# Ciberseguridad

## Contextualización

Se entiende por ciberseguridad todas las prácticas, tecnologías, procesos y medidas que estén orientadas a la protección de los sistemas informáticos, redes, dispositivos y datos de ataques cibernéticos, accesos no autorizados, daños o robos. Su objetivo principal es la protección de la información y de sus características básicas: confidencialidad, integridad, disponibilidad y autenticidad de los sistemas y usuarios en las diferentes redes digitales.

### Componentes clave de la ciberseguridad:

## Confidencialidad

La información que comparte sólo debe ser proporcionada a personas autorizadas. Esto se logra mediante diversas herramientas como cifrado y control de acceso.

## Integridad

La integridad de los datos se refiere al hecho de que ningún medio no autorizado puede cambiar los datos de ninguna manera para hacerlos incorrectos o poco confiables durante algún tiempo.

## Disponibilidad

Si los sistemas, datos y servicios deben estar disponibles para los usuarios autorizados cuando lo requieran, sin interrupción en los servicios.

## Autenticidad

Verificar la identidad de usuarios y sistemas para asegurarse de que solo aquellos autorizados pueden acceder a la información o realizar acciones.

### Áreas clave de la ciberseguridad:

Seguridad de redes

Ralentiza la propagación de ataques como hacking, malware, o accesos no autorizados a las redes informáticas, y facilita su detección gracias a programas como firewalls, sistemas de detección de intrusiones, entre otros programas de monitoreo.

## Seguridad de la información

Garantiza la protección de datos tanto en reposo como en tránsito mediante técnicas como el cifrado y la gestión de derechos de acceso.

## Seguridad de aplicaciones

Protege las aplicaciones contra vulnerabilidades que puedan ser explotadas por hackers para acceder a datos o sistemas. Involucra pruebas de seguridad, parches y actualizaciones.

## Gestión de identidades y accesos

Controla y asegura que solo los usuarios autorizados puedan acceder a los sistemas y datos, utilizando métodos como la autenticación multifactor (MFA) y la gestión de permisos.

## Respuesta ante incidentes

Implica la preparación y respuesta eficaz a los ataques cibernéticos cuando ocurren, minimizando el impacto y recuperando los sistemas afectados.

### Principales amenazas en ciberseguridad:

## Malware

Software malicioso diseñado para dañar o comprometer sistemas, como virus, troyanos y ransomware.

## Phishing

Ataques que buscan engañar a los usuarios para que revelen información sensible, como contraseñas o datos financieros.

## Ataques de denegación de servicio (DDoS)

Intentos de sobrecargar un sistema o red, impidiendo el acceso a servicios legítimos.

Exploits de vulnerabilidades: Ataques que se aprovechan de fallos o errores en el software para acceder a sistemas.

# Avances tecnológicos (Inventos)

La ciberseguridad ha estado experimentando un crecimiento debido al desarrollo y adopción de las más variadas tecnologías innovadoras, que han modificado tanto la defensa de sistemas como formas de combatir las amenazas. Seguidamente se describirán los adelantos tecnológicos clave de este crecimiento y posicionamiento: Inteligencia Artificial (IA), Blockchain, Computación en la nube e Internet de las Cosas (IoT).

## Inteligencia Artificial (IA) y su impacto en la ciberseguridad

La Inteligencia Artificial (IA) ha revolucionado la ciberseguridad al permitir una defensa más eficaz frente a las amenazas cibernéticas. Las capacidades avanzadas de la IA permiten monitorear y analizar grandes volúmenes de datos en tiempo real, identificando patrones y anomalías que podrían indicar un ataque.

Aplicaciones de IA en la ciberseguridad

Detección proactiva de amenazas: La IA puede identificar comportamientos anómalos o patrones inusuales en el tráfico de red, lo que ayuda a detectar ataques antes de que causen daños. Esto es especialmente útil en la detección de amenazas avanzadas, como los ataques de día cero.

## Automatización de la respuesta a incidentes

La integración de la IA permite que los sistemas respondan automáticamente a las amenazas sin intervención humana, con el fin de reducir el tiempo de respuesta y mitigar daños potenciales.

## Análisis predictivo

ML ayuda a predecir futuras amenazas basadas en datos históricos y forma en que está cambiando la trayectoria de la amenaza, permitiendo que la organización esté mejor preparada ante posibles ataques.

Reconocimiento de patrones de phishing:

La IA puede analizar correos electrónicos y comunicaciones en busca de indicios de ataques de phishing, detectando y bloqueando mensajes maliciosos.

# Ejemplo de invento tecnológico

Plataformas de seguridad basadas en IA: Sistemas como Darktrace y Cylance utilizan IA para detectar amenazas cibernéticas en tiempo real, anticipándose a posibles ataques y minimizando las consecuencias.

# Blockchain como herramienta de seguridad

El Blockchain o cadena de bloques, inicialmente desarrollada para el ámbito de las criptomonedas, ha demostrado ser una herramienta poderosa para la ciberseguridad debido a su naturaleza descentralizada y su capacidad para garantizar la integridad de los datos. Blockchain ofrece una forma segura de registrar transacciones y sin necesidad de intermediarios, lo que aumenta la protección contra accesos acciones no autorizadas o manipulaciones.

# Aplicaciones de blockchain en la ciberseguridad

## Inmutabilidad de los registros

gracias a la tecnología blockchain, es posible generar registros de datos que no pueden ser alterados sin que ello quede detectado. Se garantiza la integridad de los datos guardados; algo importantísimo en sectores críticos como finanzas y salud.

## Gestión segura de identidades

Blockchain permite un control descentralizado de las identidades, lo que dificulta el robo de datos personales o la suplantación de identidad. Los sistemas de identidad basados ​​en blockchain pueden eliminar la necesidad de contraseñas vulnerables.

## Contratos inteligentes (smart contracts)

Estos contratos automatizados, ejecutados en blockchain, pueden garantizar la seguridad de transacciones y acciones sin la intervención de terceros, minimizando el riesgo de fraude o interferencias maliciosas.

# Ejemplo de invento tecnológico

## Blockstack

Una plataforma que utiliza blockchain para crear un ecosistema descentralizado de aplicaciones y gestionar identidades de forma segura, asegurando que los datos de los usuarios no sean vulnerables a ataques centralizados.

# Computación en la nube (Cloud Computing) y su impacto en la ciberseguridad

La computación en la nube ha transformado la infraestructura tecnológica, permitiendo a las organizaciones almacenar y procesar grandes volúmenes de datos sin la necesidad de mantener hardware local. Sin embargo, también ha planteado nuevos desafíos de ciberseguridad. A medida que más empresas migran a la nube, se han desarrollado soluciones de seguridad específicas para garantizar la protección de los datos almacenados y procesados ​​en estos entornos.

# Contribuciones de la computación en la nube a la ciberseguridad

## Seguridad como servicio (SECaaS)

Los proveedores de servicios en la nube como Amazon Web Services (AWS), Microsoft Azure y Google Cloud ofrecen soluciones de ciberseguridad integradas como el cifrado de datos, la autenticación multifactor (MFA) y la detección de amenazas.

Resiliencia ante desastres

La computación en la nube permite a las organizaciones mantener copias de seguridad distribuidas geográficamente, mejorando la recuperación ante desastres en caso de ataques cibernéticos.

## Protección dinámica

Las plataformas en la nube están diseñadas para adaptarse automáticamente a las amenazas emergentes. Las actualizaciones automáticas y los parches de seguridad ayudan a proteger las infraestructuras sin manual de intervención.

## Análisis en tiempo real

La computación en la nube permite el análisis y monitoreo de grandes volúmenes de datos en tiempo real, facilitando la detección temprana de vulnerabilidades y ataques.

# Ejemplo de invento tecnológico

Google Chronicle

Un servicio de ciberseguridad en la nube que utiliza la infraestructura de Google para analizar grandes cantidades de datos sobre amenazas en tiempo real, mejorando la detección y respuesta ante ciberataques.

# Internet de las Cosas (IoT) y sus desafíos de ciberseguridad

El Internet de las Cosas (IoT) ha conectado dispositivos cotidianos, como electrodomésticos, sensores industriales y vehículos, a internet, lo que ha permitido una mayor automatización y eficiencia. Sin embargo, cada dispositivo conectado amplía la superficie de ataque, lo que aumenta los riesgos de seguridad.

# Contribuciones y desafíos del IoT en la ciberseguridad

Ampliación de la superficie de ataque

Cada dispositivo IoT puede convertirse en un punto de entrada para los ciberdelincuentes si no está adecuadamente protegido. Muchos dispositivos IoT carecen de seguridad básica, como autenticación o cifrado.

## Ataques masivos DdoS

Los dispositivos IoT comprometidos pueden ser utilizados como parte de botnets para lanzar ataques masivos de denegación de servicio distribuido (DDoS), como se vio en el ataque de Mirai Botnet en 2016.

## Gestión segura de dispositivos

La integración de soluciones de ciberseguridad en IoT, como el cifrado de extremo a extremo y la autenticación multifactor, es clave para proteger estos dispositivos y las redes a las que están conectados.

## Segmentación de redes IoT

Mantener los dispositivos IoT en redes segmentadas puede limitar el alcance de un ataque, evitando que un dispositivo comprometido comprometa toda la infraestructura.

# Ejemplo de invento tecnológico

## Plataformas de seguridad para IoT

Empresas como Armis han desarrollado soluciones específicas para proteger entornos de IoT mediante el monitoreo continuo de dispositivos y la detección de amenazas en tiempo real.