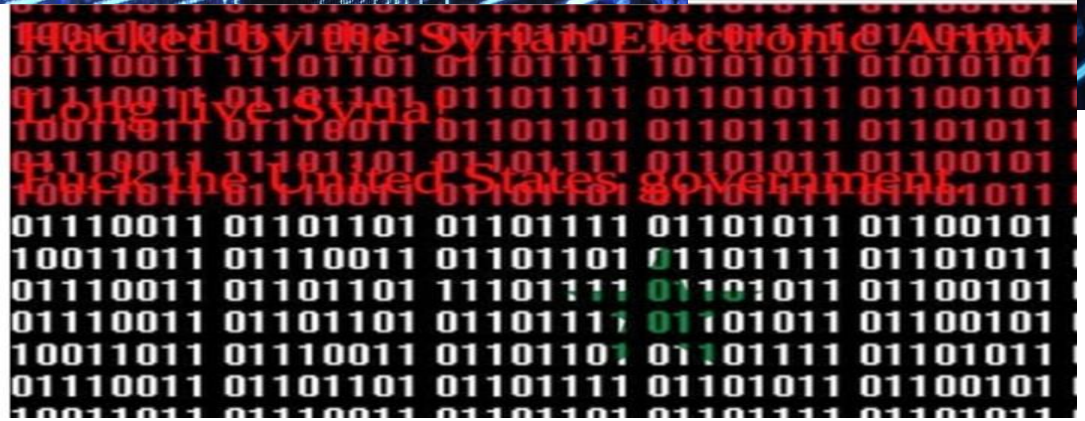
SIMPOSIO 2015
PROSPECTIVAS DEL GOBIERNO ELECTRÓNICO EN VENEZUELA

SEGURIDAD DE DATOS ELECTRÓNICOS

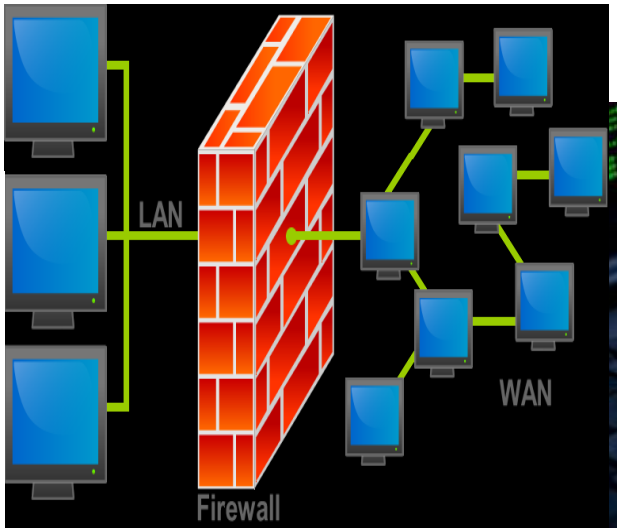
UNEFA - Asamblea Nacional, 2 de julio de 2015



Dr. Sergio Teijero
Profesor e Investigador Asociado
Universidad Central de Venezuela
UNEFA

Los defensores tienen que cerrar todas las puertas. Porque

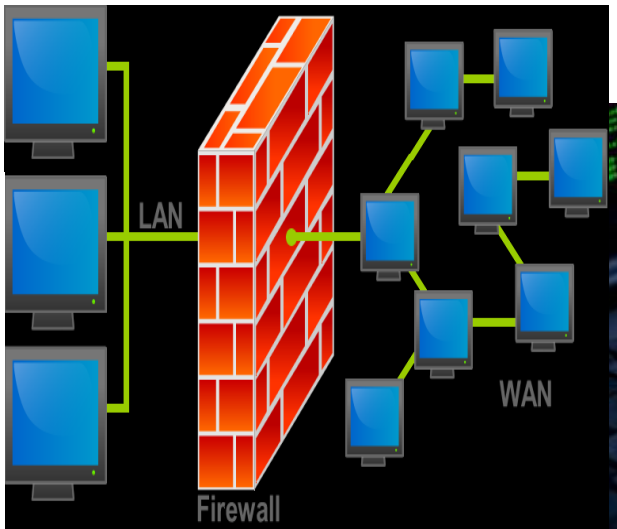
Los invasores sólo necesitan encontrar* una *abierta.



Veamos el siguiente video

SEGURIDAD INFORMATICA - POLITICAS PARA CUIDAR SUS DATOS

https//www.youtube.com/watch?v=jkvpLKRfwt4



¿QUÉ ES SEGURIDAD DE DATOS?

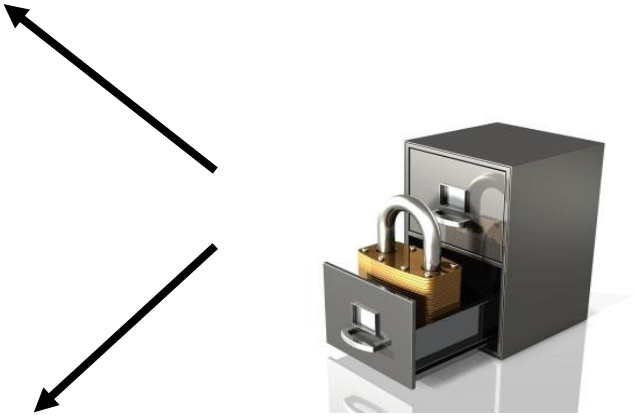
Son todas aquellas medidas preventivas tomadas por el ser humano, las organizaciones y los sistemas tecnológicos que permitan resguardar y proteger los datos y la información, buscando mantener la confidencialidad, la autenticidad y la integridad de la misma

¿QUÉ ES SEGURIDAD DE DATOS?

Para el usuario que tiene datos en un sistema de información, las expectativas sobre su seguridad incluyen:

Que pueda tener acceso a los datos cuando los necesite

Que los datos no desaparezcan espontáneamente



Que los datos no se alteren sin autorización

Que los datos no se lean sin autorización

¿QUÉ ES SEGURIDAD DE DATOS?

Estas expectativas pueden verse frustradas por varios factores como son: *Accidentales*

El software tiene errores

El hardware no es confiable y puede fallar

Puede haber un desastre natural que destruye el sistema o sus datos

Un administrador que accidentalmente limpia la base de datos y no existe respaldo

¿QUÉ ES SEGURIDAD DE DATOS?

Los factores intencionales son los ataques informáticos e incluyen:

Un intruso que lee y modifica los datos

Alguien falsifica mi identidad y manda mensajes en mi nombre

Alguien bombardea el sistema con tanto tráfico que el mismo colapsa

Alguien interviene en los medios físicos de la red para captar información o engañar al sistema

¿QUÉ ES SEGURIDAD DE DATOS?

Ataques informales

Amenazas o sobornos

Traidores (los empleados resentidos)

Los entretenidos

Los incompetentes y los no-interesados

¿QUÉ ES SEGURIDAD DE DATOS?

¿Qué tipo de protección se necesita para protegerse de ataques intencionales e informales?

- **Confidencialidad.** El contenido de un mensaje sólo se revela a quien puede descifrarlo.
- **Autentificación.** Un usuario o proceso puede comprobar su identidad.

- **Autorización.** Un usuario o proceso puede mostrar que tiene ciertos derechos de acceso.
- **Integridad.** Un mensaje no ha sido alterado indebidamente.

¿QUÉ ES SEGURIDAD DE DATOS?

¿Cómo se distingue entre *autentificación* y *autorización*?

Para viajar en avión, tengo que presentar un boleto en el mostrador del aeropuerto, junto con la cédula o pasaporte. Esto es autentificación.

Una vez dentro del avión, tengo que mostrar el pase de abordaje, pero nadie me pide la cédula. Esto es autorización.

POLÍTICA DE SEGURIDAD

Las políticas de seguridad permiten crear conexiones seguras, enviar y recibir información encriptada y filtrar accesos de información

Una adecuada *política de seguridad* debe garantizar, primordialmente, la integridad de los datos y un adecuado control de acceso.

Idear una política de seguridad de red requiere que la organización estime, en alto grado, el valor de la información.

La política debe aplicarse a la información almacenada en las computadoras, así como a la información que atraviesa una red.

POLÍTICA DE SEGURIDAD

La política de seguridad debe contener:

- **Los usuarios que requieren ingresar a los recursos de la red, identificando la clase de usuario.**
- **Qué tipo de privilegio de red es aceptable para cada usuario.**

- **Qué tipo de uso será restringido.**
- **Contraseña inicial de usuario con cambio periódico.**
- **Responsabilidades del usuario.**
- **Guías para el uso de los recursos.**
- **Sanciones a quienes violen la política de seguridad.**

POLÍTICA DE SEGURIDAD

La política también deberá contener las responsabilidades de los administradores del sistema.

Cuando ocurran amenazas a la seguridad de la red o violaciones, el administrador podrá examinar los directorios y archivos privados del usuario para diagnosticar la amenaza, operando de inmediato hasta el límite establecido en la política de seguridad

NIVELES DE SEGURIDAD

Nivel D1. **Es el más elemental y se refiere a los sistemas operativos de bajo nivel que no distinguen entre usuarios y no tienen control sobre la información que puede introducirse en los medios de almacenamiento.**

Nivel C, mediante C1 y C2

C1, sistema de protección de seguridad discrecional, donde los usuarios deben identificarse por medio de un nombre y una contraseña para determinar, sus derechos de acceso a los programas e información.

C2, utiliza niveles de autorización para proteger a los usuarios.

NIVELES DE SEGURIDAD

Nivel B, mediante B1, B2 y B3

B1, **protección de seguridad etiquetada, soporta seguridad de multinivel, como la secreta y la utrasecreta, y parte del principio de que un objeto bajo control de acceso obligatorio, no puede aceptar cambios en los permisos realizados por el dueño del archivo.**

B2, **protección estructurada, requiere que se etiquete cada objeto y se refiere al problema de comunicación de objetos de diferentes niveles de seguridad.**

NIVELES DE SEGURIDAD

***Nivel B3*, nivel de dominios de seguridad, refuerza a los dominios con la instalación de hardware y requiere que la estación de trabajo del usuario se conecte al sistema por medio de una ruta de acceso segura.**

***Nivel A.* Diseño verificado es el más elevado, incluye todos los componentes de los niveles inferiores y el hardware y software son protegidos para evitar violaciones.**

CRIPTOGRAFÍA

Es la ciencia de la seguridad de mensajes.

Entre sus términos básicos se encuentran:

Mensaje

Codificación del mensaje (encriptamiento)

Recuperación del texto original (desencriptamiento)

Los algoritmos de criptografía utilizan una llave para el encriptamiento y desencriptamiento. Un mensaje puede ser desencriptado únicamente si la llave de desencriptamiento, coincide con la llave de encriptamiento.

ALGORITMOS DE ENCRIPTAMIENTO

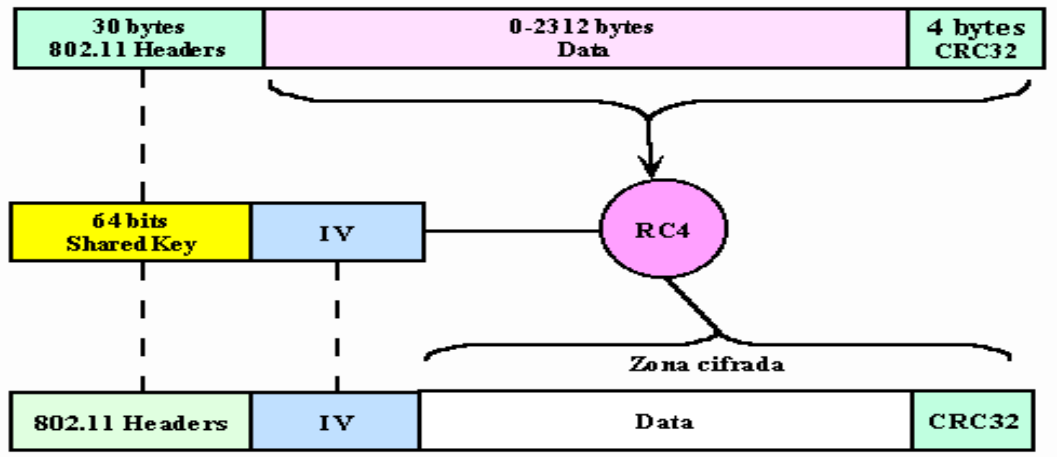
Los dos tipos básicos de algoritmos de encriptamiento son: el simétrico o llave secreta y el asimétrico o llave pública.

El simétrico, utiliza la misma llave para encriptar y desencriptar y el asimétrico utiliza llaves diferentes, siendo la llave secundaria derivada de la primera.

Existen otros tipos de algoritmos de encriptamiento como son: los de mezcla de funciones y los de generación de números aleatorios.

ALGORITMOS DE ENCRIPTAMIENTO

Los algoritmos por *mezcla de funciones,* presentan una combinación de funciones de encriptamiento de modo, que la única forma de desencriptar el mensaje es corriendo la misma rutina con sus correspondientes llaves.



Los algoritmos por *generación de números aleatorios,* generan llaves numéricas de forma aleatoria que son utilizadas por el ente de encriptamiento y desencriptamiento.

FIRMAS DIGITALES Y FIREWALL

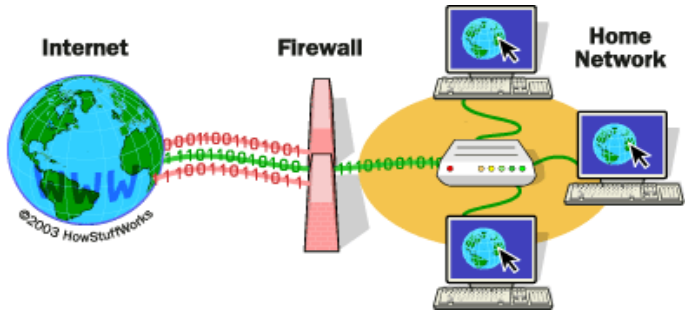
Las *firmas digitales* son bloques de datos que han sido codificados con una llave secreta y que se pueden decodificar con una llave pública, siendo utilizados principalmente para verificar la autenticidad del mensaje o la de una llave pública.

Para ofrecer seguridad en la comunicación entre dos redes se utiliza la técnica de FIREWALL

FIREWALL

Un *firewall o cortafuego* es un filtro de paquetes configurado para proteger a una organización contra el tráfico de una red. El FIREWALL

Decide los servicios que pueden ser accesados desde el exterior de una red privada



Quiénes pueden ejecutar estos servicios

Qué servicios pueden correr los usuarios de la red hacia el exterior

FIREWALL

Todo el tráfico entre dos redes pasa a través del firewall

Desde el punto de vista de la política de seguridad el FIREWALL:

- Delimita el perímetro de defensa y la seguridad de la organización
- Es un punto de comprobación entre una red privada y una o más redes públicas
- Es la única pasarela entre la red que protege y el exterior

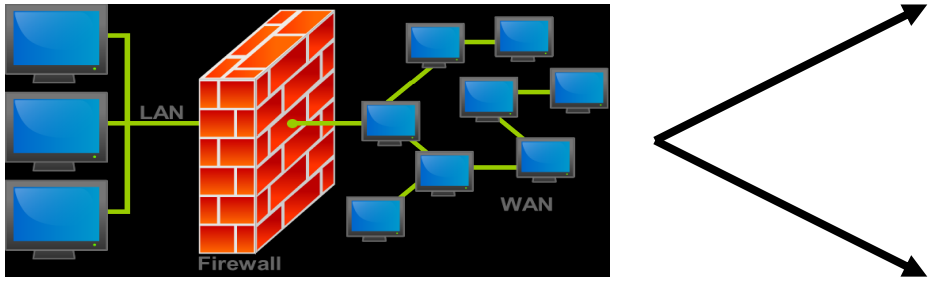
Todo tráfico debe pasar a través del cortafuego y ser filtrado basándose en las reglas, especificadas en la tarjeta de interfaz de red, mediante la cual se accedió al cortafuego

FIREWALL

Los cortafuegos actúan de acuerdo a parámetros introducidos por el diseñador, por lo que aquellos paquetes de información, que no se encuentran dentro de esos parámetros, como una amenaza de peligro, los dejará pasar.

Las limitaciones principales de un FIREWALL son:

- El hueco que no se tapa y es descubierto por un hacker, que puede abrir un hueco diferente y borrar las pruebas o indicios del ataque original.



- No provee de herramientas contra la filtración de software o archivos infestados con virus.

HERRAMIENTAS HACKER

Protocolo *SNMP.* **Usado para examinar la tabla de ruteo que usa la red y conocer su topología.**

Programa TraceRoute. **Revela detalles de la red y los enrutadores.**

Protocolo *Whois.* **Provee datos acerca del servidor de nombres de la red.**

Protocolo *Finger.* **Revela información sobre los usuarios (login, número telefónico, entre otros).**

Programa *Ping.* **Es empleado para localizar un host en particular y al correrlo en diferentes IP construir una lista de host residentes en la red.**

HERRAMIENTAS HACKER

ISS **(Internet Security Scanner) o el *SATAN* (Security Analisys Tool for Auditing Networks).**

Penetran en el dominio de la red y buscan huecos de seguridad.

El administrador de la red puede usar estas herramientas para determinar cuál es el grado de vulnerabilidad de su red y volverla más segura, ya sea cambiando el diseño de firewall o conseguir cómo tapar los huecos del sistema

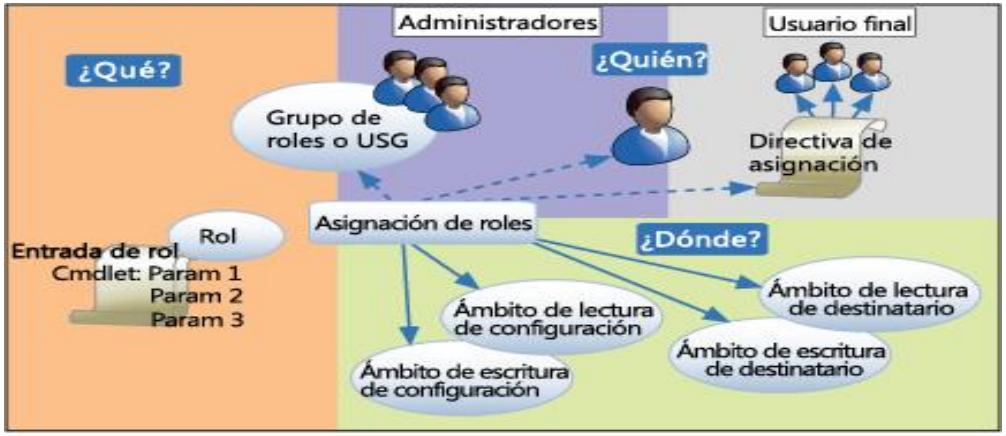
SEGURIDAD BASADA EN EL USUARIO

Utiliza contraseñas y otros controles de acceso para autentificar las identidades de los usuarios antes de permitirles el acceso.

Uno de los esquemas más seguros es el de la *triple A* (AAA), Autenticación, Autorización y Contabilidad

SEGURIDAD BASADA EN EL USUARIO

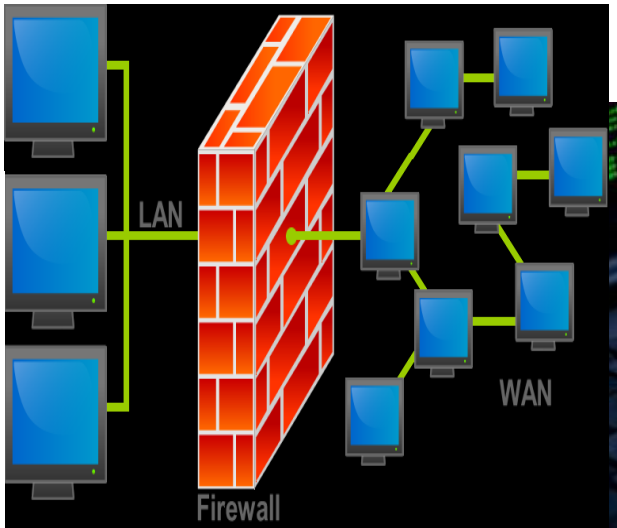
***Autenticación*. Valida la identidad del usuario como auténtica antes de conceder el acceso. *Autorización*. Concede al usuario el privilegio de acceder a las reglas y comandos del sistema. *Contabilidad*. Recopila datos para realizar el seguimiento de los modelos de uso a cada usuario individual.**



Son tres funciones en orden secuencial: primero, se le permite al usuario acceder, segundo, se le otorgan ciertos privilegios cuando esta dentro y tercero, se guarda una historia sobre lo que hace mientras esta dentro.

Los defensores tienen que cerrar todas las puertas. Porque

Los invasores sólo necesitan encontrar* una *abierta.



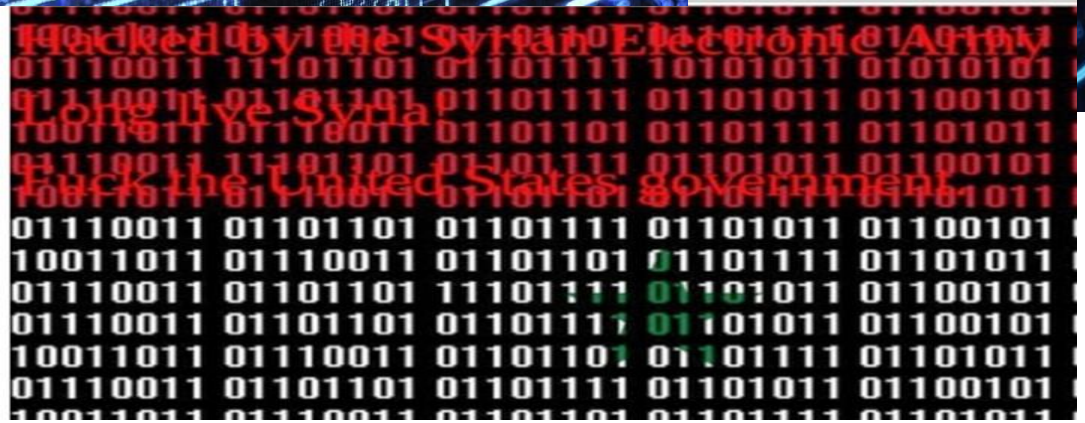
SIMPOSIO 2015

PROSPECTIVAS DEL GOBIERNO ELECTRÓNICO EN VENEZUELA

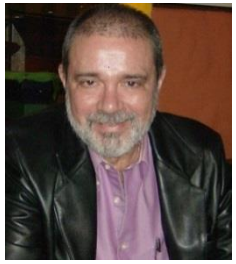
SEGURIDAD DE DATOS ELECTRÓNICOS

UNEFA - Asamblea Nacional, 2 de julio de 2015

MUCHAS GRACIAS



Dr. Sergio Teijero
Profesor e Investigador Asociado
Universidad Central de Venezuela
UNEFA



Dr. Sergio Teijero Páez

Profesor e Investigador Asociado

Conferencista nacional e internacional

Dicta cursos y asesora proyectos y tesis en las áreas de:

Información, Tecnología, Comunicaciones, Automatización, Gestión del Conocimiento, Organizaciones Inteligentes, Redes Sociales, E-Learning, Inteligencia Artificial, Sistemas Expertos, Inteligencia Emocional, Social, Ejecutiva, Creativa, Espiritual, Ecológica y Múltiples Inteligencias para el Aprendizaje

E-mail: steijero@gmail.com / steijero@cantv.net

Teléfono móvil: ***0416-6335561 / 04166720458***