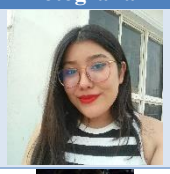
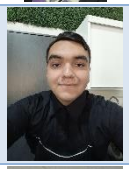
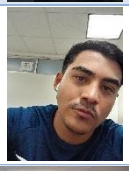
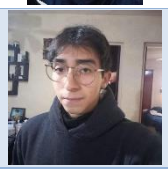
UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FIME
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

| | |
|---|---|
| **Unidad de Aprendizaje** | Sistemas Operativos |
| **Grupo** | 006 |
| **Periodo Escolar** | Agosto-Diciembre 2024 |
| **Profesor** | Dra. Norma Edith Marín Martínez |
| **Actividad** | Fundamental #4 |
| **Equipo** | #4 |

| Fotografía | Matrícula | Apellidos | Nombre(s) | PE | Participación |
|---|---|---|---|---|---|
|  | 1934482 | Aguilar Moreno | Alondra Guadalupe | IAS | 95% |
|  | 1973188 | Gallegos Moreno | Laura Alicia | ITS | 92% |
|  | 2003718 | Cruz Bernal | Cassandra Lizbeth | ITS | 90% |
|  | 1996031 | Bustos Pérez | Raymond | ITS | 95% |
|  | 2052020 | López Chávez | Gerardo Haziel | IAS | 85% |
|  | 1737931 | Pérez Maldonado | Ricardo Daniel | IAS | 83% |
|  | 2128081 | Moreno Barajas | Yahir | ITS | 95% |

20/10/2024

# INDICE

# Introducción

Las redes y la seguridad en sistemas distribuidos son dos pilares fundamentales en el mundo tecnológico actual. Con la creciente dependencia de la digitalización en todos los aspectos de nuestra vida, desde el entretenimiento hasta las transacciones financieras y la atención médica, la necesidad de redes robustas y seguras se ha vuelto más crítica que nunca. En este contexto, los sistemas distribuidos emergen como una solución clave para manejar la complejidad y las demandas de los servicios y aplicaciones modernas.

Un sistema distribuido se refiere a una colección de computadoras independientes que aparecen para el usuario como una única computadora coherente. Estos sistemas permiten que múltiples dispositivos trabajen juntos para lograr un objetivo común, distribuyendo la carga de trabajo y proporcionando redundancia para mejorar la confiabilidad y el rendimiento. Sin embargo, la naturaleza distribuida de estos sistemas introduce desafíos únicos en términos de comunicación, coordinación y seguridad.

Además de la eficiencia y la velocidad, la seguridad de la red es un aspecto crítico que no puede ser pasado por alto en los sistemas distribuidos. La transmisión de datos entre los nodos del sistema debe ser segura y protegida contra amenazas como el espionaje, la manipulación y el acceso no autorizado. Las técnicas de cifrado, los protocolos seguros y las medidas de autenticación son esenciales para proteger la integridad y la confidencialidad de la información que circula a través de la red.

La seguridad en sistemas distribuidos va más allá de la protección de la red y abarca aspectos como la autenticación de usuarios, el control de acceso, la auditoría y la recuperación ante desastres. Con múltiples nodos interactuando entre sí, es fundamental implementar políticas de seguridad coherentes y robustas que se apliquen de manera uniforme en todo el sistema distribuido. Esto requiere una planificación cuidadosa, una implementación meticulosa y una vigilancia continua para detectar y mitigar cualquier vulnerabilidad o brecha de seguridad que pueda comprometer la integridad del sistema.

Los sistemas distribuidos también presentan desafíos únicos en términos de coordinación y gestión de recursos. La escalabilidad, la disponibilidad y la tolerancia a fallos son características esenciales que deben ser cuidadosamente diseñadas e implementadas para garantizar un rendimiento óptimo y una operación sin problemas. Las técnicas como el balanceo de carga, la replicación de datos y los algoritmos de consenso son fundamentales para optimizar la utilización de los recursos y garantizar la continuidad del servicio incluso en caso de fallos o interrupciones inesperadas.

En conclusión, las redes y la seguridad en sistemas distribuidos son áreas interconectadas que desempeñan un papel crucial en la construcción de infraestructuras tecnológicas robustas y confiables en el mundo digital de hoy. La evolución continua de la tecnología y la creciente interconexión de dispositivos y sistemas plantean nuevos desafíos y oportunidades que requieren una atención cuidadosa y una innovación constante en el diseño, la implementación y la gestión de redes y sistemas distribuidos seguros y eficientes.

# Amenazas de la seguridad

Como sabemos en la era digital, la seguridad de los sistemas informáticos se ha convertido en una preocupación central para individuos, empresas y gobiernos. Con el crecimiento exponencial de la información digital y la dependencia de las tecnologías de la información, la identificación y compresión de la vulnerabilidades y amenazas se han vuelto esencial para garantizar la integridad, la identificación y comprensión de las vulnerabilidades y amenazas se ha vuelto esencial para garantizar la integridad, confidencialidad y disponibilidad de datos. Existen tres grupos de amenazas en las cuales se enfrentan los sistemas informáticos.

## Desastres del entorno.

Estos son entornos naturales o causados por el hombre que pueden tener un impacto devastador en la infraestructura y operación de los sistemas informáticos. Entre las amenazas más comunes se encuentran:

- *Desastres naturales.*

Inundaciones, terremotos, huracanes e incendios forestales pueden causar daños físicos a los centros de datos y equipos, afectando así la disponibilidad y recuperación de la información.

- *Fallos de la energía.*

Interrupciones en los suministros eléctrico o fluctuación de voltaje puede provocar la perdida de datos y daños en los equipos electrónicos.

- *Fallos de Hardware.*


El envejecimiento, el desgaste y los defectos de los componentes hardware pueden llevar a fallos inesperados y pérdida de información.

## Amenazas en el Sistema.

Se refieren a las vulnerabilidades y ataques dirigidos específicamente contra el software, aplicaciones y configuraciones de los sistemas informáticos. Algunas de las amenazas más relevantes incluyen:

- *Malware.*

Software malicioso como virus, gusanos, troyanos y ransomware que pueden comprometer la integridad y confidencialidad de la información.

- *Vulnerabilidades del Software.*

Errores de programación y fallos de seguridad en aplicaciones y sistemas operativos que pueden ser explotados por los atacantes para acceder y controlar los sistemas.

### Amenazas en la Red.

Se relacionan con los riesgos asociados a la transmisión y comunicación de datos a través de redes publicas y privadas, las amenazas más comunes en este ámbito son la intercepción de datos, ataques de Phishing o ataques.

La seguridad de los sistemas informáticos es un desafío constante que requiere una comprensión profunda de las vulnerabilidades y amenazas que pueden afectar a los sistemas en diferentes ámbitos. Adoptar una estrategia de seguridad integral, que abarque la protección contra desastres del entorno, amenazas en el sistema y amenazas en la red, es esencial para garantizar la protección y resiliencia de los sistemas informáticos en el mundo digital actual.

## Tipos de virus

Los virus informáticos son programas o fragmentos de código malicioso diseñados para poder infectar y dañar los sistemas informáticos, robar información o tomar el control de dispositivos.

### Gusanos malware

Son programas maliciosos que se propagan automáticamente a través de redes informáticas sin la intervención del usuario. Los gusanos no necesitan adjuntarse a un archivo ejecutable para infectar un sistema. Una vez que un gusano infecta un dispositivo, pueden estos replicarse y enviar copias de si mismo a otros dispositivos conectados a la misma red.

Estos gusanos pueden causar una variedad de problemas, como la degradación del rendimiento del sistema, la interrupción de servicios de redes y el robo de información personal.

### Troyano

Son programas maliciosos que se disfrazan como software legitimo para engañar a los usuarios y hacer que instalen el malware en sus dispositivos. Una vez instalado, un troyano puede permitir a los ciberdelincuentes acceden y controlar el sistema infectado de forma remota. Estos troyanos pueden ser utilizados para robar información sensible, como contraseñas y datos bancarios, o para instalar otros tipos de malware en el sistema comprometido.

### Spyware

El tipo de malware diseñado para recopilar información sobre las actividades de los usuarios sin su conocimiento o consentimiento. Esto puede incluir la captura de datos de navegación, el registro de pulsaciones de teclas, la monitorización de mensajes de correo electrónico y la recopilación de

información personal. El spyware puede ser utilizado con fines publicitarios, para rastrear el comportamiento del usuario o para robar información sensible.

La presencia de spyware en un sistema puede comprometer la privacidad y la seguridad de los usuarios, y puede llevar a la exposición de información personal y financiera.

### Adware

Es un tipo de malware que muestra anuncios no deseados en el dispositivo infectado. Aunque el adware puede parecer menos peligroso que otros tipos de malware, puede ser muy molesto y afectar algunos programas de adware puede recopilar información sobre los hábitos de navegación de los usuarios y compartir estos datos con terceros sin su consentimiento. En algunos casos, el adware puede ser vinculado a otros tipos de malware, como spyware o ransomware, que pueden causar daños mas graves en el sistema infectado.

### Ransomware

Este tipo de malware que cifra los archivos del sistema infectado y exige un rescate para restaurar el acceso a los datos. Una vez que se infecta un dispositivo, bloquea los archivos y muestra un mensaje de rescate solicitando un pago a cambio de la clave de descifrado. Aquí los ciberdelincuentes suelen exigir el pago en criptomonedas para dificultar el seguimiento de las transacciones. Este puede causar perdidas de datos importantes, interrupciones en las operaciones comerciales y daños financieros significativos para las víctimas.

Para poder protegerse contra estos tipos de virus informáticos, es esencial tomar medidas de seguridad proactivas, como mantener el software y los sistemas operativos actualizados, utilizar programas antivirus y antimalware de confianza, evitar el hacerle clic en enlaces o descarga adjuntos de fuentes desconocidas, y realizar copias de seguridad regulares de los datos importantes.

## Tipos de intrusos

### Hackers.

Son profesionales de la seguridad de la informática que buscan vulnerabilidades en sistemas y redes para mejorar la seguridad. Actúan dentro de un marco legal y con permiso explicito.

### Crackers o Hackers Maliciosos.

Son individuos o grupos que buscan explorar vulnerabilidades con fines maliciosos, como robo de datos, fraudes o daño a sistemas.

### Script Kiddies.

Son individuos con conocimientos informáticos básicos que utilizan herramientas y scripts preexistentes para llevar a cabo ataques sin entender completamente como funcionan.

### Insiders Maliciosos.

Son empleados o personas con acceso legitimo a un sistema que abusan de sus privilegios para causar daño o robar información.

### Botnets.

Son redes de dispositivos comprometidos que son controlados remotamente por un atacante para llevar a cabo ataques masivos, como ataques DDoS.

### Sniffers.

Son individuos que se decían a rastrear y tratar de recomponer y descifrar los mensajes que circulan por redes de ordenadores como internet.

### Spammers.

Son los responsables del envío masivo de miles de mensajes de correo electrónico no solicitados a través de redes como Internet, provocando el colapso de los servidores y la sobrecarga de los buzones de correo de los usuarios.

### Piratas informáticos.

Son los individuos especializados en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre propiedad intelectual.

## Tipos de autentificaciones

Este es el proceso que debe de seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quien es) y autenticación (demostrar que el usuario es quien dice ser). La autentificación por si sola no verifica derechos de acceso del usuario.

### Autenticación basada en conocimiento.

Este método requiere que el usuario proporcione información secreta, como contraseñas, PIN o respuestas a preguntas de seguridad.

### Autenticación basada en posesión.

Implica el uso de dispositivos físicos como tarjetas inteligentes, tokens OPT o llaves USB de seguridad.

### Autenticación basada en características físicas.

Utiliza rasgos físicos únicos del usuario, como huellas dactilares, reconocimiento facial , iris o voz.

### Autenticación basada en comportamiento.

Analiza el comportamiento del usuario al interactuar con un sistema, como patrones de escritura, clics del mouse o hábitos de navegación.

## Niveles de seguridad

Los niveles de seguridad son esenciales para poder proteger información, sistemas y redes contra amenazas y ataques. Estos niveles varían dependiendo del entorno en el que se encuentren y los activos que se pretenden proteger.

En la clasificación del Departamento de Defensa de los Estados Unidos de Norte América estos niveles permiten imponer limites y condiciones que debe reunir un sistema completo para alcanzar un esquema determinado de seguridad tanto en Hardware, Software o Datos. Los niveles son D, C, B y A, de menor a mayor seguridad, teniendo a su vez algunas subdivisiones.

### Nivel de usuario.

El nivel de seguridad en un usuario se refiere a las prácticas y medidas que adopta un individuo para proteger su información personal y sus dispositivos. Algunas medidas básicas incluyen:

Contraseñas seguras: Utilizar contraseñas robustas y únicas para cada cuenta, combinando letras, números y símbolos.

Autenticación de dos factores (2FA): Activar la 2FA para añadir una capa adicional de seguridad al iniciar sesión en cuentas.

Actualizaciones regulares: Mantener actualizado el sistema operativo y las aplicaciones para protegerse contra vulnerabilidades conocidas.

Conciencia de phishing: Ser consciente de los intentos de phishing y no hacer clic en enlaces sospechosos o proporcionar información personal.

Uso de VPN: Utilizar una red privada virtual (VPN) al conectarse a redes públicas o Wi-Fi no seguras para proteger la información transmitida.

### Nivel de seguridad en una red.

El nivel de seguridad en una red se refiere a las medidas implementadas para proteger la infraestructura de red, los datos que circulan por ella y los dispositivos conectados. Algunas prácticas comunes incluyen:

Firewalls: Implementar firewalls para filtrar el tráfico entrante y saliente, y bloquear actividades maliciosas.

Segmentación de red: Dividir la red en segmentos más pequeños para limitar el acceso a los recursos sensibles.

Detección y prevención de intrusiones (IDS/IPS): Utilizar sistemas de detección y prevención de intrusiones para identificar y bloquear actividades anómalas.

Actualizaciones y parches: Mantener actualizados los dispositivos de red y los sistemas operativos para protegerse contra vulnerabilidades.

Control de acceso: Implementar políticas de control de acceso para limitar quién puede acceder a la red y a qué recursos.

## Nivel de seguridad en una empresa.

El nivel de seguridad en una empresa es más complejo y abarca múltiples aspectos, desde la protección de la infraestructura de TI hasta la gestión de riesgos y la formación de empleados. Algunas medidas clave incluyen:

Políticas de seguridad: Establecer políticas y procedimientos de seguridad claros y documentados que guíen las prácticas de seguridad en toda la organización.

Gestión de identidad y acceso (IAM): Implementar soluciones IAM para gestionar y controlar el acceso a los recursos y datos de la empresa.

Auditorías de seguridad: Realizar auditorías periódicas para evaluar y mejorar la postura de seguridad de la empresa.

Formación y concienciación: Capacitar a los empleados en prácticas de seguridad y concienciarles sobre los riesgos de seguridad.

Respuesta a incidentes: Establecer un plan de respuesta a incidentes para manejar y mitigar los incidentes de seguridad de manera efectiva.

Los niveles de seguridad en un usuario, en una red y en una empresa son fundamentales para proteger la información y los activos contra amenazas y ataques. Adoptar medidas de seguridad adecuadas en cada nivel y mantenerse actualizado sobre las mejores prácticas de seguridad son clave para mantener un entorno seguro y protegido.

# Conclusión.

En el panorama actual de la era digital, la seguridad informática se ha convertido en una piedra angular para individuos, empresas y gobiernos. Con el crecimiento exponencial de la información digital y la creciente dependencia de la tecnología de la información, la identificación y comprensión de las vulnerabilidades y amenazas se han vuelto cruciales para garantizar la integridad, confidencialidad y disponibilidad de los datos.

Las amenazas a la seguridad de los sistemas informáticos se pueden agrupar en tres categorías principales: desastres del entorno, amenazas en el sistema y amenazas en la red. Los desastres del entorno pueden ser tanto naturales como provocados por el hombre, como inundaciones, terremotos, fallos de energía y fallos de hardware, que pueden causar daños físicos a los centros de datos y equipos, afectando así la disponibilidad y recuperación de la información. Por otro lado, las amenazas en el sistema se refieren a vulnerabilidades y ataques dirigidos específicamente contra el software, aplicaciones y configuraciones de los sistemas informáticos, como el malware y las vulnerabilidades del software. Finalmente, las amenazas en la red están relacionadas con los riesgos asociados a la transmisión y comunicación de datos a través de redes públicas y privadas, como la intercepción de datos y los ataques de phishing.

Entre los tipos de virus informáticos más comunes se encuentran los gusanos, troyanos, spyware, adware y ransomware. Estos programas maliciosos pueden causar una variedad de problemas, desde la degradación del rendimiento del sistema y la interrupción de servicios de redes hasta el robo de información personal y financiera. Además, los tipos de intrusos que pueden comprometer la seguridad informática incluyen hackers, crackers, script kiddies, insiders maliciosos, botnets, sniffers, spammers y piratas informáticos. Cada uno de estos actores tiene sus propias motivaciones y técnicas para llevar a cabo ataques maliciosos, que van desde el robo de datos y fraudes hasta el daño a sistemas y redes.

En conclusión, podemos decir que la seguridad de los sistemas informáticos es un desafío constante que requiere una comprensión profunda de las vulnerabilidades y amenazas que pueden afectar a los sistemas en diferentes ámbitos. Adoptar una estrategia de seguridad integral, que abarque la protección contra desastres del entorno, amenazas en el sistema y amenazas en la red, es esencial para garantizar la protección y resiliencia de los sistemas informáticos en el mundo digital actual. Además, es crucial que los usuarios, las redes y las empresas adopten medidas de seguridad proactivas y mantengan una postura de seguridad sólida y actualizada para proteger la información y los activos contra las amenazas y ataques en constante evolución.

**Conclusión individual.**

## Yahir Moreno Barajas

Dia con día, la seguridad Informática se convierte cada vez más en un tema más presente e importante, es lógico que, conforme el uso de la tecnología incrementa en nuestra sociedad, el número de ataques y advertencies que hay que seguir, también aumentará. Es por esto que, la seguridad es un tema súmamente importante, el cual todas las personas que habitúan usar tecnología deben aprender. Así mismo, es igual de importante ver hacia el pasado, sobre las consecuencias que han dejado previos ciber ataques masivos, para estudiarlos y llegar a soluciones justo antes de que algún nuevo ciber ataque ocurra, o, por defecto, si este llegase a ocurrir, poder controlar los daños que este cause y no se vuelva de carácter global como lo ha pasado con otros virus en el pasado.

## Alondra Guadalupe Aguilar Moreno

En resumen, enfatiza la relevancia crítica de la seguridad informática ante las múltiples amenazas que pueden comprometer los sistemas, ya sea por desastres naturales o ataques cibernéticos. Se destaca la necesidad de adoptar medidas de protección sólidas y actualizadas, junto con la educación continua de los usuarios, como elementos esenciales para reducir riesgos como el malware, el robo de datos y las vulnerabilidades del sistema. Solo mediante un enfoque integral y preventivo es posible asegurar la protección y la estabilidad de los sistemas en el mundo digital actual.

## Cassandra Lizbeth Cruz Bernal

Para concluir puedo decir que el conocer sobre todos estos tipos de amenazas que existen y el saber cómo evitarlas es de gran importancia para nosotros ya que nuestro futuro literalmente depende de la tecnología y debemos de ser lo más cuidadosos posibles a la hora de trabajar.

## Ricardo Daniel Pérez Maldonado

En la actualidad la era digital ya es muy demandante para el mundo; por eso desde el inicio de la red se han implementado medidas de seguridad más fuertes para mantener segura la información de usuarios, clientes, empresas que con el paso de tiempo tienen que actualizarse para poder estar seguros ante los tipos de amenazas que existen en la red; ya que como sabemos nadie está exento de algún ataque; por eso es importante resolver alguna vulnerabilidad de nuestros dispositivos en la que esos ataques se puedan centrar para robar algún tipo de información confidencial o realizar algún otro atraco. Un ejemplo; podría ser es como los Bancos que tienen información confidencial de clientes y realizan transacciones financieras; su nivel de seguridad es extremadamente alto y deben tener esa política y redes de seguridad enormes; es increíble como a lo largo de los años esto se fue actualizando ya que años atrás podríamos decir que eran más

vulnerables a ataques. Con la creciente dependencia de la digitalización se ha hecho la necesidad ya de tener una red de seguridad critica; ir actualizando sobre los tipos de amenazas, adaptar estrategias para poder tener sistemas o software seguros.

## Gerardo Haziel Lopez Chavez

Para concluir con este tema, solo me queda decir que debemos cuidar nuestra información personal. Es súper importante hoy en día, porque enfrentamos cosas como desastres naturales, virus y hackers. Tener una estrategia completa es clave para mantener seguros nuestros datos y sistemas. También, es esencial estar siempre al tanto de las actualizaciones de software y educar a todos sobre cómo reconocer las amenazas. Esto nos ayuda a estar un paso adelante y proteger nuestra información personal.

## Laura Alicia Gallegos Moreno

Las redes y la seguridad en sistemas son fundamentales para garantizar la integridad, confidencialidad y disponibilidad de los datos y servicios en un entorno digital. A medida que las redes se expanden y las amenazas cibernéticas se vuelven más sofisticadas, asegurar las infraestructuras de TI es un desafío continuo. Una conclusión clave es que no existe una solución única que garantice una seguridad completa. Es necesario implementar una combinación de buenas prácticas, herramientas, y tecnologías avanzadas (como firewalls, sistemas de detección de intrusos, criptografía, y autenticación multifactorial) junto con una cultura de ciberseguridad sólida. Además, la vigilancia constante, actualizaciones regulares y la educación de los usuarios son esenciales para mitigar riesgos y reducir vulnerabilidades.

## Raymond Bustos Perez

En un entorno cada vez más digital, la seguridad informática se ha vuelto esencial para proteger la información y los sistemas frente a una amplia gama de amenazas. Estas se agrupan en tres categorías principales: desastres del entorno, amenazas en el sistema y amenazas en la red. Cada una de ellas plantea riesgos que pueden afectar la integridad, confidencialidad y disponibilidad de los datos. Los ataques pueden provenir tanto de desastres naturales como de actores malintencionados, como virus informáticos y hackers. Ante este panorama, es imprescindible adoptar una estrategia de seguridad integral que incluya protección ante estos riesgos y que las organizaciones y usuarios mantengan medidas de seguridad proactivas y actualizadas. Solo así se puede asegurar la resiliencia y protección de los sistemas en el mundo digital actual.

# Bibliografia

Stallings, W. (2017). Computer Security: Principles and Practice. Pearson.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.

Cisco. (2020). Cisco Annual Internet Report (2018–2023). Cisco Systems, Inc.

"Understanding Computer Viruses: What They Are and How to Protect Against Them", Norton, disponible en: https://www.norton.com

"Types of Malware and How to Defend Against Them", McAfee.

"Ransomware: A Cybersecurity Threat Overview", Cybersecurity and Infrastructure Security Agency (CISA).

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson Education.

Whitman, M. E., & Mattord, H. J. (2018). Principios de seguridad de la información. Cengage Learning.