Seguridad

UANL
UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN

FIME
FACULTAD DE INGENIERÍA MECÁNICA Y ELÉCTRICA

Sistemas operativos

Salón: 2302 Grupo: 001

Dra. Norma Edith Marín Martínez

Alumno: Hector Emmanuel Jaramillo Granados

Matricula: 1986819 Carrera IAS

Actividad fundamental 4

Como introducción.
Por seguridad, nosotros entendemos…

- Confianza de que todo estará bien
- Sentirnos protegidos
- Y si nada de lo anterior sucede, mínimamente podemos defendernos

Trasladando el significado a sistemas operativos

- En un sistema operativo la seguridad es prioridad por:
  - Archivos personales: Copias de documentos tales como actas de nacimiento, identificaciones.
  - Datos bancarios: Estados de cuenta, transferencias, depósitos de efectivo.
  - Archivos empresariales: Información de clientes y/o proveedores, inventarios.
  - Etcétera…
- Por tanto, seguridad es privacidad e integridad

¿Qué amenaza nuestra seguridad?

- No todo es seguro, por muy trabajado que se encuentre un sistema operativo siempre habrá algún problema que pueda vulnerar la seguridad de nosotros los usuarios, seamos personas que la utilizan para mero entretenimiento o gente que utiliza su dispositivo para la escuela o trabajo, a todos nos afecta.
- Estas vulnerabilidades podrían pasar desapercibidas si la gente se enfocara solamente en usar el sistema para lo que esta diseñado, pero hay otro tipo de usuario que se dedica a buscar esos errores para aprovecharlos de alguna forma.

Virus o malware

- Son programas maliciosos, hay de diferentes tipos y su ejecución puede ser desde un programa ejecutable hasta en documentos o scripts de sitios web.
- Nos perjudican gravemente porque provocan que nuestros equipos funcionen lentos o hasta la perdida y robo de información.
- Que nuestra seguridad sea vulnerada por este tipo de software es de lo peor que nos puede pasar.

Gusanos

- Tienen el objetivo de propagarse a través de redes por si mismos, no necesitan interacción del usuario.
- Por esa razón son muy peligrosos y de propagación rápida.
- Provocan que se sobrecarguen los sistemas.
- El más famoso:
  - *MyDoom* (Mi perdición) causo daños por más de $38 MMDD en 2004 que se envió masivamente por correo electrónico, tanto así que en su fecho llego a ser responsable de 25% del total de correos electrónicos enviados.
  - Su método de propagación era tomar correos electrónicos de equipos infectados y reenviarse, así hasta conseguir los suficientes para realizar ataques de denegación de servicio (DDoS, distributed denial-of-service) con el objetivo de apagar servidores o sitios web.

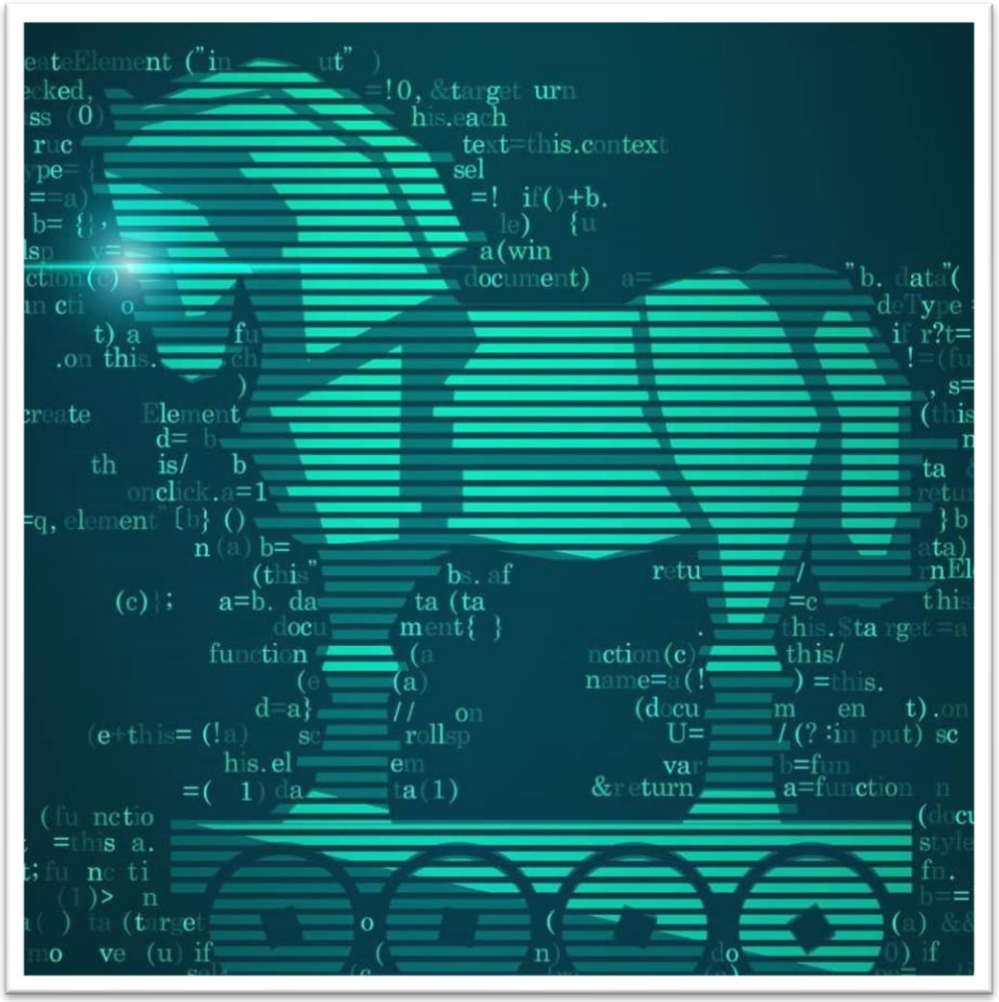
Adware

- Este tipo de malware es particularmente molesto porque añade publicidad no deseada en el sistema, los más comunes son los que se colocan en las pestañas de los navegadores, instalando barras de búsqueda con el objetivo de redireccionar a los usuarios a un motor de búsqueda donde muestre publicidad. No solo con navegadores, también se añade a aplicaciones de la computadora para seguir mostrando ese contenido indeseado.

Spyware

- Este tipo de software también se instala sin conocimiento alguno del usuario, como lo dice el nombre 'Spy' se refiere a espía, su función es recopilar todo tipo de información del usuario, desde actividades que realiza hasta monitorear sus micrófonos y cámaras.
- Es muy peligroso porque esta información es enviada a un usuario malicioso sin conocimiento del afectado lo que se traduce como posible uso malicioso de la misma, en casos más extremos puede llegar hasta chantajes con el objetivo de obtener dinero o cosas a cambio.

Troyanos



- Tienen este nombre porque referencian a al 'Caballo de Troya', que fue un artefacto enorme con forma de caballo que fue obsequiado a los troyanos aparentando ser un obsequio normal, pero en el interior se escondían soldados para conquistar la ciudad.
- Este tipo de malware se basa en el concepto anterior, se disfraza de software legitimo, como instaladores de programas de uso común, cuando se instalan puede realizar acciones maliciosas sin que el usuario lo sepa, desde el robo de información hasta permitir el acceso a atacantes remotos.
- GameOver Zeus fue uno muy famoso, se propagaba a través de inyección de código en el navegador y procesos del sistemas, con el objetivo de capturar usuarios y contraseñas para después enviarlos a su servidor.

Ransomware

- Este probablemente es el malware mas problemáticos de los mencionados.
- Se encarga de cifrar los archivos del usuario y exige un rescate (dinero) para devolverlos, un secuestro de información.
- Si no pagas se pierde todo, en una empresa puede ser fatal.
- Se propagan por correo electrónico incitando a que descargues y abras archivos, software maliciosos y sitios web infectados. Además de propagarse en redes enteres como las de escuelas y empresas.
- El más famoso de los últimos años fue CryptoLocker:
  - Diseñado para afectar solamente a Windows (El más usado)
  - Te infecta con un ZIP con contraseña, poner la contraseña y ejecutar el PDF estas infectado.

Los intrusos

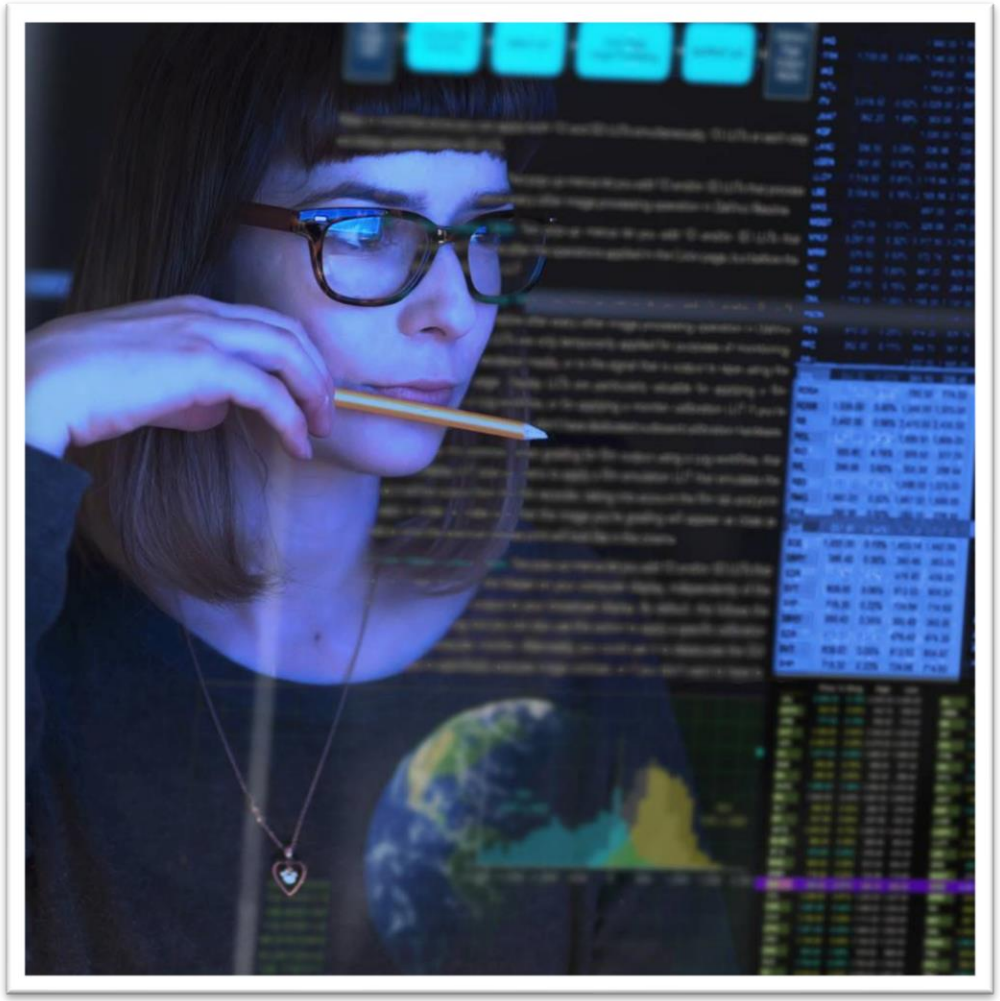
- Gracias al malware, para nuestra desgracia, quedamos expuestos a tener gente indeseada en nuestros equipos y redes.
- Estos intrusos normalmente se dividen en tres categorías.
  - Usuario fraudulento
  - Suplantador de identidad
  - Usuario clandestino
- Se mencionaran otros tipos de intrusos.

Usuario enmascarado

- Son usuarios que acceden de manera ilegal a recursos de un sistema u organización, registrándose con información falsa para acceder a un sistema con el objetivo de conseguir información que normalmente no tendría.
- Protegerse de este tipo de intruso es importante, cuando alguien esta usando tu sistema es porque deberías de saber que es una persona confiable.

Usuario Infractor

- Usuarios que tienen permiso para acceder al sistema pero que hace mal uso de este mismo.
- Abusan de su poder para acceder a información a la que normalmente no debería de ver.



Usuario clandestino

- Igual tiene acceso al sistema, pero tiene la particularidad de tener acceso administrativo, pudiendo utilizar la información de manera inapropiada para obtener ganancias.

Hackers

- Es otro tipo de intruso que son expertos en informática; dominan varios lenguajes de programación, arquitectura de computadoras, servicios y protocolos de comunicación, sistemas operativos, etc.
- Se dividen en tres categorías:
  - Éticos / Sombrero blanco
  - Malintencionados / Sombrero negro
  - Sombrero gris
  - Hacktivistas

Éticos / Sombrero blanco

- Usan sus conocimientos para detectar problemas de seguridad y ayudar a organizaciones a protegerse de los hackers de sombrero negro.
- Tienen la intención de ayudar, no perjudicar
- Buscan puntos débiles y hacen recomendaciones para hacer correcciones.
- Ejemplo:
  - Tim Berners-Lee, inventor de la *world wide web* se considera dentro de este grupo.

Malintencionados / Sombrero negro

- Son los hackers que tienen malas intenciones.
- Tienen la intención de acceder a sistemas de forma ilegal para causar daño.
- Pueden destruir información, robarla y hacer otro tipos de delitos cibernéticos.
- Ejemplo:
  - Kevin Mitnick: Famoso hacker estadounidense, el FBI llego a ofrecer millones por su captura.
  - Hackeo empresas de tecnología como Motorola, San Diego Supercomputer Center, IBM, etc.

Sombrero gris

- Hackers que no son blancos o negros.
- Cuando encuentran un punto débil no la explotan con fines maliciosos, pero tampoco le dirá a otros como explotarlos.
- Sus acciones dependen de como vean la situación.
- Ejemplo:
  - En 2013, Khali Shreateh encontró una vulnerabilidad en Facebook que permitía a cualquier usuario publicar en el muro de cualquier perfil de la red social como si esa persona lo hubiese escrito. Esto en manos de un spammer hubiese resultado fatal…
  - Reporto el problema a la red social pero no le prestaron la debida atención, entonces fue que decidido pasar de un tono de hacker blanco a negro.
  - Uso la vulnerabilidad para informar que existía el problema y lo publico en el perfil del creador de Facebook, Mark Zuckerberg. Evidentemente fue escuchado cuando eso paso.

Hacktivistas

- Son activistas y hackers a la vez.
- Atacan a organizaciones que ellos consideran que hacen cosas injustas, desde dependencias gubernamentales hasta empresas multinacionales.
- Básicamente actúan para promover agendas políticas.
- Ejemplo:
  - El grupo Guacamaya: Operan en Hispanoamérica. Son hackers antiimperialistas y ecologistas, actúan en defensa de los recursos, sus objetivos son empresas extractivas y fuerzas represivas.
  - Fueron responsables del hackeo a la SEDENA (México) donde se comprometieron 6TB de información clasificada.

Autentificaciones

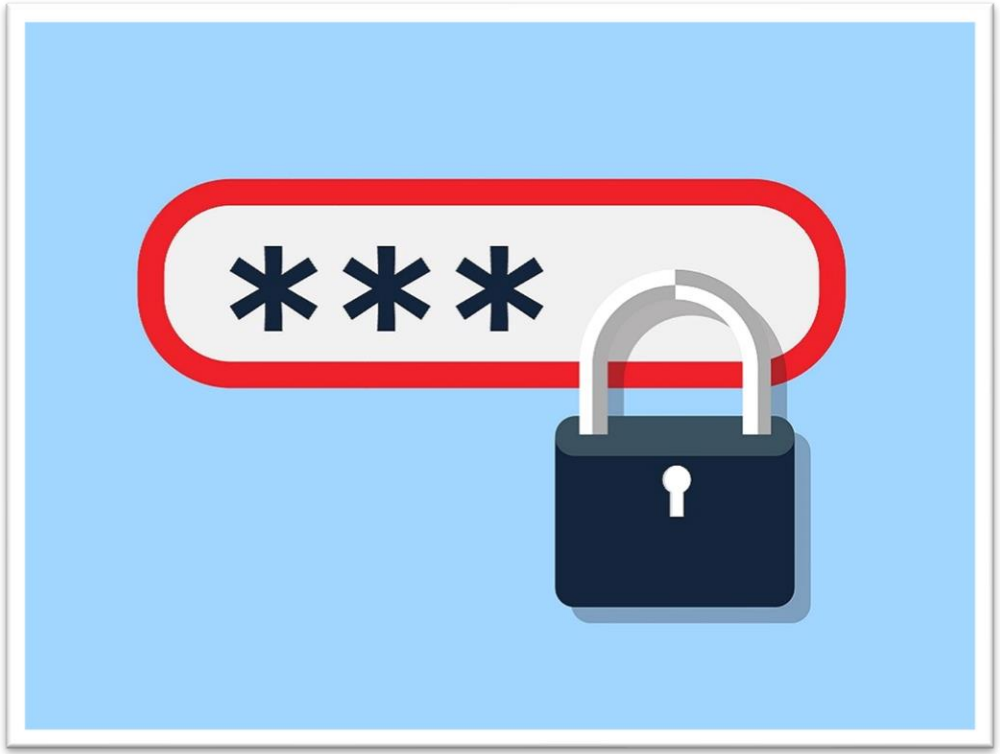
- Son el proceso de validar a la identidad de los usuarios antes de permitir el acceso a una función del sistema.
- Esta se realiza a través de, normalmente, usuario y contraseña o medios de autentificación biométrica como la huella digital.
- Es algo de lo que no se puede prescindir.

Tipos de autentificaciones

- Contraseña.
- Tarjeta inteligente.
- Huella digital.
- Certificado digital.

Contraseña

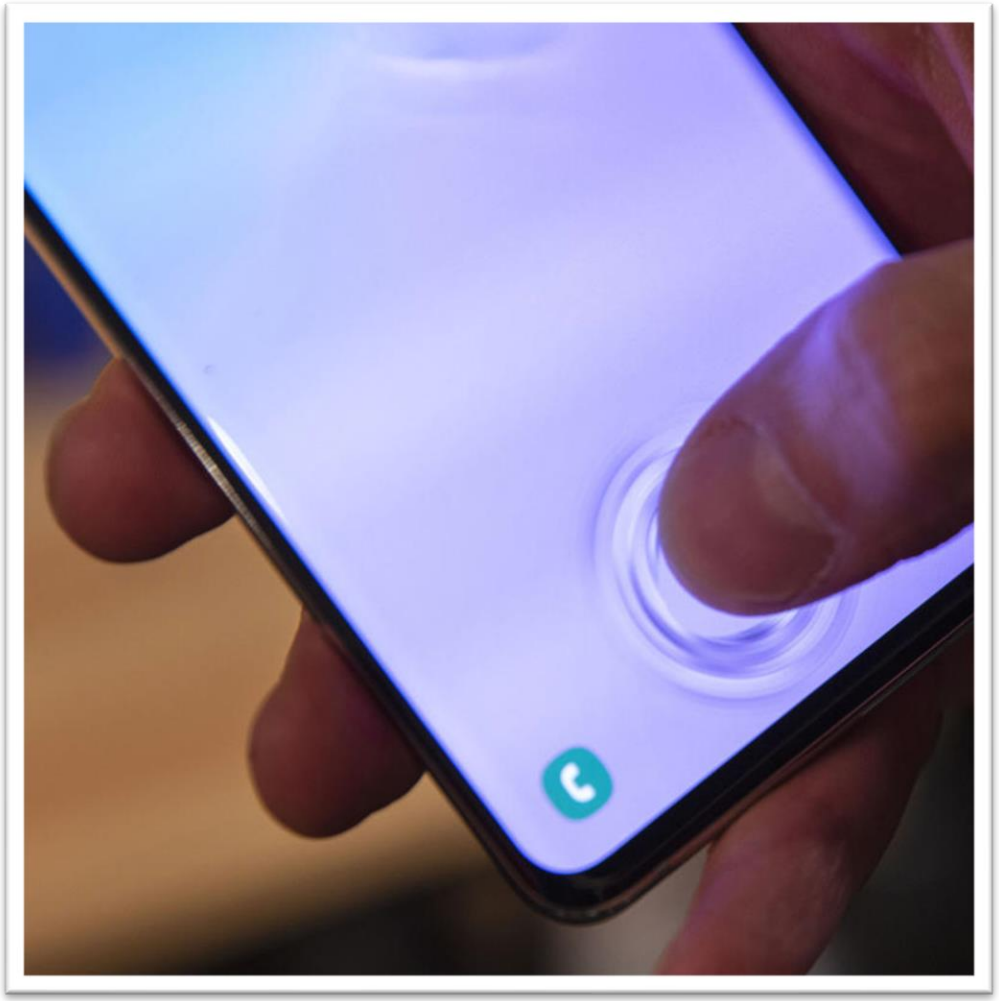
- Es el método más común de autentificación, en donde un usuario tiene que comprobar su identidad ingresando una contraseña para acceder al sistema.
- Estas contraseñas se almacenan en una base de datos segura, aquí se comparan las credenciales ingresadas por el usuario y la base de datos.
- Si coinciden se deja acceder.



Tarjenta inteligente

- Usan la tecnología NFC (near field communication)
- Esta tecnología permite el uso de pequeños chips que guardan información.
- Cuando un lector lee la tarjeta puede verificar la identidad del usuario.

Huella digital



- Parecido al anterior por el tema del lector.
- Para el registro se requiere presencia física del usuario a dar de alta para registrar la huella.
- Cuando el lector detecta la huella busca coincidencias para algún usuario.
- Si hay coincidencia se ingresa.
- El uso más común de este tipo de autentificación es dado en los smartphones, donde se usa como principal método de autentificación.

Certificado digital

- Es un archivo emitido por alguna organización.
- Contiene la información de autentificación única para un usuario.
- Un ejemplo de esto es la e.firma del SAT.
- Tramitar estos certificados igual se requiere de presencia del usuario.

Niveles de seguridad que se pueden implementar

- Usuario
- Red
- Organización

Usuarios

- Este nivel de seguridad esta enfocado en los usuarios, sus credenciales de acceso y su protección.
- Esta centrado en garantizar que los usuarios sean legítimos (usuarios y contraseñas validos)
- Para esto, también:
  - Requieren contraseñas seguras, es decir; largas, complejas (números, mayúsculas, caracteres). Cambiarlas cada cierto tiempo es importante.
  - Autentificación multifactorial: Se refiere a que, para acceder se requiere que el usuario proporcione más de un método de autentificación.
  - Complementando lo mencionado anteriormente, se aplican políticas de contraseñas para aumentar la seguridad de contraseñas.
  - Los permisos de acceso también se deben de tratar con cuidado, solo darse a usuarios que deberían de tenerlos y revocarse cuando ya no sea conveniente.

Red

- Enfocado en la protección de la red de una organización, es decir, su infraestructura de red, comunicación y dispositivos de red.
- Ayudan a garantizar a que las organizaciones resistan ataques.
- Usan medidas como:
  - Implementación de firewall
  - Prevención de intrusos
  - Seguridad de Wi-Fi y VPN

Organizaciones

- Este nivel esta orientado a la protección de los procesos, políticas y procedimientos.
- Las medidas a implementar se centran en garantizar que hayan políticas y procesos para proteger recursos y la capacitación de los empleados para cumplir con las políticas.
- Medidas que se toman:
  - Políticas de seguridad: Requisitos para la protección de activos y recursos.
  - Gestión de incidentes: Procedimientos para responder a eventos de seguridad, como un ataque.
  - Capacitación de seguridad: Como mencionamos anteriormente, se deben de capacitar a los empleados para que comprendan a que se enfrentan y como actuar.

Análisis de posibles problemas

- Es la identificación de posibles amenazas que pueden afectar la seguridad de los recursos de información de una organización.
- Como por ejemplo ataques de hackers, virus, fallas de hardware.
- Para hacer el análisis, se puede hacer una evaluación de riesgos o una auditoria de seguridad.

Prevención de desastres

- De por si la palabra provoca algo de inseguridad, el que llega a ocurrir uno en cualquier organización es algo terrible.
- Por eso se deben implementar medidas de prevención para minimizar el impactos de los desastres.
- Medidas comunes son:
  - Copias de seguridad de la información: Se hacen cada cierto tiempo.
  - Utilizar sistemas de alimentación ininterrumpida para evitar interrupciones de energía, se pueden usar plantas de emergencias si es requerido. Con el fin de mantener el hardware en buen estado

Administración de riesgos

- Es la identificación, evaluación y corrección de los riegos que puedan afectar la seguridad de recursos de una organización.
- Se logra a través de políticas y procedimientos claros para identificación y evaluación.
- Se deben implementar medidas de corrección adecuadas para los riegos identificados.

Seguridad en…

- Hardware
- Software
- Archivos e información

Hardware

- Se refiere a la seguridad de los dispositivos que se usan para el control de tráfico de una red. Como los firewalls de hardware.
- También a las aplicaciones que se usan para proteger computadoras y dispositivos de cualquier tipo de daño.
- Esta seguridad se considera que es la que mas proporciona niveles de seguridad.
- Funciona como capa adicional para sistemas de seguridad de alta importancia.

Software

Esta seguridad se usa para la protección de programas y aplicaciones contra ataques de hackers.

Es necesaria para garantizar la integridad de datos, autenticidad de los mismos y que se encuentren constantemente disponibles.

Se busca que desde el inicio de desarrollo de alguna aplicación se implementen medidas de protección.

Archivos e información

- Es importante que los archivos de una organización estén protegidos contra el acceso no autorizado.
- Así mismo, para asegurarnos de ello, se implementan herramientas como el control de acceso, que dicta que usuarios pueden acceder a archivos.
- También políticas de retención de datos que garanticen que cuando se vayan a eliminar archivos, se haga de forma segura.

Soluciones para el hardware

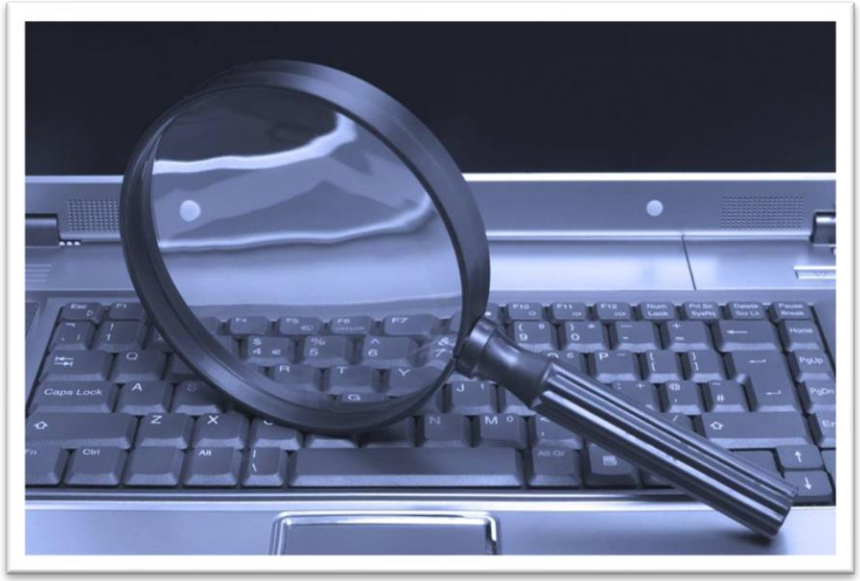
- Con respecto al hardware, hay que mantenerlo seguro, como mencionábamos, puede ser una capa muy fuerte de seguridad.
- Esto no lo exenta de que físicamente puedan intentar acceder a el con fines maliciosos.
- Es por esto que, si queremos que el hardware este lo más seguro posible, se debe limitar el acceso a las habitaciones donde se encuentra a solo personal autorizado.
- Protegerlo de picos eléctricos que puedan destruir el aparato en cuestión, por eso recalco nuevamente el uso de UPS para mantener a salvo y con voltaje correcto al hardware.
- Así como monitorizar el equipo para supervisar el rendimiento.

Soluciones para el software

- Es crucial tener protección contra ataques de hackers
- Mediante actualizaciones de seguridad para los componentes de un sistema nos aseguramos que vulnerabilidades que se puedan presentar no tengan mucha presencia en nuestra organización, de preferencia que sean automáticas para que cuando salgan se instalen de inmediato.
- El uso de antivirus es vital, no podemos prescindir de el, el escaneo en tiempo real es prácticamente obligatorio y nos mantiene seguros de cualquier amenaza que se llegue a presentar.
- La capacitación del empleado es también de lo más importante, podemos tener la mejor preparación previa pero si un empleado descarga software que le pide desactivar antivirus…

Soluciones para archivos e información

- Aquí también es necesaria la capacitación del empleado.
- Estar protegido contra acceso no autorizado, incluyendo el cifrado de información.
- Realización de auditorias para verificar que los archivos no se hayan alterado de forma maliciosa



Conclusiones

- A lo largo de la presentación y en la investigación de la misma se pudo observar que la seguridad es prioridad primero, el que no se tengan herramientas ni la capacitación para enfrentarse a los problemas que se puedan presentar puede acabar en un desastre que haga a una organización perder mucho dinero.
- Si se va a hacer algo, se debe de planear para que cumpla con medidas de seguridad desde etapas tempranas de desarrollo, así puedes reducir el riesgo de que en etapas futuras tengas algún problema.
- No debemos de prescindir de la seguridad, para nada, ¡prohibido!

Referencias

- Stallings, W. (2005). *Sistemas operativos: aspectos internos y principios de diseño*. PRENTICE HALL.
- V. (2022, October 27). *Configuración de directivas de auditoría de seguridad avanzada (Windows 10) - Windows security*. Microsoft Learn. https://learn.microsoft.com/es-es/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
- *Hackers de sombrero negro, blanco y gris: definición y explicación*. (2023, January 16). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/definitions/hacker-hat-types
- *Desastres informáticos: previsión y prevención*. (2013, January 23). IDG Communications S.A.U. https://www.computerworld.es/archive/desastres-informaticos-prevision-y-prevencion
- *Cómo funciona la seguridad con huellas dactilares - Ayuda de Chromebook*. (n.d.). https://support.google.com/chromebook/answer/10368863?hl=es-419
- *Guacamaya - Enlace Hacktivista*. (n.d.). https://enlacehacktivista.org/index.php?title=Guacamaya

- M. (2023c, March 4). *Protección de los niveles de seguridad de acceso con privilegios*. Microsoft Learn. https://learn.microsoft.com/es-es/security/privileged-access-workstations/privileged-access-security-levels
- Europa Press. (n.d.). *Un "hacker" demuestra una vulnerabilidad en Facebook a través del muro de Zuckerberg*. europapress.es. https://www.europapress.es/portaltic/socialmedia/noticia-hacker-demuestra-vulnerabilidad-facebook-traves-muro-zuckerberg-20130819104612.html
- Mitnick Security Consulting. (n.d.). *About Kevin Mitnick | Mitnick Security*. https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security
- *CryptoLocker: What is it? - Panda Security*. (n.d.). https://www.pandasecurity.com/en/security-info/cryptolocker/
- Cveticanin, N., & Cveticanin, N. (2023, January 20). *What Is the Most Dangerous Computer Virus in History?* Dataprot. https://dataprot.net/articles/most-dangerous-computer-virus/