# INSTITUTO POLITÉCNICO NACIONAL


ESCUELA SUPERIOR DE CÓMPUTO

INGENIERIA EN SISTEMAS COMPUTACIONALES

MATERIA: SISTEMAS OPERATIVOS

PROFESOR: ARAUJO DIAZ DAVID

PRESENTA:

RAMIREZ BENITEZ BRAYAN

NÚMERO DE LISTA:

27

GRUPO: 2CV17

## TAREA 6:

## SEGURIDAD

CIUDAD DE MEXICO JUNIO DE 2021

**1. ¿Cuáles son las dos facetas que tiene la seguridad?**

**R:** Dos de las facetas más importantes son la perdida de datos y los intrusos.

**2. Mencione tres causas comunes de perdida de datos.**

**R:**

• Actos divinos: Incendios, inundaciones, terremotos, guerras, revoluciones o ratas que roen las cintas o discos flexibles.

• errores de Hardware o Software: Mal funcionamiento de la CPU, discos o cintas ilegibles, errores de telecomunicación o errores en el programa.

• Errores Humanos: Entrada incorrecta de datos, mal montaje de las cintas o el disco, ejecución incorrecta del programa, perdida de cintas o discos.

**3. ¿Cuáles son las dos clases de intrusos (descríbalos brevemente)?**

**R:**

- Los intrusos pasivos solo desean leer archivos que no están autorizados a leer.
- Los intrusos activos desean hacer cambios no autorizados a los datos. Si se desea diseñar un sistema seguro contra los intrusos, es importante tener en cuenta el tipo de intruso con el que se desea tener protección.

**4. ¿Cuáles son algunas categorías comunes de intrusos activos?**

**R:**

• Curiosidad casual de usuarios no técnicos. Muchas personas tienen en sus escritorios terminales para sistemas con tiempo compartido y, por la naturaleza humana, algunos de ellos leerán el correo electrónico de los demás u otros archivos, si no existen barreras en frente de ellos.

• Conocidos husmeando. Algunos estudiantes, programadores de sistemas, operadores y demás personal técnico consideran como un reto personal romper la seguridad del sistema de cómputo local. A menudo son muy calificados y están dispuestos a invertir una cantidad sustancial de su tiempo en este esfuerzo.

• Un intento deliberado de hacer dinero. Algunos programadores en banco han intentado penetrar un sistema bancario con el fin de robarle al banco. Los esquemas han variado desde cambiar el software para truncar y no redondear el interés, para quedarse con una pequeña fracción de dinero, hasta sacar dinero de las cuentas que no se han utilizado en anos o el "correo negro”.

• Espionaje comercias o militar. El espionaje indica un intento serio y fundamentado por parte de un competidor u otro país para robar programas, secretos comerciales,

patentes, tecnología, diseño de circuitos, planes de comercialización, etc. A menudo, este intento implica la cobertura de cables o el levantamiento de antenas hacia la computadora con el fin de recoger su radiación electromagnética.

**5. Describa tres fallas de seguridad famosas en los sistemas operativos.**

**R:**

- Navegación insegura por internet: Las vulnerabilidades de los navegadores web pueden comprometer la seguridad de un sistema, la información y hacer más fácil el camino de un hacker para un ataque.
- Uso de software pirata: Los softwares piratas pueden ser utilizados para sembrar troyanos y virus en las computadoras y dado que el software carece de respaldo puesto que es pirata, el usuario es privado de soporte técnico quedando a expensas del ataque sin ayuda.
- Mal uso de dispositivos de almacenamiento portátil: Dado a la gran practicidad de estos dispositivos, mejoras en los procedimientos para traspaso de información en el ambiente laboral y las capacidades de almacenamiento, los dispositivos de almacenamiento portátil han sido utilizados para descargar información sensible y privilegiada de clientes de las organizaciones pudiendo hacer mal uso de ella. El uso de estos dispositivos debe ser controlado, para usuarios selectos y con dispositivos predeterminados.

**6. ¿Qué es un caballo de Troya y una bomba lógica?**

**R:** Básicamente, un troyano en un programa malicioso que aparenta ser inofensivo para persuadir a la gente para que lo descargue. A los troyanos les corresponde el honor de ser una de las primeras formas de malware. Su nombre fue acuñado en un informe de las Fuerzas Aéreas de los EE. UU. De 1974, que enumeraba todas las formas hipotéticas en que un sistema informático podría ser vulnerado.

Del término en inglés LogicBomb. Una bomba lógica es un programa informático que se instala en una computadora y permanece oculto hasta cumplirse una o más condiciones preprogramadas para entonces ejecutar una acción. A diferencia de un virus, una bomba lógica jamás se reproduce por sí sola.

**7. Mencione cuatro aspectos sobre la seguridad que todo diseñador de sistemas debe de tomar en cuenta.**

**R:**

1. Físico. El nodo o nodos que contengan los sistemas informáticos deben dotarse de medidas de seguridad físicas frente a posibles intrusiones armadas o subrepticias por parte de potenciales intrusos. Hay que dotar de seguridad tanto a las habitaciones donde las maquinas residan como a los terminales o estaciones de trabajo que tengan acceso a dichas maquinas.

2. Humano. La autorización de los usuarios debe llevarse a cabo con cuidado, para garantizar que solo los usuarios apropiados tengan acceso al sistema. Sin embargo, incluso los usuarios autorizados pueden verse “motivados” para permitir que otros usen su acceso. También pueden ser engañados para permitir el acceso de otros, mediante técnicas de ingeniería social. Uno de los tipos de ataque basado en las técnicas de ingeniería social es el denominado phishing; con este tipo de ataque, un correo electrónico o página web de aspecto autentico llevan a engaño a un usuario para que introduzca información confidencial. Otra técnica comúnmente utilizada es el análisis de desperdicios, un término autorizado a la computadora. Estos problemas de seguridad son cuestiones relacionadas con la gestión y con el personal, más que problemas relativos a los sistemas operativos.
3. Sistema operativo. El sistema debe autoprotegerse frente a los diversos fallos de seguridad accidentales o premeditados. Un problema que este fuera de control puede llegar a constituir un ataque accidental de denegación de servicio. Asimismo, una cierta consulta a un servicio podría conducir a la revelación de contraseñas o un desbordamiento de la pila podría permitir que se iniciara un proceso no autorizado. La lista de posibles fallos es casi infinita.
4. Red. Son muchos los datos en los modernos sistemas informáticos que viajen a través de líneas arrendadas privadas, de líneas compartidas como Internet, de conexiones inalámbricas o de líneas de acceso telefónico. La interceptación de estos datos podría ser tan dañina como el acceso a un computador, y la interrupción en la comunicación podría constituir un ataque remoto de denegación de servicio, disminuyendo la capacidad de uso del sistema y la confianza en el mismo por parte de los usuarios.

**8. ¿Qué es un virus?**

**R:** Un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos.

**9. ¿Cómo funciona un programa virus?**

**R:** Una vez que un virus se adjunta a un programa, archivo o documento, el virus permanecerá inactivo hasta que alguna circunstancia provoque que el equipo o dispositivo ejecute su código. Para que un virus infecte un equipo, se debe ejecutar el programa infectado, lo cual provocará que el código del virus se ejecute. Es decir que el virus podría permanecer inactivo en el equipo, sin mostrar grandes indicios o síntomas. Sin embargo, una vez que el virus infecta el equipo, puede infectar a otros de la misma red. Los virus pueden realizar acciones devastadoras y molestas, por ejemplo, robar contraseñas o datos, registrar pulsaciones de teclado, dañar

archivos, enviar spam a sus contactos de correo electrónico e, incluso, tomar el control de su equipo.

**10. Describa los seis principios generales que pueden servir como guía para diseñar sistemas seguros.**

**R:**

1. Partir siempre de un modelo de permisos mínimos, es mejor ir escalando privilegios por demanda de acuerdo a los perfiles establecidos en las etapas de diseño.
2. Si se utiliza un lenguaje que no sea compilado, asegurarse de limpiar el código que se pone en producción, para que no contenga rutinas de pruebas, comentarios o cualquier tipo de mecanismo que pueda dar lugar a un acceso indebido.
3. Nunca confiar en los datos que ingresan a la aplicación, todo debe ser verificado para garantizar que lo que está ingresando a los sistemas es lo esperado y además evitar inyecciones de código.
4. Hacer un seguimiento de las tecnologías utilizadas para el desarrollo. Estas van evolucionando y cualquier mejora que se haga puede dejar obsoleta o inseguras versiones anteriores.
5. Todos los accesos que se hagan a los sistemas deben ser validados.
6. Para intercambiar información sensible utilizar protocolos para cifrar las comunicaciones, y en el caso de almacenamiento la información confidencial debería estar cifrada utilizando algoritmos fuertes y claves robustas.

**11. ¿Qué es la verificación de autenticidad de usuarios?**

**R:** La autenticación consiste en la verificación de las credenciales con las que se identificó el usuario, es decir, se demuestra que realmente es quién dice ser. Estas credenciales son conocidas como factores de autenticación. La autorización son las acciones que se permiten realizar al usuario con dichas credenciales.

**12. ¿Cómo funciona y que problemas existen al emplear una contraseña como medida de seguridad?**

**R:** La seguridad de la contraseña es una medida de la efectividad de una contraseña contra ataques de adivinación o de fuerza bruta. En su forma habitual, estima cuántas pruebas necesitaría un atacante que no tiene acceso directo a la contraseña, en promedio, para adivinarla correctamente. La seguridad de una contraseña depende de la longitud, la complejidad y la imprevisibilidad.

**13. En que consiste la identificación física para seguridad.**

**R:** Autenticación física La autenticación física se basa en algún objeto físico que posee el usuario, o en alguna característica física del usuario; en tal caso utiliza algún tipo de mecanismo biométrico.

**14. Mencione algunas medidas preventivas para seguridad.**

**R:**

1.- Sentido común: La prudencia es la mejor barrera contra el malware. Cuidar especialmente el apartado de descargas e instalación de aplicaciones de sitios no seguros; la navegación por determinadas páginas de Internet; la apertura de correos electrónicos o archivos adjuntos no solicitados o que llegan de remitentes desconocidos o los que llegan de redes sociales o aplicaciones de mensajería que contienen vulnerabilidades explotables por los ciberdelincuentes para las campañas de malware.

2.- Actualizar el sistema operativo y aplicaciones: Todos los sistemas operativos cuentan con herramientas para mantener actualizados sus equipos. Y son de uso obligado porque incluyen actualizaciones de seguridad contra amenazas conocidas. Igual importante que lo anterior es la actualización de aplicaciones instaladas a las últimas versiones ya que éstas suelen incluir parches de seguridad. Cuando las versiones son más antiguas, tienen mayor riesgo de ser atacadas por ciberdelincuentes que encuentran vulnerabilidades en el programa, con especial incidencia en algunas como Java, Adobe Flash o Reader.

3.- Proteger los navegadores: Todos los navegadores web incluyen características avanzadas de seguridad cuya activación debemos revisar y configurar porque son las aplicaciones con las que accedemos a Internet y sus servicios. Además del cifrado de extremo a extremo en la sincronización o el aislamiento de procesos (sandbox), debemos prestar atención a los avisos sobre sitios inseguros que muestran los navegadores. También revisar las extensiones instaladas porque algunas son fuente frecuente de introducción de malware. Otra posibilidad interesante para mejorar la privacidad es utilizar una sesión en “Modo Invitado” el cual está totalmente desligado del perfil original del usuario, incluyendo configuración o historial.

4.- Cuidar las contraseñas: Además del uso de técnicas avanzadas de identificación biométrica en equipos que las incluyan, la regla de oro para estar seguro en línea es contar con una contraseña aleatoria fuerte y distinta para cada sitio web, especialmente para uso en los destinados a banca en línea y comercio electrónico.

5.- Realizar copias de seguridad: La seguridad al 100% en un mundo conectado simplemente no existe y no sólo por un virus ya que un error en el hardware puede

provocar la pérdida de preciada información personal y/o profesional. La realización de copias de seguridad es por tanto altamente recomendable para un usuario o profesional que pretenda proteger la información personal y corporativa de un equipo informático. además de ser una tarea de mantenimiento que contribuye a la salud del hardware. Las copias de seguridad deben almacenarse en un dispositivo de almacenamiento externo al de nuestro equipo o en un servicio de almacenamiento en nube.

6.- Activar la restauración del sistema: La restauración de los sistemas operativos es una herramienta que puede “salvarnos la vida” ante un error del software, instalación de drivers o de alguna aplicación que no funciona correctamente y también ante la entrada de un virus en nuestro equipo. Las herramientas de recuperación del sistema permiten revertir los cambios realizados en los archivos del sistema operativo, configuración, ajustes, controladores, claves del registro o programas instalados, y que en ocasiones desestabiliza el sistema operativo.

**15. Describa en qué consisten los dominios de protección para seguridad.**

**R:** Un dominio de protección es un conjunto de pares (objeto, operaciones); cada par identifica un objeto y las operaciones permitidas sobre él. En cada instante, cada proceso ejecuta dentro de un dominio de protección. Los procesos pueden cambiar de un dominio a otro en el tiempo; el cómo depende mucho del sistema. En UNIX, se asocia un dominio a cada usuario+grupo; dado un usuario y el grupo al cual pertenece, se puede construir una lista de todos los objetos que puede acceder y con qué operaciones. Cuando un usuario ejecuta un programa almacenado en un archivo de propiedad de otro usuario B, el proceso puede ejecutar dentro del dominio de protección de A o B, dependiendo del bit de dominio o SETUSERID bit del archivo. Este mecanismo se usa con algunos utilitarios.

**16. ¿Qué son las listas de control de acceso?**

**R:** Es una serie de instrucciones que controlan que en un router se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

Las ACL configuradas realizan las siguientes tareas:

- Limitan el tráfico de la red para aumentar su rendimiento. En una entidad, por ejemplo, si su política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que lo bloqueen, lo que reduce considerablemente la carga de la red y aumenta su rendimiento.

- Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro lo haga a esa misma área.
- Filtran el tráfico según su tipo. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de redes sociales.
- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos.

Los routers no tienen configuradas de manera predeterminada las ACL, por lo que no filtran el tráfico por sí solos si antes no fueron programados. El tráfico que ingresa al router se encamina solamente en función de la información de la tabla de ruteo; sin embargo, cuando se aplica una ACL a una interfaz de red, se realiza la tarea adicional de evaluar todos los paquetes de la red a medida que pasan a través de la misma, para determinar si se pueden reenviar.

**17. ¿Qué es una lista de capacidades?**

R: En este caso, a cada proceso se le asocia una lista de capacidades. Cada capacidad corresponde a un objeto más las operaciones permitidas.

Cuando se usan capacidades, lo usual es que, para efectuar una operación M sobre un objeto *O*, el proceso ejecute la operación especificando un puntero a la capacidad correspondiente al objeto, en vez de un puntero al objeto. La sola posesión de la capacidad por parte del proceso quiere decir que tiene los derechos que en ella se indican. Por lo tanto, obviamente, se debe evitar que los procesos puedan "falsificar" capacidades.

Un problema de las capacidades es que puede ser difícil revocar derechos ya entregados. En Amoeba, cada objeto tiene asociado un número al azar, grande, que también está presente en la capacidad. Cuando se presenta una capacidad, ambos números deben coincidir. De esta manera, para revocar los derechos ya otorgados, se cambia el número asociado al objeto. Problema: no se puede revocar selectivamente. Las revocaciones con ACL son más simples y más flexibles.

**18. En qué consisten los canales encubiertos.**

**R:** Es un canal que puede ser usado para transferir información desde un usuario de un sistema a otro, usando medios no destinados para este propósito por los desarrolladores del sistema. Para que la comunicación sea posible suele ser necesario un preacuerdo entre el emisor y el receptor que codifique el mensaje de una forma que el receptor sea capaz de interpretar. Esta muy relacionado con la esteganografía.

## Referencias


*6.5 Concepto de seguridad - Materia SisOperativos*. (s. f.). SisOperativos. Recuperado 12 de mayo de 2021, de https://sites.google.com/site/materiasisoperativo/unidad-6-proteccion-y-seguridad/6-5-concepto-de-seguridad

*ACL: Lista de Control de Accesos*. (s. f.). ACL. Recuperado 12 de mayo de 2021, de https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html

*Â¿QuÃ© es un virus informÃ¡tico?* (s. f.). Virus informatico. Recuperado 12 de mayo de 2021, de https://mx.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

*Bomba lógica | UNAM-CERT*. (s. f.). Bomba Logica. Recuperado 12 de mayo de 2021, de https://www.cert.unam.mx/glosario/bomba-l%C3%B3gica

ExsystemNews. (2021, 30 abril). *10 fallas principales de seguridad informática*. Exsystemusa. https://www.exsystemusa.com/single-post/2018/02/14/10-fallas-principales-de-seguridad-inform%C3%A1tica

*info@citel*. (s. f.). Infocitel. Recuperado 12 de mayo de 2021, de http://www.oas.org/en/citel/infocitel/2006/junio/seguridad_e.asp

Ranchal, J. (2020, 5 marzo). *10 acciones básicas para mejorar tu seguridad informática »*. MuySeguridad. Seguridad informática. https://www.muyseguridad.net/2018/11/09/10-acciones-basicas-para-mejorar-la-seguridad-informatica/

*SEGURIDAD Y MECANISMO DE PROTECCION EN LOS S.O. - carlos2987*. (s. f.). SisOperativos. Recuperado 12 de mayo de 2021, de https://sites.google.com/site/carlosraulsan2987/home/sistemas-operativos/unidad-6/seguridad-y-mecanismo-de-proteccion-en-los-so