Seguridad En Los Sistemas Operativos

¿Qué Es La Seguridad? (I)

- Según la definición de la Real Academia de la Lengua, seguridad es la cualidad de seguro, y seguro es algo libre y exento de todo peligro, daño o riesgo.

- Entonces se puede decir que la seguridad informática es un sistema informático exento de peligro.

¿Qué Es la Seguridad? (II)

- Seguridad Informática:
- “Es un conjunto de métodos y herramientas destinados a proteger los sistemas informáticos ante cualquier amenaza.”

¿Qué Es Un Sistema Operativo?

- Un Sistema Operativo es un conjunto de programas de procesos con las rutinas de control necesarias para mantener continuamente operativos dichos programas.

Funciones De Un SO

- Abstracción del hardware.
- Compartir los recursos justamente.
- Proteger a todos los procesos de los demás.
- Proteger a los datos de los usuarios.
- Asegurar la integridad de la información.

¿Qué Es Seguridad Informática?(I)

- En el ámbito informático, la seguridad debe garantizar en el sistema:
- **Consistencia:** Debe comportarse como esperamos.
- **Servicio:** Prestar los servicios de manera confiable, constante y consistente.

¿Qué Es Seguridad Informática? (II)

- **Protección:** Si un programa tiene errores, no debe afectar a la ejecución de otros procesos.
- **Control de acceso:** Los datos generados por un usuario no deben ser accesibles a otro usuario.
- **Autenticación:** El sistema debe poseer los mecanismos necesarios para asegurarse que un usuario es quien dice ser y tiene suficientes privilegios.

¿Qué Es Una Herramienta De Seguridad?

- Es un programa que corre en espacio de usuario diseñado para ayudar al administrador a mantener su sistema seguro, alertándolo o realizando por sí mismo las acciones necesarias.

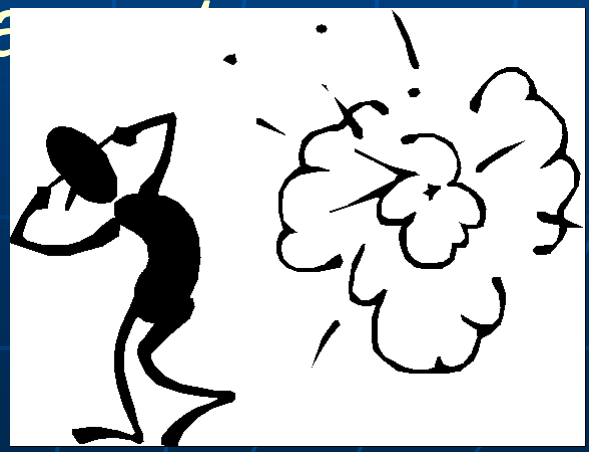
Las Herramientas De Seguridad Pueden Ser:

- Orientadas a host: Trabajan exclusivamente con la información disponible dentro del host (configuración, bitácoras, etc.).

- Orientadas a red: Trabajan exclusivamente con la información proveniente de la red (barridos de puertos, conexiones no autorizadas, etc.).

Muy Importante:

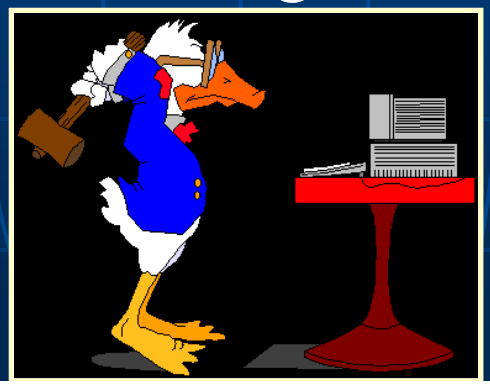
- *Toda herramienta de seguridad útil para el administrador es también útil para un atacante.*
- *Toda herramienta de seguridad disponible para un administrador debemos asumir que está también disponible para un ata*



Amenazas A La Seguridad (I)

- A la hora de proteger nuestros recursos es primordial identificar las *vulnerabilidades* y *amenazas* que ciernen contra ellos.

- Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad.



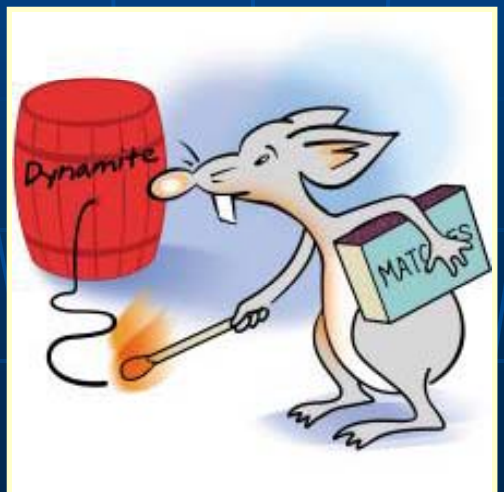
Amenazas A La Seguridad (II)

- Una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad.

- *Entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.*

Identificación De Amenazas

- Se suelen dividir las amenazas en tres grandes grupos en función del ámbito o la forma en que se pueden producir:
  - **Desastres del entorno.**
  - **Amenazas en el sistema.**
  - **Amenazas en la red.**



Clasificación De Amenazas (I)

- Desastres del entorno: se incluyen los posibles problemas relacionados con la ubicación del entorno de trabajo.

- Se han de tener en cuenta desastres naturales (terremotos, inundaciones), desastres producidos por elementos cercanos, como los cortes de fluido eléctrico.

Clasificación De Amenazas (II)

- Amenazas en el sistema: Contemplan todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas.

- Como ser: Fallos en el sistema operativo, medidas de protección que éste ofrece, fallos en los programas, copias de seguridad.

Clasificación De Amenazas (III)

- Amenazas en la red: Cada día es menos común que una máquina trabaje aislada de todas las demás.
- Se tiende a comunicar equipos mediante redes locales, intranets o Internet, y esta interconexión acarrea nuevas y peligrosas amenazas a la seguridad.

Clasificación De Amenazas (IV)

- Es necesario analizar aspectos relativos al cifrado de los datos en tránsito por la red, a proteger una red local del resto de Internet, o a instalar sistemas de autenticación de usuarios remotos.

Consideraciones Sobre Amenazas(I)

- Algo importante a la hora de analizar las amenazas es analizar los potenciales tipos de atacantes que pueden intentar violar nuestra seguridad.

- Es normal pensar en piratas informáticos llamados hackers, pero en realidad, la inmensa mayoría de problemas de seguridad vienen dados por atacantes internos a la organización afectada.

Consideraciones Sobre Amenazas (II)

- No siempre hemos de contemplar a las amenazas como actos intencionados contra nuestro sistema, muchos problemas pueden ser ocasionados por accidentes.

- Por ej.: Un operador que derrama una taza de café sobre una terminal hasta un usuario que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de programación.

Niveles De seguridad (I)

- Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia.

- Como no es posible la certeza absoluta, el elemento de riesgo siempre esta presente, independiente de las medidas que tomemos.

Niveles De Seguridad (II)

- Entendemos como *Seguridad Informática* a un conjunto de técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos, lo que requiere también un nivel organizativo.

TECNOLOGIA + ORGANIZACIÓN
= Sistema de Seguridad

Niveles De Seguridad (III)

Las Técnicas De Respaldo (Backup) y Sistemas Redundantes

- Los Sistemas de Respaldo y sistemas redundantes son dos técnicas para proteger los datos contra pérdida por borrado accidental o desastres fortuitos.

- Ambos sistemas son complementarios en cuanto a la seguridad que ofrecen ya que tanto los respaldos como la redundancia, por si solos, no cubren toda la necesidad.

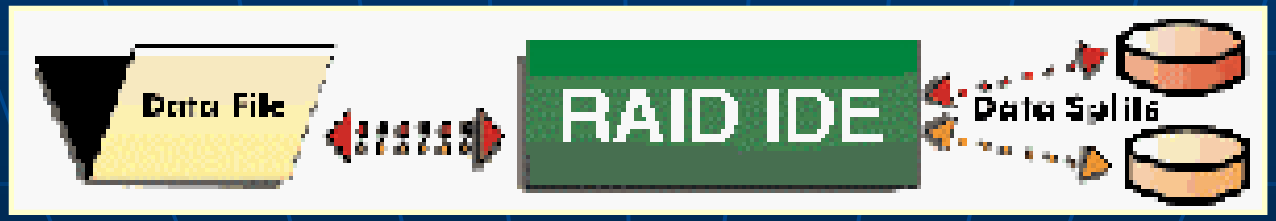
Sistemas RAID (I)

- Es un conjunto de unidades de disco que aparecen lógicamente como si fueran un solo disco.
- Los datos, distribuidos en bandas, se dividen entre dos o más unidades.
- Esta técnica incrementa el rendimiento y proporciona una redundancia que protege contra el fallo de uno de los discos de la formación.

Sistemas RAID (II)

- Para el sistema operativo, un RAID aparenta ser un sólo disco duro lógico.

- Los sistemas RAID se implementan en 7 configuraciones o niveles: RAID 0 a RAID 6.



Sistemas RAID (III)

- Cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y coste .
- También existen combinaciones de niveles de RAID.

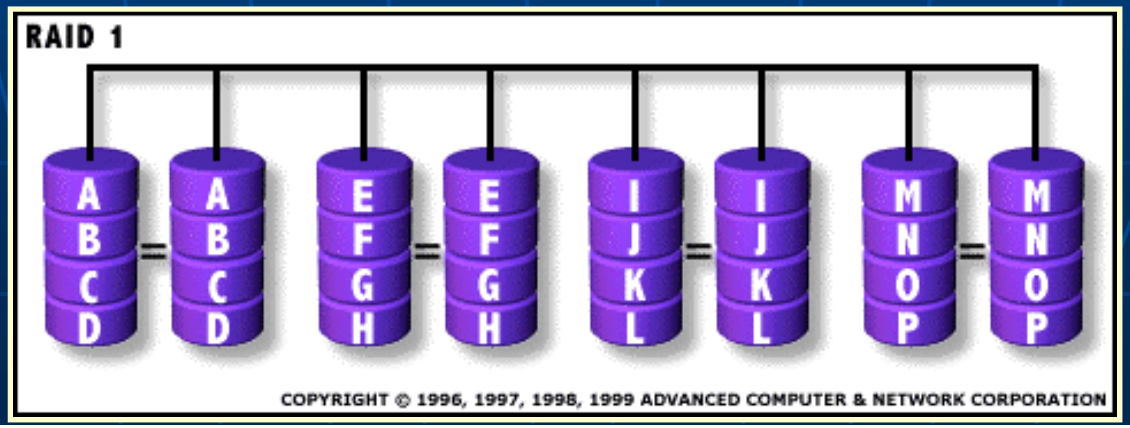
RAID 0: *Conjunto de discos divididos sin tolerancia a fallos (No Redundante).*

- La información se graba y se lee en paralelo entre varios discos.
- El rendimiento es muy bueno.

RAID 1: Espejo y Duplexing

Usa un tipo de configuración conocido como "mirroring".

- La información de un disco es completamente duplicada en otro disco.
- Se desperdicia el 50% de la capacidad y sólo maneja dos discos.



Tolerancia a Fallos

- Tolerancia a fallos es la capacidad de un sistema a responder a un suceso inesperado, como ser un fallo de suministro eléctrico o un fallo de hardware, de forma que no se pierdan datos.

Backups

- El "backup" consiste en realizar copias de seguridad de la información. Estas copias pueden realizarse de forma manual y periódica.
- ¿Cual es el objeto de hacer copias manualmente si tenemos un sistema redundante?.

Ventajas De Los Backups

- Es que por efectuarse según ciertos períodos, la información respaldada no es exactamente igual a la actual.

- Esto permite cierta protección contra los errores humanos, borrado accidental o uso negligente ya que si nos damos cuenta a tiempo, antes de que se cometa un backup del error, se pueden recuperar los datos con cierto desfase de tiempo y solo será necesario actualizar ese desfase

Virus y Troyanos (I)

- Existe una gran variedad de virus y troyanos cuyos efectos van desde los simplemente molestos hasta los que destruyen información específica o bien toda la contenida en el disco duro.

- Lo característico de los virus es que una vez que se instalan en el ordenador pasan largo tiempo sin provocar ningún efecto, aparte de infectar a todos los demás programas que se ejecuten

Virus y Troyanos (II)

- Los mecanismos conocidos para la propagación de virus son los archivos ejecutables, es decir aquellos con extensión .exe, .com o .bat.

- También en los componentes de Microsoft Office que aceptan macros con el lenguaje Visual Basic para Aplicaciones, principalmente Word y Excel con macros.

Virus y Troyanos (III)

- Pese a sus diferentes efectos, virus y troyanos comparten características comunes en su forma de operar y propagarse.

- Cabe señalar que los antivirus actuales detectan indistintamente virus y troyanos.

Confidencialidad, Integridad y Disponibilidad De La Información

- Lo importante es proteger la información. Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad.

- La seguridad informática se dedica principalmente a proteger:
  - La confidencialidad,
  - La integridad,
  - La disponibilidad de la información.

Confidencialidad De La Información

- La información solo puede ser conocida por individuos autorizados. Existen infinidad de posibles ataques contra la privacidad, especialmente en la comunicación de los datos.

- La transmisión a través de un medio presenta múltiples oportunidades para ser interceptada.

Integridad De La Información

- Se refiere a la seguridad de que una información no ha sido alterada, borrada, reordenada, copiada, etc., durante el proceso de transmisión o en su propio equipo de origen.

- Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

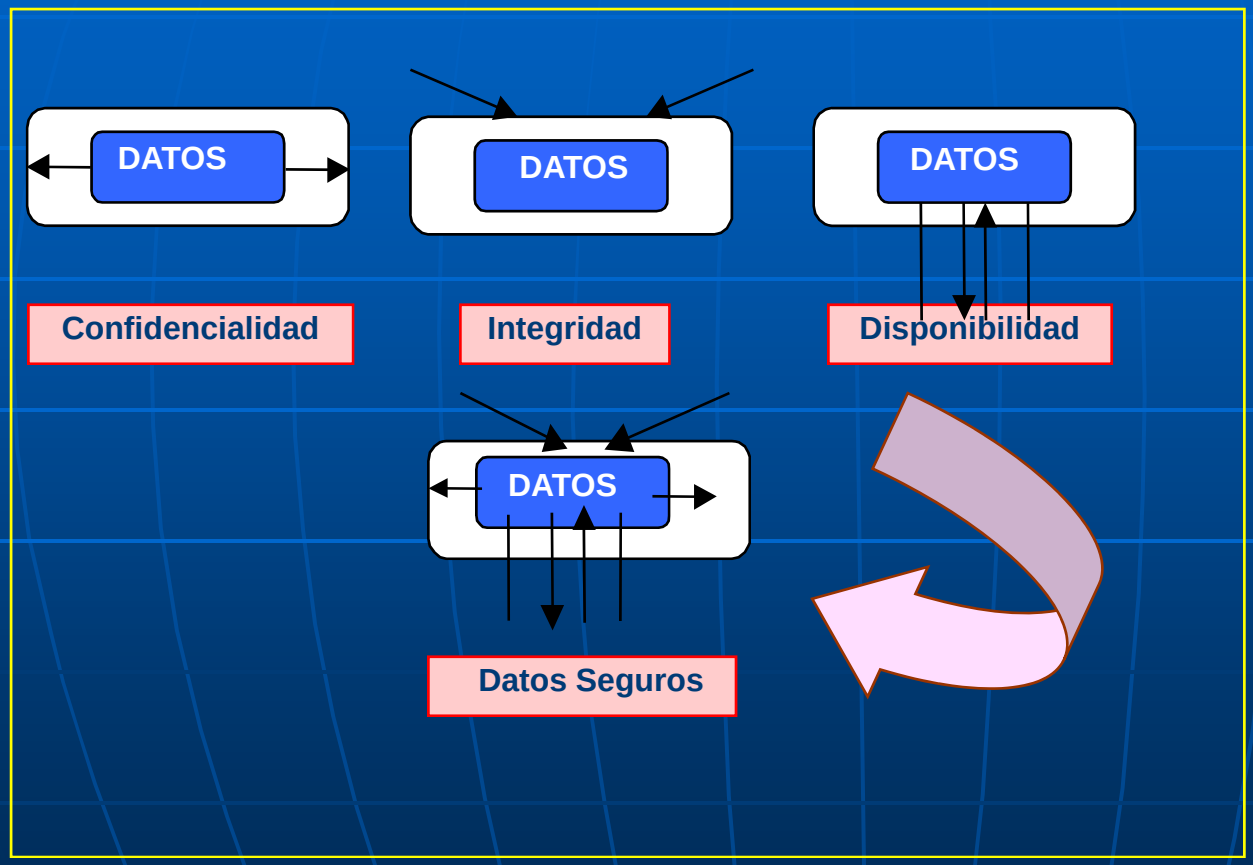
Disponibilidad De La Información

- Se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite.

- Esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

Datos Seguros

Si se cumplen los principios vistos anteriormente los datos están protegidos y seguros.



Esto es: los datos sólo pueden

ser conocidos por aquellos usuarios

que tienen privilegios sobre ellos,

sólo usuarios autorizados los

podrán crear o bien modificar,

y tales datos deberán estar

siempre disponibles.

Contramedidas o Métodos De Defensa

- Las medidas de seguridad que pueden establecerse en un sistema informático son de cuatro tipos fundamentales:
  - Físicas.
  - Lógicas.
  - Administrativas.
  - Legales.

Medidas Físicas (I)

- Aplican mecanismos para impedir el acceso directo o físico no autorizado al sistema. También protegen al sistema de desastres naturales o condiciones medioambientales adversas.

Medidas Físicas (II)

- Existen tres factores fundamentales a considerar:
  - El acceso físico al sistema por parte de personas no autorizadas.
  - Los daños físicos por parte de agentes nocivos o contingencias.
  - Las medidas de recuperación en caso de fallo.

Medidas Físicas: Tipos De Controles (I)

- Control de las condiciones medioambientales como ser temperatura, humedad, polvo, etc.
- Prevención de catástrofes, esto es incendios, tormentas, cortes de fluido eléctrico, sobrecargas, etc.
- Vigilancia, incluye cámaras, guardias, etc.

Medidas Físicas: Tipos De Controles (II)

- Sistemas de contingencia como fuentes de alimentación ininterrumpida, estabilizadores de corriente, fuentes de ventilación alternativa, etc.
- Sistemas de recuperación: copias de seguridad, redundancia, sistemas alternativos geográficamente separados y protegidos, etc.
- Control de la entrada y salida de materiales como elementos desechables, consumibles, material anticuado, etc.

Medidas Lógicas (I)

- Incluye las medidas de acceso a los recursos y a la información y al uso correcto de los mismos, así como a la distribución de las responsabilidades entre los usuarios.

Medidas Lógicas: Tipos De Controles (I)

- Establecimiento de una política de control de accesos. Incluyendo un sistema de identificación y autentificación de usuarios autorizados y un sistema de control de acceso a la información.
- Definición de una política de instalación y copia de software.
- Uso de la criptografía para proteger los datos y las comunicaciones.

Medidas Lógicas: Tipos De Controles (II)

- Uso de cortafuegos (FireWall) para proteger una red local de Internet.
- Definición de una política de copias de seguridad.
- Definición de una política de monitoreo (logging) y auditoría (auditing) del sistema.

Medidas Lógicas (II)

- Dentro de las medidas lógicas se incluyen también aquellas relativas a las personas y que podríamos denominar Medidas Humanas. Se trata de definir las funciones, relaciones y responsabilidades de distintos usuarios potenciales del sistema.

Medidas Lógicas (III)

- A cada grupo se le aplicará una política de control de accesos distinta y se le imputaran distinto grado de responsabilidades sobre el sistema, podemos identificar:

  - El administrador del sistema y en su caso el administrador de la seguridad.
  - Los usuarios del sistema.
  - Las personas relacionadas con el sistema pero sin necesidad de usarlo.
  - Las personas ajenas al sistema.

Medidas Administrativas (I)

- Son aquellas que deben ser tomadas por las personas encargadas de definir la política de seguridad para ponerla en práctica, hacerla viable y vigilar su correcto funcionamiento.

Medidas Administrativas: Tipos

- Documentación y publicación de la política de seguridad y de las medidas tomadas para ponerla en práctica.
- Debe quedar claro quien fija la política de seguridad y quien la pone en práctica.
- Establecimiento de un plan de formación del personal.

Medidas Administrativas (II)

- Los usuarios deben ser conscientes de los problemas de seguridad de la información a la que tienen acceso.
- Los usuarios deben conocer la política de seguridad de la empresa y las medidas de seguridad tomadas para ponerla en práctica.

Medidas Administrativas (III)

- Además deben colaborar, a ser posible voluntariamente, en la aplicación de las medidas de seguridad.
- Los usuarios deben conocer sus responsabilidades respecto al uso del sistema informático, y deben ser conscientes de las consecuencias de un mal uso del mismo.

Medidas Legales

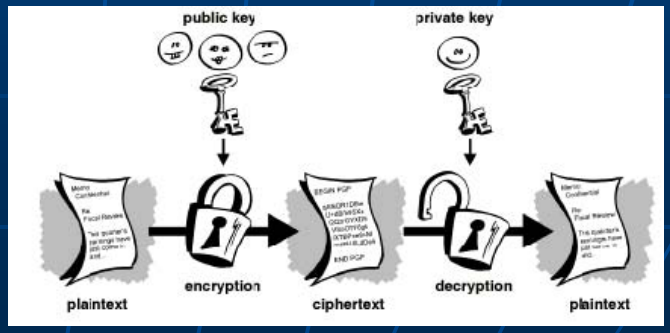
- Se refiere más a la aplicación de medidas legales para disuadir al posible atacante o para aplicarle algún tipo de castigo a posteriori.

- Este tipo medidas trascienden el ámbito de la empresa y normalmente son fijadas por instituciones gubernamentales e incluso instituciones internacionales.

Concepto De Criptosistema

- El diccionario de la Real Academia Española de la Lengua define la criptografía como "el arte de escribir con clave secreta o de forma enigmática".

- La Criptografía es un conjunto de técnicas que mediante la utilización de algoritmos y métodos matemáticos sirven para cifrar y descifrar mensajes.



¿Qué Cosas Hacen A Un Sistema Seguro? (I)

- Un tratamiento total de seguridad debe incluir seguridad externa e interna:
- La Seguridad Externa debe asegurar la instalación computacional contra intrusos y desastres como incendios e inundaciones. Concedido el acceso físico, el Sistema Operativo debe identificar al usuario antes de permitirle el acceso a los recursos.

¿Qué Cosas Hacen A Un Sistema Seguro? (II)

- La Seguridad Interna trata de los controles incorporados al hardware y al Sistema Operativo para asegurar la confiabilidad, operabilidad y la integridad de los programas y datos.

Control De Acceso Al Sistema

- Dentro de un sistema de seguridad, cada usuario ha de tener su parcela de trabajo perfectamente definida y delimitada.

- Por encima de ellos, para solucionar incidencias, instalar nuevas aplicaciones y asegurar que la comunicabilidad con el exterior siempre obedezca a los intereses y objetivos por los cuales se instala el sistema, debe existir la figura del Administrador.

Administrador De Seguridad

- Es todo aquel que posee un nivel de acceso superior al del propio Usuario para realizar tareas de instalación/desinstalación, mantenimiento y soporte del sistema.

Control De Acceso A Datos

- Lo fundamental de la seguridad interna es controlar el acceso a los datos almacenados.

- Los derechos de acceso más comunes son:
  - Acceso de lectura.
  - Acceso de escritura.
  - Acceso de ejecución.

Otra Transformación Criptográfica: La Firma Digital

- Puede ser definida como una secuencia de datos electrónicos (bits) que se obtienen mediante la aplicación a un mensaje determinado de un algoritmo (fórmula matemática) de cifrado.

- Equivale funcionalmente a la firma autógrafa en orden a la identificación del autor del que procede el mensaje.

La Firma Digital

- Desde un punto de vista material, la firma digital es una simple cadena o secuencia de caracteres que se adjunta al final del cuerpo del mensaje firmado digitalmente.

- Se basa en la utilización combinada de técnicas distintas de criptografía.

Sistemas Operativos Seguros

- Principales Amenazas y Contramedidas de los SO:

Amenaza	Descripción	Técnicas de reducción de riesgos
Suplantación de la identidad	Acceso ilegal a un sistema de forma local o remota.	Características de seguridad de compatibilidad de autenticación: Passport, Kerberos y de certificados X.509, entre otras.
Alteración de datos	Modificación malintencionada de los datos.	Características de seguridad de compatibilidad de autorización y protección contra modificaciones: listas de control de acceso (ACL), privilegios, sistema de archivo cifrado (EFS), firmas digitales, etc.

Amenaza	Descripción	Técnicas de reducción de riesgos
Repudio	Negación de una acción por parte de Determinados usuarios sin que otra parte tenga forma De demostrarlo.	Características de seguridad de compatibilidad de autenticación, autorización y seguridad: auditoría, firmas digitales, etc.
Revelación De información	Revelación de información a individuos que no deberían tener acceso a la misma.	Características de seguridad de autorización y protección contra modificaciones: autorización, protocolos de seguridad mejorados, cifrado, etc.

Amenaza	Descripción	Técnicas de reducción de riesgos
Negación de servicio	Negación del servicio a usuarios con acceso válido.	Características de seguridad de compatibilidad de seguridad de conexión a Internet: servidor de seguridad, autenticación, autorización, filtrado, límite de ancho de banda, entre otras.
Elevación de privilegio	Un usuario sin Privilegios Obtiene Acceso Privilegiado Para Comprometer o destruir El sistema.	Características de seguridad de autenticación, autorización y administración de seguridad: directiva de grupo, restricciones de sistema o software, etc.

Descripción General De Windows Vista (I)

- Microsoft realiza importantes inversiones en tecnología para hacer que los clientes tengan mayor seguridad.

- Parte de estos esfuerzos consiste en utilizar un ciclo de vida de desarrollo de seguridad para desarrollar software más seguro y proporcionar innovaciones tecnológicas en la plataforma para ofrecer varios niveles de defensa o "defensa en profundidad".

Descripción General De Windows Vista (II)

- Windows Vista incluye muchas características y mejoras de seguridad para proteger equipos cliente frente a la última generación de amenazas, entre las que se incluyen gusanos, virus y otro software malintencionado (*malware*).

Seguridad De Windows Vista (I)

- Protección de cuentas de usuario permite a los usuarios trabajar y cambiar la configuración común sin necesidad de tener privilegios de administrador.

- Esto evita que los usuarios realicen cambios potencialmente peligrosos en sus equipos, sin que esto limite su capacidad de ejecutar aplicaciones.

Seguridad De Windows Vista (II)

- El explorador Web integrado de Windows Vista, Microsoft Internet Explorer, incluye muchas mejoras de seguridad que protegen a los usuarios del "phishing" y de ataques de suplantación de identidad.

- Las nuevas características incluyen Internet Explorer en modo protegido, que ayuda a evitar la eliminación o modificación de valores de configuración y de datos de los usuarios por parte de sitios Web malintencionados o de código dañino.

Seguridad De Windows Vista (III)

- Las funciones de Windows Vista contra el código dañino detectan muchos tipos de software potencialmente sospechosos.
- Pueden preguntar al usuario si desean permitir que las aplicaciones realicen cambios que podrían ser malintencionados.

Seguridad De Windows Vista (IV)

- El nuevo filtro de salida del servidor de seguridad proporciona control administrativo para aplicaciones de igual a igual que permiten compartir archivos y otras aplicaciones similares que las empresas deseen restringir.

Seguridad De Windows Vista (V)

- El Endurecimiento de Servicios de Windows limita el daño que pueden causar los atacantes en el improbable caso de que logren poner en peligro un servicio.

- Esto reduce el riesgo de que los atacantes realicen cambios permanentes en el cliente de Windows Vista o que ataquen otros equipos de la red.

Seguridad De Windows Vista (V)

- Los administradores pueden utilizar la protección de acceso a la red para evitar que los clientes que no cumplan con la directiva interna de mantenimiento del sistema se conecten a la red interna y distribuyan código dañino a otros equipos.

Seguridad de Windows Vista (VI)

- Gracias al inicio seguro, los usuarios de empresas con equipos que cuentan con el correspondiente hardware de habilitación se pueden beneficiar de la protección de datos en caso de pérdida o robo de equipos.

- Las unidades de disco duro de un equipo que se ejecuta con inicio seguro estarán completamente cifradas lo que impide el acceso a los datos, los archivos, los mensajes de correo electrónico y la propiedad intelectual para cualquiera que trate de utilizar un equipo sin permiso.

Seguridad De Windows Vista (VII)

- Finalmente, para asegurar que los departamentos de TI puedan elegir entre una gran variedad de mecanismos de autenticación, Windows Vista incluye una nueva arquitectura de autenticación que otros fabricantes podrán ampliar con mayor facilidad.
- Esto hará posible contar con una mayor opción de tarjetas inteligentes, escáneres de huellas digitales y otras formas de autenticación segura. Todas estas mejoras de seguridad harán que los usuarios tengan más confianza al utilizar sus PC.

Recomendaciones De Seguridad En Sistemas Distribuidos (I)

- Efectuar un análisis de riesgos: Trazar todos los elementos que conforman nuestro sistema (hardware y software) y observar cuáles involucran más o menos riesgo.
- Esto desembocará en un plan de seguridad cuyo objetivo es disminuir el riesgo total del sistema, que se puede modelar como la suma de los riesgos de sus componentes:

Recomendaciones De Seguridad En Sistemas Distribuidos (II)

- RIESGO TOTAL=RIESGO(componente 1)+ RIESGO(componente 2) ...
- El riesgo de cada componente está en función directa a las pérdidas que ocasionaría el que éste deje de operar, así como en función de cuán vulnerable es dicho componente en este momento.

Recomendaciones De Seguridad En Sistemas Distribuidos (III)

- Lo más valioso debe alejarse de lo más vulnerable: Es decir, conviene separar o dividir un componente de alto riesgo en dos partes suficientemente alejadas e independientes a fin de que el riesgo total disminuya.

Recomendaciones De Seguridad En Sistemas Distribuidos (IV)

- Por ejemplo, los portales de comercio electrónico deben dar cara a Internet, siendo vulnerables en principio, y a la vez manejar información muy costosa, como transacciones con tarjeta de crédito.

- Esto los convierte en un sistema de alto riesgo. Sin embargo es casi universal la separación que se efectúa entre los componentes dedicados a dar cara a Internet (como los Web Servers) y los componentes que manipulan la información comercial (generalmente sistemas DBMS.)

Recomendaciones De Seguridad En Sistemas Distribuidos (V)

- Mantener las cosas simples: Un sistema complejo es más difícil de asegurar y potencialmente proporciona una mayor cantidad de puertas abiertas a los atacantes.

- Un ejemplo citado es la seguridad de una red de estaciones Windows manipulada por usuarios inexpertos. No resulta práctico efectuar un profundo trabajo de seguridad en las estaciones, más allá de la instalación del antivirus, puesto que por un lado, son muchas, y por otro, los usuarios suelen modificar la configuración en tanto instalan y desinstalan su software sin dar aviso a nadie.

Recomendaciones De Seguridad En Sistemas Distribuidos (VI)

- Asegurar la seguridad en todos los niveles: No confiar el sistema a un único mecanismo de seguridad.

- Esto obliga a implementar la seguridad no en un único punto evidentemente vulnerable, sino en todos los lugares por donde fluye la información al interior de cada componente involucrado.

Recomendaciones De Seguridad En Sistemas Distribuidos (VII)

- Encriptar tanto como sea posible: Los canales de comunicación más vulnerables o de mayor cercanía al público requieren una encriptación "más fuerte", es decir, más difícil de descifrar por los curiosos o atacantes.

- Las herramientas capaces de hacer esto son muchas, dependiendo del contexto en que nos encontremos. Por ejemplo, los sistemas DBMS más avanzados incorporan la encriptación como una opción normal para los datos almacenados.

Recomendaciones De Seguridad En Sistemas Distribuidos (VIII)

- No confiar en la autenticación estándar: Es de rigor que la autenticación también sea cada vez más sofisticada, lo cual implica abandonar para siempre diversos mecanismos estándar muy arraigados.

- No usar la configuración estándar: Por lo general los sistemas operativos y las aplicaciones se instalan con una configuración determinada y de carácter genérico.

Recomendaciones De Seguridad En Sistemas Distribuidos (IX)

- La seguridad hacia el interior: La mayor amenaza de ataques al sistema no proviene de fuera, sino que parte desde el interior de la organización.

- El análisis de riesgos debe incluir posibles ataques originados en el interior, incluyéndose el robo de contraseñas, la modificación de archivos de configuración, la desactivación de las barreras de protección, etc.

Recomendaciones De Seguridad En Sistemas Distribuidos (X)

- Educar a los usuarios: Una de las mayores ayudas que puede recibir un hacker que intenta infiltrarse en el sistema consiste en obtener información acerca de éste, donde muchas veces la interacción encubierta con los usuarios de la organización, obtienen la contraseña en medio de una conversación desinteresada.

- Esto se suele denominar "Ingeniería Social".

Recomendaciones De Seguridad En Sistemas Distribuidos (XI)

- Descargas de software de Internet: Como regla general, el software no debería ser descargado de Internet, sino adquirido de una fuente confiable.
- Si esto es imprescindible, debemos asegurarnos que el software que descargamos es realmente lo que hemos pretendido descargar y que no ha sido modificado.

Recomendaciones De Seguridad En Sistemas Distribuidos (XII)

- No permitir conexiones directas desde la red interna a Internet:
  No deberíamos conectar nuestra red interna a Internet, sin embargo como es imprescindible para nuestra organización, debemos buscar algún mecanismo de protección.

Recomendaciones De Seguridad En Sistemas Distribuidos (XIII)

- Una de las soluciones más generalizadas la constituyen los sistemas denominados proxy.
- Los usuarios de nuestra red local, se conectan aparentemente a Internet, pero realmente lo hacen hacia el programa proxy.
- La función de éste es básicamente conectarse a Internet. El resultado es que los posibles atacantes observarán al proxy conectándose, pero no podrán acceder a la red interna.

Las Herramientas De Seguridad e Internet (I)

- La seguridad es una de las preocupaciones principales del administrador de red.

- Hay muchas páginas inseguras en Internet y la mayor parte de nosotros desconoce lo que realmente pasa durante la transmisión de datos, o si éstos pueden venir acompañados de virus o intrusos.

Las Herramientas De Seguridad e Internet (II)

- Es necesario desarrollar un sistema que proteja a la red interna de la otra red como Internet.
- Mediante el uso de herramientas equipadas para evitar automáticamente que un usuario no-autorizado ataque al equipo.

Cortafuegos o *Firewall (I)*

- Es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red.

Cortafuegos o *Firewall (II)*

- La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet.

Ventajas De Un Cortafuegos

- Protección de intrusiones: El acceso a ciertos segmentos de la red de una organización, sólo se permite desde máquinas autorizadas de otros segmentos de la organización o de Internet.

- Protección de información privada: Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios.

Políticas Del Cortafuegos(I)

- Hay dos políticas básicas en la configuración de un cortafuegos :

- Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten.

Políticas Del Cortafuegos(II)

- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado.

- *La política restrictiva es la más segura.*

Detección De Intrusiones

- Es el proceso de monitorizar redes de ordenadores y sistemas en busca de violaciones de políticas de seguridad. Los sistemas de detección de intrusiones están compuestos por tres elementos funcionales básicos:

Detección De Intrusiones: Elementos Funcionales

- Una fuente de información que proporciona eventos de sistema.
- Un motor de análisis que busca evidencias de intrusiones.
- Un mecanismo de respuesta que actúa según los resultados del motor de análisis.

Servicio De Autenticación Kerberos

- Kerberos es un servicio de autenticación que “cuida las puertas de la red”.
- En una red con usuarios que solicitan servicios desde muchas terminales, hay tres enfoques básicos que se pueden utilizar para dar control de acceso.

Kerberos: Enfoques Para El Control De Acceso

- No hacer nada: Confiar en que la máquina en la que el usuario está "logueado" evite accesos no autorizados.
- Requerir que el host pruebe su identidad, pero confiar en su palabra sobre quién es el usuario.
- Requerir que el usuario pruebe su identidad para cada servicio solicitado.

Kerberos: Niveles De Protección (I)

- Kerberos provee tres niveles distintos de protección.

- *Autenticación:* Prueba que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la conexión de red y luego se asuma que los siguientes mensajes de una dirección de red determinada se originan desde la parte autenticada.

Kerberos: Niveles De Protección (II)

- *Integridad de datos:* Asegura que los datos no se modifican en tránsito. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo. Éstos se denominan mensajes seguros.

- *Privacidad de datos:* Asegura que los datos no son leídos en tránsito. En este caso no sólo se autentica cada mensaje sino que también se encripta. Éstos son mensajes privados.

¿Qué Son Las Políticas De Seguridad Informática (PSI)? (I)

- Las PSI establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.
- Es una descripción de los que deseamos proteger y el por qué de ello.

¿Qué Son Las PSI? (II)

- Deben ofrecer explicaciones comprensibles acerca de por qué deben tomarse ciertas decisiones, transmitir por qué son importantes estos u otros recursos o servicios.

- Deben mantener un lenguaje común, libre de tecnicismos y términos legales que impidan una comprensión clara de las mismas, sin sacrificar su precisión y formalidad dentro de la empresa.

Elementos De Una PSI (I)

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

Elementos De Una PSI (II)

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

Elementos De Una PSI (III)

- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que ella tiene acceso.

¿Cómo Desarrollar Una PSI? (I)

- 1) Identifique y evalúe los activos: Qué activos deben protegerse y cómo protegerlos:

- Hardware: terminales, estaciones de trabajo, procesadores, teclados, unidades de disco, impresoras, líneas de comunicación, cableado de la red, servidores de terminales.

¿Cómo Desarrollar Una PSI? (II)

- Software: sistemas operativos, programas fuente, programas objeto, programas de diagnóstico, utilerías, programas de comunicaciones.

- Datos: durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos, en tránsito sobre medios de comunicación.

¿Cómo Desarrollar una PSI? (III)

- Personas: usuarios, personas para operar los sistemas.

- Documentación: sobre programas, hardware, sistemas, procedimientos administrativos locales.

¿Cómo Desarrollar Una PSI? (IV)

- 2) Identifique las amenazas: ¿Cuáles son las causas de los potenciales problemas de seguridad?
- Considere la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran.

- 3) Evalué los riesgos: Debe calcularse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tienen el potencial para causar mucho daño.

¿Cómo Desarrollar Una PSI?(V)

- 4) Asigne las responsabilidades: Seleccione un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa.

- Sería ideal la participación de un representante por cada departamento de la compañía.

¿Cómo Desarrollar una PSI? (VI)

- 5) Establezca políticas de seguridad: Estos documentos deben tener información específica relacionada con las plataformas informáticas, las plataformas tecnológicas, las responsabilidades del usuario y la estructura organizacional.

- De esta forma, si se hacen cambios futuros, es más fácil cambiar los documentos subyacentes que la política en sí misma.

¿Cómo Desarrollar Una PSI?(VII)

- 6) Implemente una política en toda la organización: La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad y reconocer quién es el propietario de los sistemas y datos específicos.

ISO 17799: La Norma Técnica Global De Seguridad

- Publicada en diciembre de 2000 por la Organización Internacional de Normas.
- Se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

Las Diez Áreas De Control De ISO 17799

- Política de seguridad.
- Organización de la seguridad.
- Control y clasificación de los recursos de información.
- Seguridad del personal.
- Seguridad física y ambiental.
- Manejo de las comunicaciones y las operaciones.
- Control de acceso.
- Desarrollo y mantenimiento de los sistemas.
- Manejo de la continuidad de la empresa.

Libro Naranja (Orange Book) (I)

- El Libro Naranja es creado por el Gobierno de EEUU ante la necesidad de evaluar la seguridad de los sistemas informáticos y tener una medición confiable.
- Se encuentra en formato texto o pdf.

Libro Naranja (Orange Book) (II)

- Define cuatro extensas divisiones jerárquicas de seguridad para la protección de la información.

- En orden creciente de confiabilidad se tienen:
  - D Protección Mínima.
  - C Protección Discrecional.
  - B Protección Obligatoria.
  - A Protección Controlada.

Libro Naranja (Orange Book) (III)

- Cada clase se define con un grupo específico de criterios que un sistema debe cubrir, para ser certificado con la evaluación en alguna clase.

- Este criterio cae en 4 categorías generales:
  - Políticas de seguridad,
  - Responsabilidad,
  - Confianza y,
  - Documentación.

Conclusión (I)

Consistencia

Autenticación

Garantizar

Servicio

Protección

Control de Acceso

Conclusión (II)

Identificar Amenazas
Y Vulnerabilidades

- Desastres del Entorno
- Amenazas al Sistema
- Amenazas a la Red

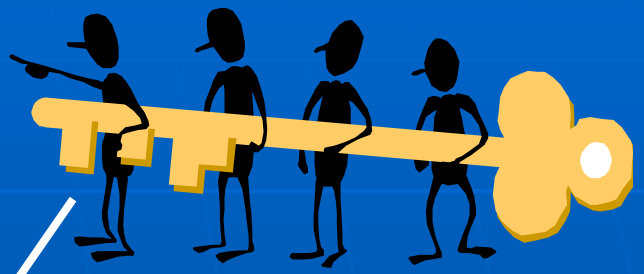
Conclusión (III)

Establecer Niveles de Seguridad que queremos lograr

- Respaldos
- Backups
- Virus y Troyanos

Conclusión: Medidas

Físicas



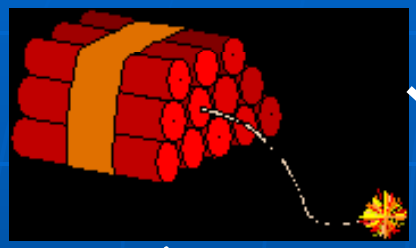
Lógicas

Tomar Medidas

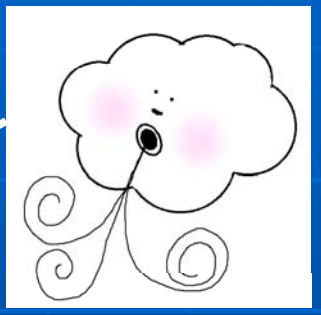
Administrativas

Legales

Conclusión: Medidas Físicas

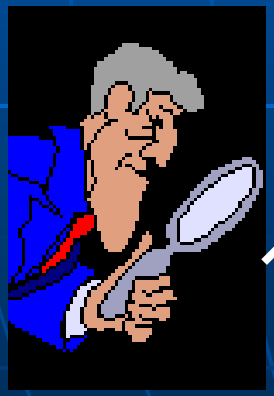


Catástrofes



Ventilación

Físicas

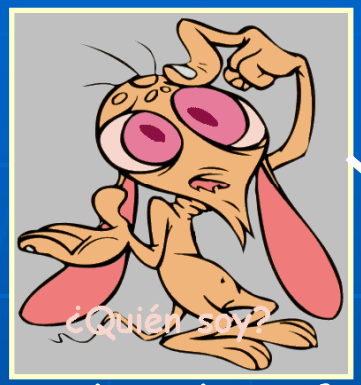


Vigilancia

Desastres ambientales

Sist. Redundantes

Conclusión: Medidas Lógicas



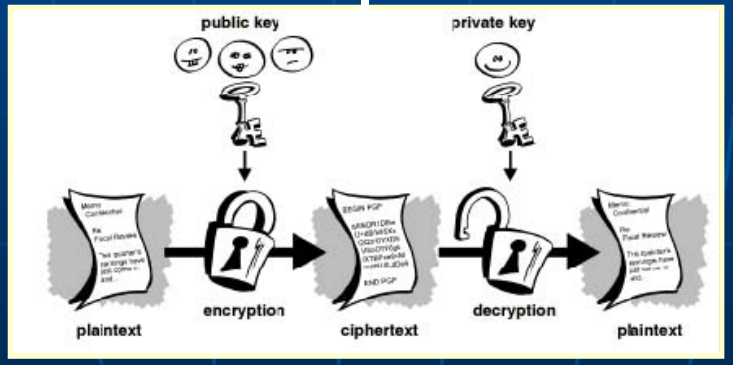
Sist. de Identificación y Autentificación

Kerberos

Cortafuegos

Lógicas

Políticas de Copia de Software



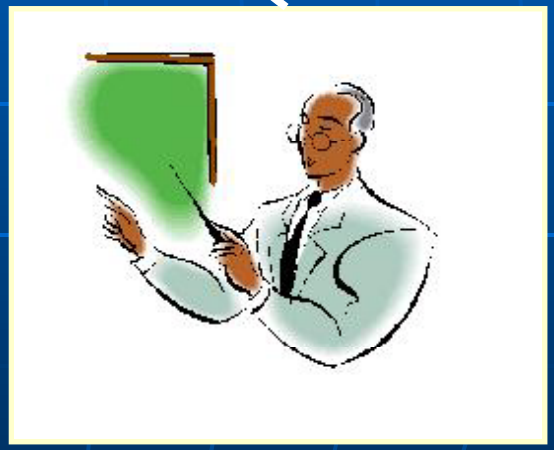
Criptografía y firma digital

Auditoría y Monitoreo

Conclusión: Medidas Administrativas

Administrativas

Establecer Políticas de Seguridad



Administrador de Seguridad

Conclusión: Redes

- Recomendaciones de Seguridad en Redes:
  - Análisis de riesgo de cada componente.
  - Alejar lo más valiosos de lo más vulnerable.
  - Asegurar la seguridad en todos los niveles.
  - Encriptar los datos.
  - No confiar en la autenticación estándar.
  - No usar configuración estándar.
  - No descargar software de Internet.
  - Educar a los usuarios.

Conclusión (IV)

- En consecuencia, la seguridad total o 100% no es posible, pues no existe ningún elemento que no esté expuesto a situaciones no controladas o inesperadas, que alteren su funcionamiento.

- Pero si tomamos las medidas preventivas e implementamos correctamente las herramientas que día a día nos brinda la tecnología, podemos lograr un Sistema Operativo Seguro.

Muchas Gracias Por La Atención

Gabriela Mojsiejczuk
Ayudante Alumno de la
Cátedra Sistemas Operativos.
UNNE