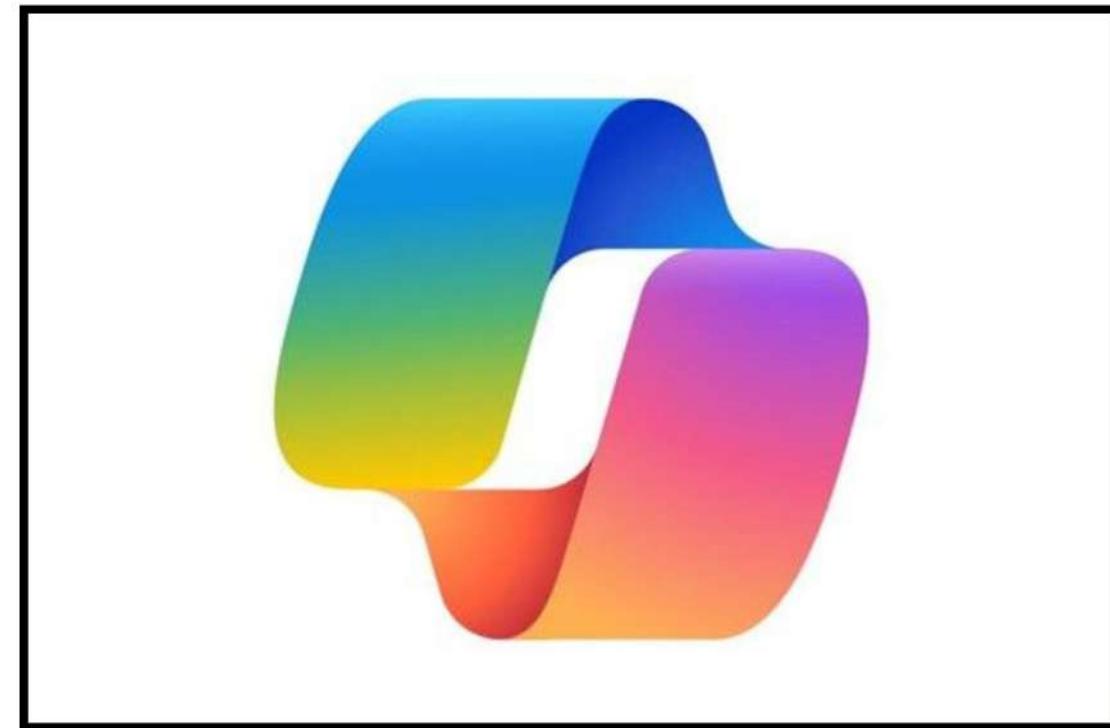


Ciberseguridad e IA

La ciberseguridad y la IA están estrechamente vinculadas. Por un lado, la IA mejora las defensas digitales mediante herramientas avanzadas como DLP (Prevención de Pérdida de Datos) y EDR (Detección y Respuesta para Endpoints). Estas tecnologías analizan grandes cantidades de datos para identificar amenazas antes de que se materialicen.



Por otro lado, los cibercriminales también aprovechan la IA para perfeccionar ataques, como la generación de mensajes de phishing altamente personalizados o deepfakes convincentes.



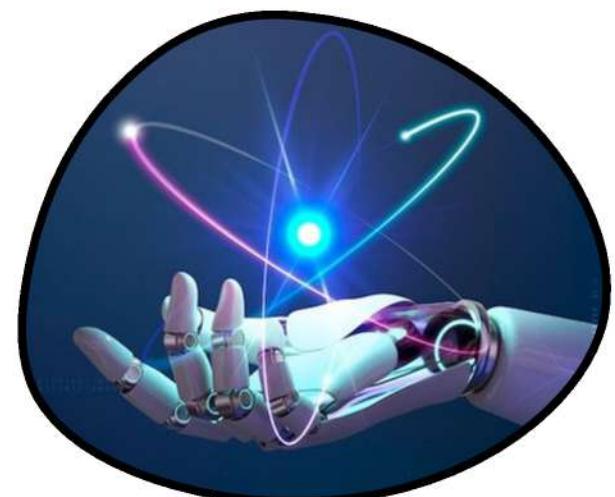
Microsoft 365 Copilot es un ejemplo de cómo integrar IA en entornos seguros. Este sistema combina grandes modelos de lenguaje con medidas de protección, garantizando que los datos generados permanezcan dentro de la organización.

Soluciones y el futuro de la IA en ciberseguridad

El futuro de la IA en ciberseguridad se centrará en sistemas autónomos capaces de responder rápidamente a nuevas amenazas. Estos sistemas combinarán análisis de datos con un entendimiento más contextual

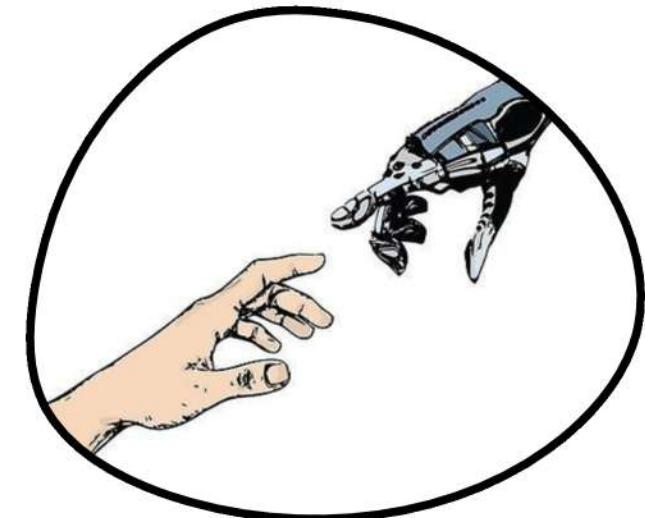
Actualización constante

Invertir en tecnología moderna y mantenerse informado sobre nuevos desarrollos es esencial para enfrentar amenazas crecientes



Integración con equipos humanos

La IA debe complementar a los equipos de TI, automatizando tareas repetitivas mientras se asegura un manejo ético y seguro.



Políticas de datos actualizadas

Políticas de datos actualizadas: Las organizaciones deben garantizar el cumplimiento de normativas de privacidad para proteger la información personal.

