ACTIVIDAD FUNDAMENTAL 4.- MULTITAREA: REDES Y SEGURIDAD: SISTEMAS DISTRIBUIDOS

EQUIPO 2:

JOSUE CARLOS MORENO MAGALLANES 1846526 ITS

ELIUD JONATHAN LUCIO GARCÍA 2000116 ITS

EMILIO DE JESUS IBARRA GUTIERREZ 2000396 IAS

VICTOR ALFONSO DELGADO BAUTISTA 2006517 IAS

DAMARIS HERNANDEZ HERNANDEZ 2005278 IAS

GREGORIO MARTINEZ MARTINEZ 2014975 IAS

INDICE

Introducción

En un mundo cada vez más conectado y digitalizado, la multitarea, las redes y la seguridad son elementos fundamentales de la infraestructura tecnológica actual. En este contexto, los sistemas descentralizados se han convertido en la base de la gestión de recursos, la comunicación eficaz y la protección de datos en un entorno cada vez más complejo.

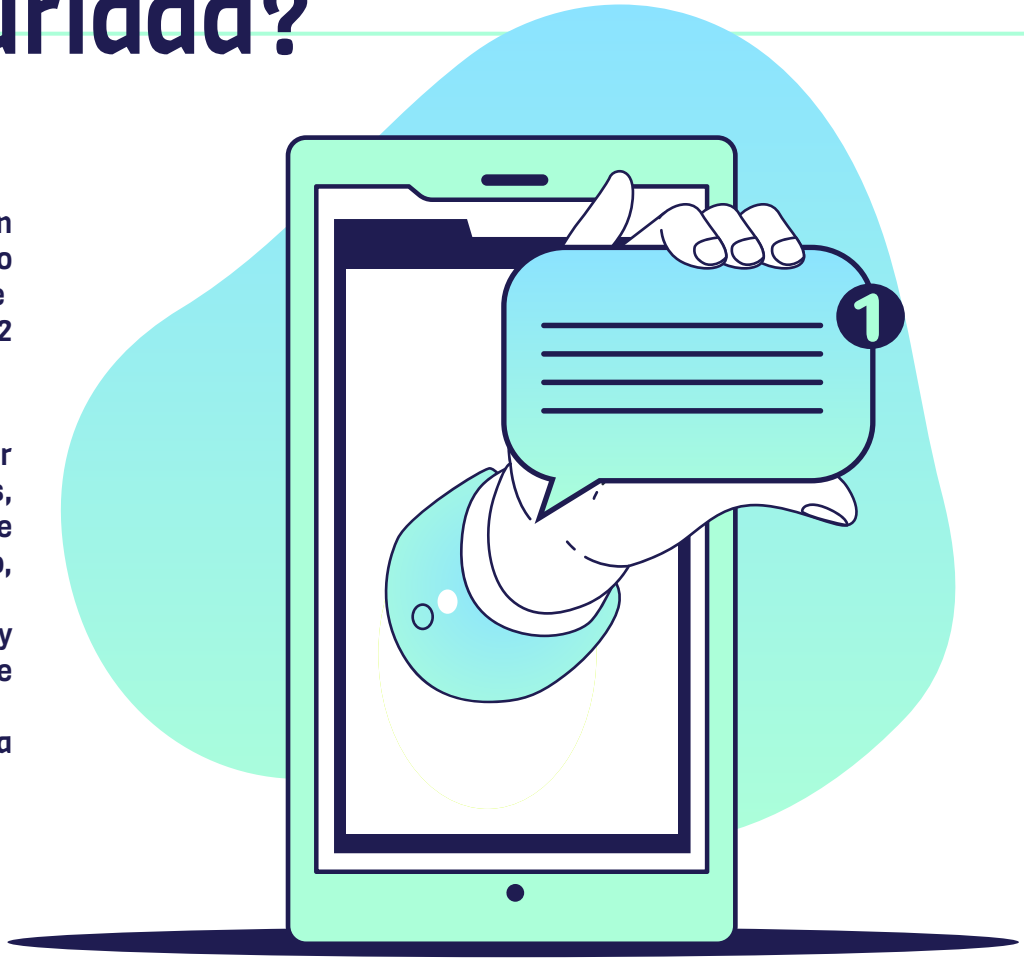
Los sistemas distribuidos se caracterizan por la distribución de recursos y tareas entre múltiples nodos interconectados, proporcionando mayor rendimiento y escalabilidad.

Esta arquitectura no sólo facilita la multitarea, sino que también plantea importantes desafíos de seguridad y gestión de datos, ya que la información debe fluir de forma segura a través de redes heterogéneas y, a menudo, públicas. Esta introducción explora la intersección de la multitarea, las redes y la seguridad en un entorno de sistemas distribuidos.

¿Qué es la seguridad?

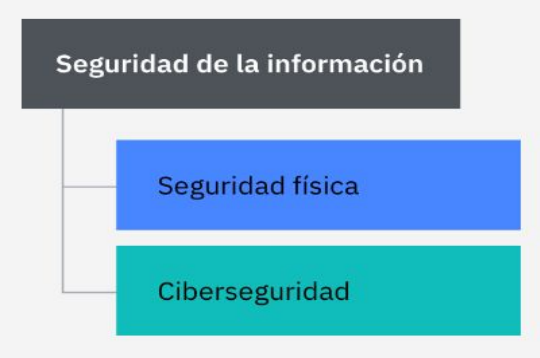
Para comprender esto, se debe saber que la seguridad en este ámbito es parte de lo que se conoce como "**seguridad de la información**", esta se encarga de proteger los datos almacenados y como tal funciona por 2 engranajes que mueven este paradigma:

- La seguridad física es la práctica de proteger físicamente activos como, por ejemplo, edificios, cámaras de seguridad, equipos y propiedades de amenazas físicas como robos, vandalismo, incendios y desastres naturales.
- La ciberseguridad es la práctica de proteger y recuperar redes, dispositivos y programas de cualquier tipo de ciberataque malicioso.
- Una buena seguridad no puede tener la una sin la otra, y ambas deben buscar los mismos objetivos.



LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se centra en el valor de la información que estamos intentando proteger, en lugar de en cómo la protegemos. El siguiente diagrama muestra que bajo la seguridad de la información hay elementos físicos y elementos digitales.



Los objetivos de la seguridad de la información a menudo se definen utilizando la tríada CID como punto de partida. CID es el código mnemónico de los tres objetivos: Confidencialidad, Integridad y Disponibilidad.

Confidencialidad *La información es privada*	Confidencialidad significa evitar que la información caiga en manos de personas no autorizadas para acceder a ella.
Integridad *La información no se ha alterado*	Integridad significa asegurarse de que la información permanece exacta y coherente, y garantizar que personas no autorizadas no puedan realizar cambios en ella.
Disponibilidad *Se puede acceder a la información siempre que sea necesario*	Disponibilidad significa acceso oportuno y fiable, y uso de la información cuando sea necesario.

ELEMENTOS CLAVE

Tecnología

La tecnología es toda la infraestructura subyacente. En la ciberseguridad, suele incluir elementos como el cifrado de dispositivos, las defensas de perímetro de red y las tecnologías anti-malware.

Personas

La acción humana es de lejos la principal causa de incidencias de ciberseguridad.

Proceso

En los negocios, la mayoría de las actividades siguen un conjunto de pasos claramente definido. Estos procesos pueden ayudar a la ciberseguridad, teniendo en cuenta la seguridad en cada uno de los pasos, o dificultar la ciberseguridad, frustrando al usuario final.

AMENAZAS

Las amenazas pueden agruparse tanto en los tipos de delincuentes, actores de amenaza, los tipos de ciberataques, razones detras, metodologias, estructuras e incluso hasta en la rentabilidad y tiempo de recuperación de un ataque.

Los actores de amenaza-intrusos

Son grupos diferentes y varían significativamente en motivación, recursos y técnicas.

1. **SCRIPT KIDDIE:** Hace referencia a aquellas personas que utilizan programas, normalmente herramientas de hackeo básicas, sin entender verdaderamente qué ocurre entre bastidores.
2. **HACKTIVISTA:** Hactivista es un término que combina "hacker" y "activista". Los hactivistas buscan un cambio político o económico y utilizarán el hackeo para conseguirlo.
3. **BANDAS:** Las bandas pueden ser desde pocas personas organizadas hasta multinacionales con cientos de miembros. Dentro de cada banda, a menudo hay especialistas que pueden comercializar con la información en la dark web.

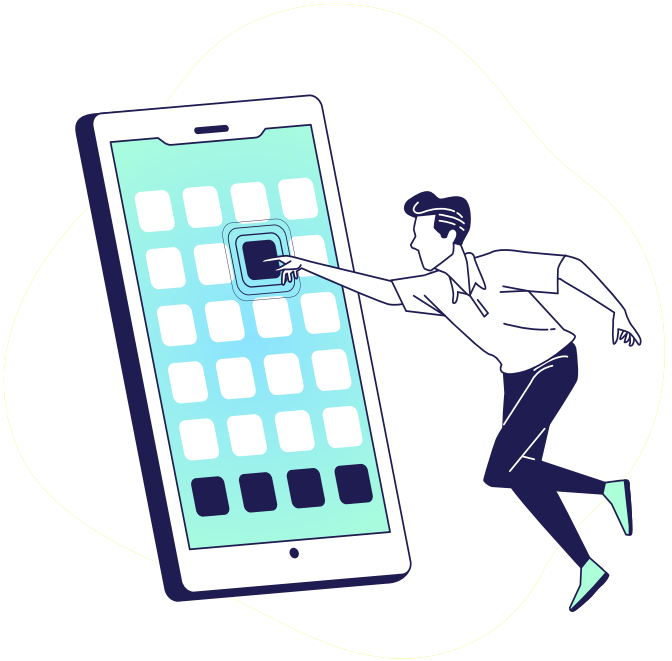
Los actores de amenaza-intrusos

4. HACKER DE ESTADO-NACIÓN:

¿Quiénes son?	¿Cuál es su objetivo?
Especialistas altamente cualificados y entrenados	Seguir planes estratégicos de varios años en una amplia gama de cuestiones
¿Qué recursos tienen?	**¿Cómo puede protegerse contra ellos?**
Presupuestos enormes, herramientas muy avanzadas e investigación puntera	Es increíblemente difícil; se requieren defensas totalmente coordinadas en todos los aspectos de la organización

5. AMENAZA INTERNA:

¿Quiénes son?	¿Cuál es su objetivo?
Miembros del personal que trabajan contra los intereses de una organización, ya sea deliberada o accidentalmente	Venganza o motivos financieros
¿Qué recursos tienen?	**¿Cómo puede protegerse contra ellos?**
No se requiere presupuesto ni tampoco recursos; utilizan el acceso que ya tienen	Supervisar el personal atentamente y garantizar que la cultura de la organización sea eficaz en la prevención de estos problemas



TIPOS DE ATAQUE

Hay muchos métodos con los que un ciberatacante puede entrar y explotar un sistema. A menudo, los ataques no son técnicos, sino una explotación de cómo las personas interactúan con el sistema de forma equivocada y vulnerable.

- **Ataque de Denegación de servicio (DoS):** Un ataque DoS es cualquier tipo de ataque que dé como resultado una caída del sistema completa o parcial.
- **Ataque de Denegación de servicio distribuida (DDoS):** Un ataque DDoS es un ataque DoS que proviene de más de una fuente al mismo tiempo.
- **Ataque de suplantación de identidad:** Un ataque de suplantación de identidad es la práctica de enviar mensajes que parecen de fuentes de confianza con el objetivo de obtener información personal o influir en los usuarios para que realicen una acción.
- **Ataque de suplantación de identidad focalizado:** Los atacantes dedican tiempo a realizar investigaciones de los destinos y crear mensajes personales y relevantes que, por lo tanto, son más efectivos.

TIPOS DE VIRUS

Malware es un término general para el software malicioso. Es un software diseñado para afectar negativamente a un usuario de destino sin el consentimiento informado del mismo.

1. **Virus informático:** Un virus es un programa malicioso que se adjunta a un archivo o programa legítimo y se ejecuta cuando el archivo infectado se abre. Los virus pueden dañar, modificar o eliminar datos en tu computadora.

2. **Gusano informático:** A diferencia de los virus, los gusanos no necesitan infectar archivos. Se propagan a través de redes y sistemas aprovechando vulnerabilidades para replicarse y causar daño, cómo ralentizar redes o robar información.

3. **Troyano (Trojan):** Los troyanos son programas maliciosos que se hacen pasar por aplicaciones legítimas. Una vez que el usuario los instala, pueden realizar acciones no deseadas en el sistema, como robar información, abrir puertas traseras para atacantes o dañar el sistema.

4. **Spyware:** Estos programas recopilan información del usuario sin su consentimiento. Pueden rastrear la actividad en línea, registrar contraseñas y robar datos personales.

Ransomware

05

El ransomware encripta los archivos de la víctima y luego exige un rescate para desbloquearlos.

Adware

06

El adware muestra anuncios no deseados en el sistema de un usuario.

Rootkit

07

Un rootkit es un conjunto de herramientas que permite a un atacante acceder y controlar de manera sigilosa un sistema, generalmente ocultando su presencia.

Botnet:

08

Una botnet es una red de computadoras infectadas que son controladas por un atacante de forma remota.

Keylogger

09

Un keylogger registra las pulsaciones de teclado de un usuario sin su conocimiento.

Scareware

10

Scareware es un software falso que muestra mensajes de advertencia falsos o alarmantes en un intento de asustar.

AUTENTICACIONES

Autenticación es el proceso que debe 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 quién es) y autenticación (demostrar que el usuario es quien dice ser). La autenticación por sí sola no verifica derechos de acceso del usuario; estos se confirman en el proceso de autorización.

En general, la seguridad de las redes de datos requiere para conceder acceso a los servicios de la red, tres procesos: (1) autenticación, (2) autorización y (3) registro.

- Autenticación: el proceso por el cual el usuario se identifica en forma inequívoca; es decir, sin duda o equivocación de que es quien dice ser.
- Autorización: el proceso por el cual la red de datos autoriza al usuario identificado a acceder a determinados recursos de la misma.
- Registro: el proceso mediante el cual la red registra todos y cada uno de los accesos a los recursos que realiza el usuario, autorizado o no.

Estos tres procesos se conocen por las siglas en inglés como AAA, o Authentication, Authorization, y Accounting.

TIPOS DE AUTENTICACIONES

Se puede efectuar autenticación usando uno o varios de los siguientes métodos:

- Autenticación por conocimientos: basada en información que sólo conoce el usuario.
- Autenticación por pertenencia: basada en algo que posee el usuario.
- Autenticación por características: basada en alguna característica física del usuario.

TIPOS DE AUTENTICACIONES QUE PODEMOS APLICAR EN USUARIOS, REDES, EMPRESA, ETC.

Autenticación por usuario y contraseña: la protección de los datos depende del usuario, ya que cada uno elige qué contraseña o PIN tendrá. Sin embargo, un problema es que los hackers pueden captar esta información, lo que vulnera la seguridad del esquema de seguridad propuesto.

Autenticación biométrica: se basa en la lectura de alguna característica física única del individuo, como una huella dactilar, un escaneo del iris o incluso la voz. Esta es una forma muy efectiva para que los sistemas validen que la persona que solicita acceso es quien dice ser.

TIPOS DE AUTENTICACIONES QUE PODEMOS APLICAR EN USUARIOS, REDES, EMPRESA, ETC.

Autenticación dos factores: el usuario necesariamente debe tener disponible el canal adicional en el proceso de inicio de sesión. Si tenemos que ingresar el nombre de usuario y la contraseña en los campos de una página web en la primera etapa de acceso y luego esperar el envío de un código por SMS al celular, necesitamos tener el dispositivo con nosotros para completar el acceso.

Autenticación por sesión: en este modelo el usuario puede autenticarse con usuario y contraseña o por algún otro método.El servidor, a su vez, crea una sesión en su memoria o base de datos y devuelve la información del usuario a través de una cookie con el identificador de la sesión creada.

TIPOS DE AUTENTICACIONES QUE PODEMOS APLICAR EN USUARIOS, REDES, EMPRESA, ETC.

Autenticación token: se creará un token que el usuario recibirá como respuesta y que le permitirá acceder a algún recurso. El estándar adoptado por una gran cantidad de aplicaciones web en la actualidad es el formato JWT (JSON Web Token) y hará que el token se firme correctamente para autenticar la solicitud a un recurso en el servidor.

Autenticación por sesión VS Token JWT: el servidor mantiene el estado de la sesión con la información del usuario, que se puede almacenar en una base de datos o en la memoria (Stateful). Con esta estrategia, podemos encontrarnos con problemas como límites de hardware. El consumo excesivo de memoria puede incluso hacer que la máquina se bloquee, dada la cantidad de llamadas al Garbage Collector,(recolector de elementos no utilizados).

ANÁLISIS DE POSIBLES PROBLEMAS

La ciberseguridad es una preocupación creciente en el mundo digital actual, con una amplia gama de amenazas potenciales que pueden afectar a individuos, empresas y gobiernos. Algunos problemas clave que han sido históricamente problemáticos y podrían continuar siéndolo en el futuro:

1. **Malware y ransomware:** Programas maliciosos que bloquean sistemas y exigen rescate.
2. **Phishing y spear phishing:** Correos electrónicos falsos que buscan engañar a los usuarios para obtener información confidencial.
3. **Fugas de datos y violaciones de privacidad:** Exposición de información sensible debido a la recopilación masiva de datos.
4. **Vulnerabilidades de IoT:** Riesgos de seguridad asociados con dispositivos conectados a Internet.
5. **Inseguridad en el software y falta de actualizaciones:** Exposición a amenazas debido a la falta de parches de seguridad en software.
6. **Amenazas de ingeniería social:** Manipulación psicológica para obtener acceso no autorizado.
7. **Ciberataques a infraestructuras críticas:** Ataques dirigidos a sistemas vitales de la sociedad.

Ejemplo común que puede ilustrar un problema de ciberseguridad:

Imagina que recibes un correo electrónico que aparentemente proviene de tu banco, indicando que debes actualizar tu información de cuenta haciendo clic en un enlace adjunto. El correo electrónico se ve auténtico, ya que utiliza el logotipo y los colores del banco, y la dirección de correo electrónico parece legítima.

Sin embargo, este correo electrónico es un caso típico de phishing, una táctica común utilizada por piratas informáticos para obtener información confidencial de los usuarios. Si haces clic en el enlace y proporcionas tu información, los delincuentes podrían acceder a tus datos bancarios, lo que podría resultar en un robo de identidad, pérdida financiera o fraude.

Ejemplo común que puede ilustrar un problema de ciberseguridad:

En este caso, la falta de conciencia sobre la seguridad cibernética podría llevarte a caer en la trampa del phishing. La educación sobre cómo identificar correos electrónicos de phishing y la importancia de no hacer clic en enlaces sospechosos son medidas fundamentales para protegerse contra este tipo de amenaza en la vida diaria.

Este ejemplo resalta la importancia de la educación continua sobre ciberseguridad para protegerse contra las amenazas en línea y mantener la privacidad y seguridad de la información personal.

PREVENCIÓN DE DESASTRES

La prevención de desastres en las redes y la seguridad cibernética son aspectos críticos en el mundo actual, donde la dependencia de la tecnología y la conectividad es fundamental.

PREVENCIÓN DE DESASTRES

Firewalls y Antivirus:

Estos se utilizan para proteger tu red contra intrusiones y malwares. Se necesitan mantener actualizados.

Uso de contraseñas fuertes:

Utilizar contraseñas fuertes y cambiarlas regularmente por cierto tiempo. Usar una combinación de letras, números y caracteres especiales.

Autenticaciones de dos factores::

Habilitar la autenticación de dos factores cuando sea posible añadir una capa adicional de seguridad.

Cifrado de datos:

Utilizar el cifrado para proteger la confidencialidad de datos mientras se transmiten a través de la red.

Ejemplo de la prevención de desastres

Una empresa que no había implementando medidas adecuadas de ciberseguridad y prevención de desastres. Un dia, un empleado abrió un correo electrónico de phishing que contenía un archivo malicioso. Como resultado, la red de la empresa se infecto con un ransomware, un tipo de malware que cifra los archivos de la empresa y exigen un rescate para desbloquear los.

Prevencion:

1- Educar a los empleados para identificar correos electrónicos que puedan contener algún enlace o archivo adjunto sospechoso.

2- Tener un software antivirus y firewall actualizado para detectar y bloquear amenazas conocidas.

3- La empresa debió haber realizado copias de seguridad regulares de sus datos y almacenarlas en un lugar seguro, todo esto para permitir la restauración de datos sin necesidad de pagar un rescate.

4- Mantener un SO y software de la empresa actualizado para ayudar a cerrar posibles vulnerabilidades que los ciberdelincuentes podrían explotar.

Ejemplo de la prevención de desastres

Resultado de las prevenciones:

Gracias a las medidas preventivas, se pudo haber estado mejor preparados para evitar estos ataques de ransomware. En lugar de perder datos y pagar un rescate, podría haber restaurado sus sistemas desde copias de seguridad.

En este ejemplo se pudo observar como se puede prevenir estos ataques, y así la empresa continuar con lo diario. La inversión en medidas preventivas adecuadas pueden ayudar a evitar incidentes costosos y perturbadores.

ADMINISTRACIÓN DE RIESGOS Y SEGURIDAD DE HARDWARE SOFTWARE

En un entorno digital altamente interconectado y vulnerable, la ciberseguridad se ha vuelto crítica. En este contexto, la administración de riesgos y la seguridad de hardware y software desempeñan un papel fundamental para proteger activos digitales y sistemas de información. Para comprender más a fondo la importancia de estos aspectos, consideremos los siguientes puntos clave:

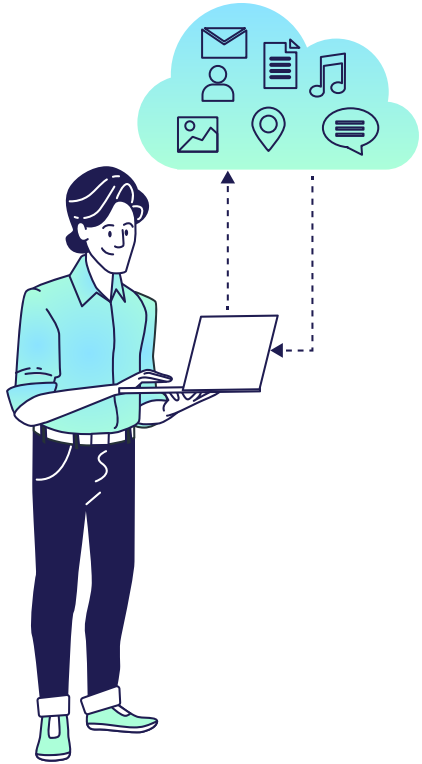
1. Creciente Dependencia Tecnológica: En un mundo donde la tecnología está ampliamente integrada en nuestras vidas, la seguridad se convierte en una prioridad absoluta. ya que la pérdida de acceso o la exposición de información sensible pueden tener consecuencias significativas.

2. Amenazas Cibernéticas Proliferantes: Con el aumento de ataques cibernéticos. La ciberseguridad se vuelve esencial para mitigar estos riesgos y mantener la integridad, confidencialidad y disponibilidad de la información.

Administración de Riesgos en la Ciberseguridad

La administración de riesgos es un proceso integral que se centra en la identificación, evaluación y mitigación de los riesgos de seguridad inherentes a los sistemas informáticos. Este proceso abarca la detección de amenazas potenciales, la implementación de controles de seguridad robustos, el cumplimiento de las normativas pertinentes y la preparación proactiva para manejar incidentes de seguridad.

Además, es importante destacar que la gestión de riesgos no es un evento aislado, sino un proceso continuo que requiere monitoreo y revisión constantes. Esto asegura que los controles de seguridad implementados siguen siendo efectivos frente a las amenazas emergentes y cambiantes. Además, la gestión de riesgos también implica la educación y formación de los usuarios, ya que el factor humano juega un papel crucial en la seguridad de los sistemas informáticos.



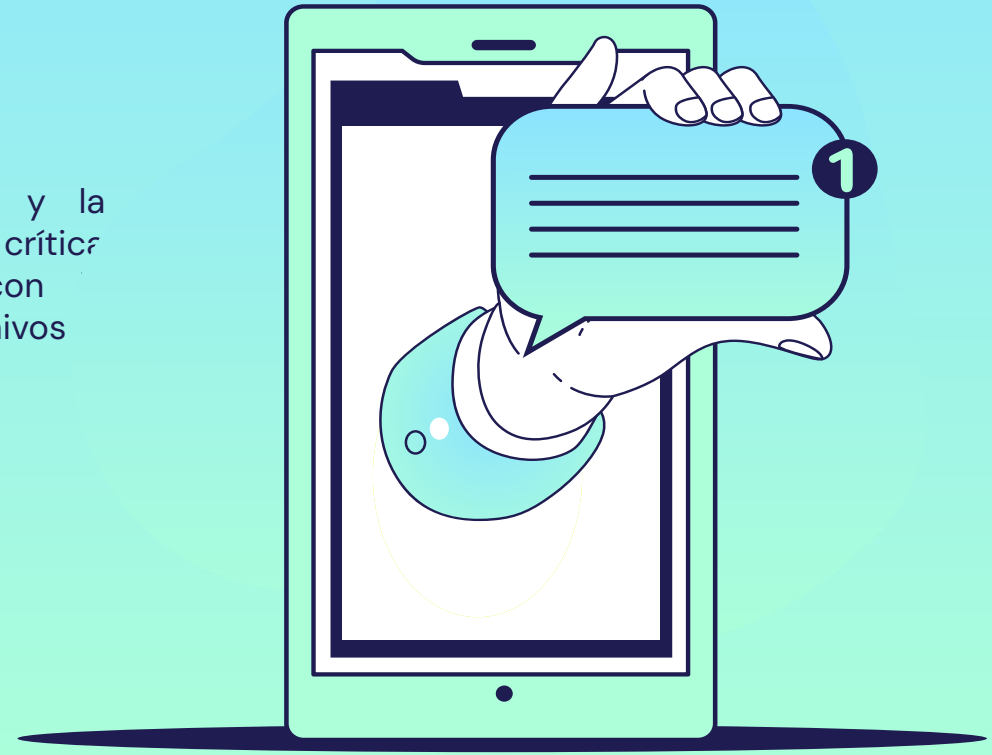
Hardware y Software en la Ciberseguridad

La ciberseguridad depende en gran medida de la seguridad de hardware y software, dos pilares esenciales para garantizar la integridad y confiabilidad de los sistemas digitales. La seguridad de hardware se centra en proteger los componentes físicos de un sistema contra accesos no autorizados y daños, mientras que la seguridad de software salvaguarda programas y sistemas operativos contra amenazas como virus, malware y ataques cibernéticos.

La seguridad de hardware se logra mediante la implementación de sistemas de seguridad en los edificios y sistemas de autenticación biométrica. Además, se utilizan cortafuegos y sistemas de detección de intrusiones para monitorear y proteger la infraestructura de red. Por otro lado, la seguridad de software involucra prácticas de desarrollo seguro, parcheo regular para corregir vulnerabilidades conocidas y el uso de software antivirus para detectar y eliminar amenazas.

Archivos e información y las posibles soluciones al respecto

La creciente dependencia de las redes y la información digital ha llevado a la necesidad crítica de abordar los desafíos relacionados con seguridad de las redes y la gestión de archivos información.



Desafíos en la Seguridad de Redes

Amenazas Cibernéticas:

- El aumento de ataques cibernéticos, como malware, ransomware y phishing, representa una amenaza constante para la integridad de las redes y la información.

Vulnerabilidades de Dispositivos:

- La diversidad de dispositivos conectados a redes, desde computadoras hasta dispositivos IoT, introduce vulnerabilidades que los atacantes pueden explotar.

Falta de Autenticación:

- La debilidad en los mecanismos de autenticación puede llevar a accesos no autorizados y violaciones de la seguridad.

Riesgos en la Nube:

- El almacenamiento y procesamiento en la nube plantean desafíos en términos de seguridad y privacidad de los datos.

Desafíos en la Gestión de Archivos e Información

Exceso de Datos:

- El volumen masivo de datos generados diariamente dificulta su gestión eficiente.

Seguridad de Datos:

- La pérdida de datos y las violaciones de seguridad son riesgos significativos, especialmente cuando se trata de información sensible.

Integridad de los Datos:

- La garantía de la integridad de los datos es esencial para evitar información incorrecta o corrompida.

Cumplimiento Normativo:

- Cumplir con las regulaciones de privacidad y seguridad de datos es un desafío constante.

Soluciones Propuestas

Seguridad de Redes:

- Firewalls Avanzados: Implementación de firewalls avanzados para monitorear y filtrar el tráfico de red, bloqueando amenazas conocidas.
- Sistemas de Detección y Prevención de Intrusiones (IDPS): Utilización de IDPS para detectar actividades maliciosas y prevenir ataques en tiempo real.
- Educación y Concientización: Programas de capacitación para usuarios y personal sobre prácticas seguras en línea y reconocimiento de amenazas.
- Actualizaciones y Parches: Mantenimiento regular y aplicación de actualizaciones y parches de seguridad para sistemas y dispositivos.

Soluciones Propuestas

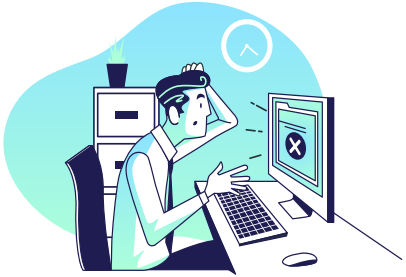
Gestión de Archivos e Información:

- Cifrado de Datos: Implementación de cifrado para proteger la confidencialidad de los datos almacenados y transmitidos.
- Copias de Seguridad Regulares: Establecimiento de rutinas de copias de seguridad para garantizar la disponibilidad y recuperación de datos en caso de pérdida.
- Gestión de Acceso: Control estricto sobre quién tiene acceso a qué datos, utilizando autenticación multifactor y políticas de acceso.
- Monitoreo Continuo: Implementación de herramientas de monitoreo para la detección temprana de irregularidades en la integridad y uso de datos.

Conclusion General

Como conclusión de equipo, nuestra colaboración en la exploración de la ciberseguridad revela que proteger la información digital es un desafío colectivo y en constante evolución. Reconocemos la importancia de implementar soluciones de seguridad sólidas, fomentar la conciencia de los usuarios y fortalecer la cooperación entre individuos, empresas y entidades gubernamentales. Al adoptar un enfoque integral para prevenir y contrarrestar amenazas cibernéticas, podemos garantizar la protección y la integridad de nuestros datos en el mundo digital de hoy.

Nuestra investigación colaborativa sobre ciberseguridad, hemos aprendido que la protección efectiva de la información digital requiere un esfuerzo conjunto y una comprensión profunda de los riesgos potenciales. La implementación de medidas de seguridad robustas, la capacitación continua de los usuarios y la coordinación entre diversas entidades son elementos clave para mitigar la creciente amenaza de ataques cibernéticos. Al fomentar una cultura de seguridad proactiva y la adopción de mejores prácticas, podemos salvaguardar la integridad de nuestros datos y garantizar un entorno digital más seguro para todos.



EMILIO DE JESUS IBARRA GUTIERREZ-2000396-IAS

La ciberseguridad es un tema crítico en la era digital actual, y diversos problemas, como el malware, el phishing, las fugas de datos y los ataques a infraestructuras críticas, representan amenazas significativas para individuos, empresas y gobiernos.

La concienciación y educación en ciberseguridad son fundamentales para protegerse contra estas amenazas y garantizar la seguridad de la información y los sistemas.

Además, la implementación de medidas proactivas, como la actualización de software y el uso de herramientas de seguridad robustas, son esenciales para mantener la integridad de los sistemas digitales.

En última instancia, la colaboración entre los sectores público y privado, junto con una vigilancia constante y una respuesta efectiva, son cruciales para hacer frente a los desafíos cada vez más complejos y sofisticados en el ámbito de la ciberseguridad.

JOSUÉ CARLOS MORENO MAGALLANES-1846526-ITS

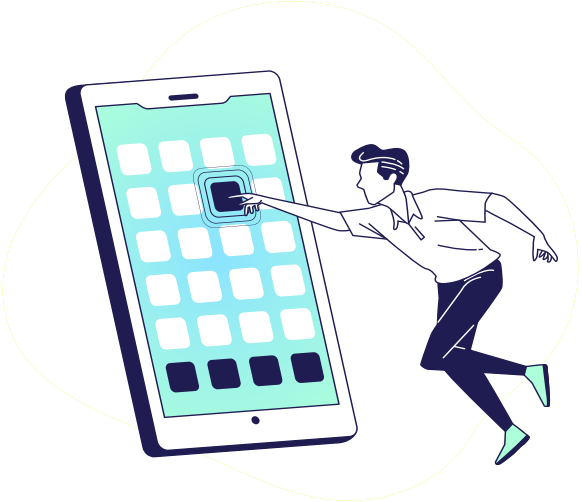
La verdad el simple hecho de hacer esta actividad me gusto mucho, pues la aborde llevando a la par un curso de ciberseguridad impartido por IBM el cual lo aprendido fue lo que plasme aquí, este tema me interesa mucho, pues es al área que me gustaría profundizar para mi trabajo a futuro, poder comprenderla mejor y aplicar explicando lo que he aprendido y descubrir nuevas cosas del tema me fue de mucha ayuda.

Este es un tema con un amplio desarrollo dia con dia y me parece muy importante que todo profesional del área digital y también los consumidores de las tecnologías comprendan este tema.

ELIUD JONATHAN LUCIO GARCÍA-2000116-ITS

La ciberseguridad se ha convertido en una parte importante de nuestras vidas en la era digital. La creciente dependencia de la tecnología y el aumento de amenazas cibernéticas hacen que la protección de activos digitales y sistemas de información sea una prioridad importante a tomar en cuenta.

En un mundo cada vez más interconectado y digitalizado, es crucial que se comprenda la importancia de la ciberseguridad y tomen medidas para proteger sus activos digitales. La educación, la inversión en tecnologías de seguridad y la adopción de mejores prácticas en ciberseguridad son pasos importantes para mantener nuestros sistemas seguros en un mundo en constante evolución tecnológica y cibernética.



GREGORIO MARTINEZ MARTINEZ 2014975 IAS

En cuanto a la actividad este tema tiene muchas area de aprendizajes, cada subtema y cada problema que puede suceder.

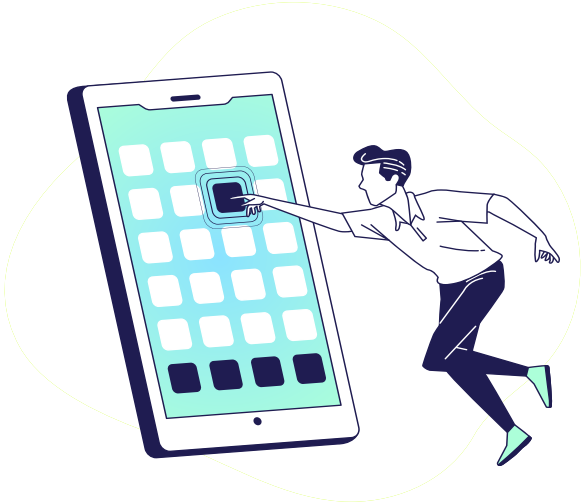
Los virus o archivos maliciosos están en cualquier lado, ya sea en las descargas o en un solo clic puede dar el acceso para que este problema entre a tu equipo y haga mal uso de tus datos.

Cada virus tiene una función, y cada uno tiene una forma de evadir los antivirus o las barreras que ayudan al equipo.

DAMARIS HERNANDEZ HERNANDEZ 2005278 - IAS

Como pudimos ver anteriormente, se necesita tener extremo cuidado con muchos dispositivos electrónicos, ya que pueden ser hackeados y nos pueden robar información importante, hay varias maneras de ser hackeado desde un virus hasta que te hacke una persona experta en el tema.

La ciberseguridad juega un papel muy importante en la actualidad, ya que desde abrir un link o descargar un archivo de dudosa procedencia puede incluso la pérdida total de la memorio o del disco duro, dependiendo sea el caso del dispositivo dañado, por eso siempre es muy importante contar con un antivirus, que solo nosotros sepamos nuestras contraseñas.



Víctor Alfonso Delgado Bautista - 2006517 - IAS

En la actualidad, la ciberseguridad se ha vuelto esencial en un mundo cada vez más interconectado y dependiente de las tecnologías de la información. La creciente amenaza de ciberataques y la proliferación de datos digitales hacen que la protección de la información sea de suma importancia. La ciberseguridad desempeña un papel crítico al salvaguardar la integridad, confidencialidad y disponibilidad de datos en redes y sistemas.

La importancia de la protección de datos radica en la confianza que los usuarios depositan en las tecnologías digitales. La pérdida de datos o las violaciones de seguridad pueden tener consecuencias significativas, desde daños a la reputación de las empresas hasta la exposición de información sensible que podría ser explotada con fines maliciosos. La protección de datos es esencial para garantizar la privacidad y la confianza en un entorno digital en constante evolución.

BIBLIOGRAFIA

IBM. (n.d.). ¿Qué es la ciberseguridad?. Bundles. Retrieved 22 October. 2023, from https://students.yourlearning.ibm.com/credential/CREDLY-b8810a57-2c5a-4bbc-81f1-9bfc649ad13d

IBM. (n.d.). Ciberseguridad: Sobre los delitos. Bundles. Retrieved 22 October. 2023, from https://students.yourlearning.ibm.com/credential/CREDLY-b8810a57-2c5a-4bbc-81f1-9bfc649ad13d

IBM. (n.d.). Ciberseguridad: Grupos de actores de amenaza. Retrieved 22 October. 2023, from https://students.yourlearning.ibm.com/credential/CREDLY-b8810a57-2c5a-4bbc-81f1-9bfc649ad13d

Protección de los sistemas informáticos contra los ataques y desastre. (s. f.). COSMO

CONSULT.https://mx.cosmoconsult.com/blog/proteccion-sistemas-informaticos-contra-ataques-desastres/

Info@citel. (s. f.). https://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp

BIBLIOGRAFIA

Latam, A. (2023, 21 abril). *Tipos de autenticación: contraseña, token, JWT, dos factores y más*. Alura. https://www.aluracursos.com/blog/tipos-de-autenticacion

González, E. (2022, 5 abril). *Los 5 principales desafíos de seguridad que deben afrontar los centros de datos*. Bit Life Media. https://bitlifemedia.com/2022/04/centros-de-datos-desafios-seguridad/

Dg. (2022, 1 febrero). *Los 10 principales desafíos y soluciones de la gestión de la información*. DG | Tecnologia Acessível. https://dgcloud.com.br/es/los-10-principales-desafios-y-soluciones-de-la-gestion-de-la-informacion/#:~:text=Los%20desaf%C3%ADos%20t%C3%ADpicos%20de%20la,sistemas%20m%C3%A1s%20antiguos%20y%20la