



# Programa de Apoyo Nacional a los más Pobres JUNTOS

Gerencia de Tecnologías de la Información

## Seguridad Perimetral

Lima, Setiembre 2008



## CONTENIDO

1.	ASPECTOS GENERALES DEL PROYECTO .....	2
1.1	OBJETIVOS .....	2
1.2	ANTECEDENTES .....	2
2.	JUSTIFICACION PARA DAR SEGURIDAD A LA RED INSTITUCIONAL.....	3
3.	DISEÑO DEL SERVICIO DE SEGURIDAD PERIMETRAL REQUERIDO .....	6
4.	ALTERNATIVAS DE SOLUCION.....	7
5.	CONCLUSIONES Y RECOMENDACIONES .....	8



## 1. ASPECTOS GENERALES DEL PROYECTO

---

### 1.1 OBJETIVOS

Proveer de una solución de seguridad perimetral integral para la red de datos del Programa JUNTOS, lo que permitirá disponer de un nivel de confianza adecuado ante los riesgos que implican la interconexión de la red de datos del Programa a Internet.

### 1.2 ANTECEDENTES

En la red de datos del Programa JUNTOS se han presentado incidentes de seguridad como los que se citan a continuación:

El 25 de Julio del presente se detectó una inconsistencia en la Página Web Institucional, las 4 últimas noticias que se muestran en la pantalla principal habían sido alteradas.

De acuerdo a la investigación realizada, se encontró que había una deficiencia en la codificación de las consultas en la página de noticias, que permitía la inyección de código SQL por un parámetro enviado a través del método \$\_GET en el URL, y obtener acceso a la información de las tablas de usuarios de la base de datos de la página web, de esa forma se podía obtener la información de los usuarios y las claves del módulo de administración de contenido, de la página web.

Aunque la contraseña de los usuarios está encriptada con codificación md5, es posible que fuera descifrada para así poder ingresar y modificar el contenido de la página Web de Juntos.

Este ataque corresponde a un patrón malicioso, el cual podría haber sido detectado si se hubiera realizado un análisis en tiempo real (a las 3am) del tráfico web.

Otro incidente detectado fue el 15 de agosto, fecha en la cual se detectó que un archivo ejecutable alojado en servidor de aplicaciones de la página web estaba infectado por virus (Salita), lo cual hizo que se cancelara el servicio de página web por 5 horas y se formateara dicho servidor.



## 2. JUSTIFICACION PARA DAR SEGURIDAD A LA RED INSTITUCIONAL

La seguridad en las redes de datos depende directamente de las amenazas a las que estén expuestas, con el acceso a Internet esa posibilidad se incrementa en forma exponencial. El ataque a una red de datos requiere por parte de quien lo realiza de mucho tiempo, conocimiento y paciencia. Curiosamente esas son las mismas características que debe tener quien la defiende, en realidad el perfil del administrador de una red y de un hacker o craker son muy parecidos, solo cambian sus intereses.

El nivel de amenaza en nuestra organización está orientada básicamente a la información con la que contamos de nuestros beneficiarios, y cualquier acceso no autorizado o no detectado para llegar a dicha información puede ser de alto riesgo o tener un alto nivel de impacto en la imagen de la Institución.

Por tanto, es indispensable que nuestra organización establezca mecanismos básicos de control y seguridad para proteger nuestra red de datos y la información que circula por ella.

Por otro lado, está la utilización inadecuada de nuestros servicios de red por parte de usuarios internos, quienes muchas veces saturan el ancho de banda del servicio de Internet para fines ajenos a la actividad laboral o ejecutan aplicaciones potencialmente peligrosas que exponen al resto de los equipos a riesgos imprevisibles.

### **SERVICIOS REQUERIDOS PARA SEGURIDAD PERIMETRAL**

Para que nuestra red de datos cuente con un nivel de seguridad que la proteja de riesgos no deseados, es necesario que se cuente, como mínimo con los servicios siguientes:

#### **1) FIREWALL**

Es el servicio de seguridad más básico y tradicional, hoy en día, este servicio se considera "necesario pero no suficiente" frente a las amenazas y técnicas de ataque de última generación.

Actualmente el programa Juntos **no cuenta** con un equipo firewall apropiado como solución para resguardar la red Institucional.

Parte de las funcionalidades del servicio está alojado en una PC alquilada ya que la PC destinada para tal fin, ha sido dado de baja desde octubre del 2007, y no ha sido repuesto, pese a que esto ha sido solicitado en reiteradas ocasiones.

La solución de Firewall en PC no es la mas recomendable considerando que hay soluciones (equipos) especializados que incluyen hardware y software pero requieren de profesionales muy especializados para la administración y monitoreo durante las 24 horas.

## 2) ANTIVIRUS PERIMETRAL

Consiste en la ubicación de un equipo que sirve como mediador entre dos redes ("gateway"), proveyendo la función de comprobación de virus en los paquetes que circula entre estas redes. En este caso, el servicio de antivirus gateway se refiere a la ubicación de un componente entre la red privada de JUNTOS y la red publica de Internet, para lo cual, analiza el trafico de correo ( smtp, pop), Web (http) y FTP.

El programa actualmente no cuenta con un antivirus perimetral.

## 3) SERVICIO IDP

La tecnología IDP (intrusión detection and prevention) posee las siguientes características principales:

- Detección de ataques y proporcionar alertas para evitarlos.
- Anulación pro-activa en tiempo real de accesos no autorizados.
- Análisis de tráfico a nivel de aplicación para evitar modificaciones no autorizadas.

El programa actualmente no cuenta con una solución IDP.

## 4) DETECCION DE ATAQUES EN TIEMPO REAL

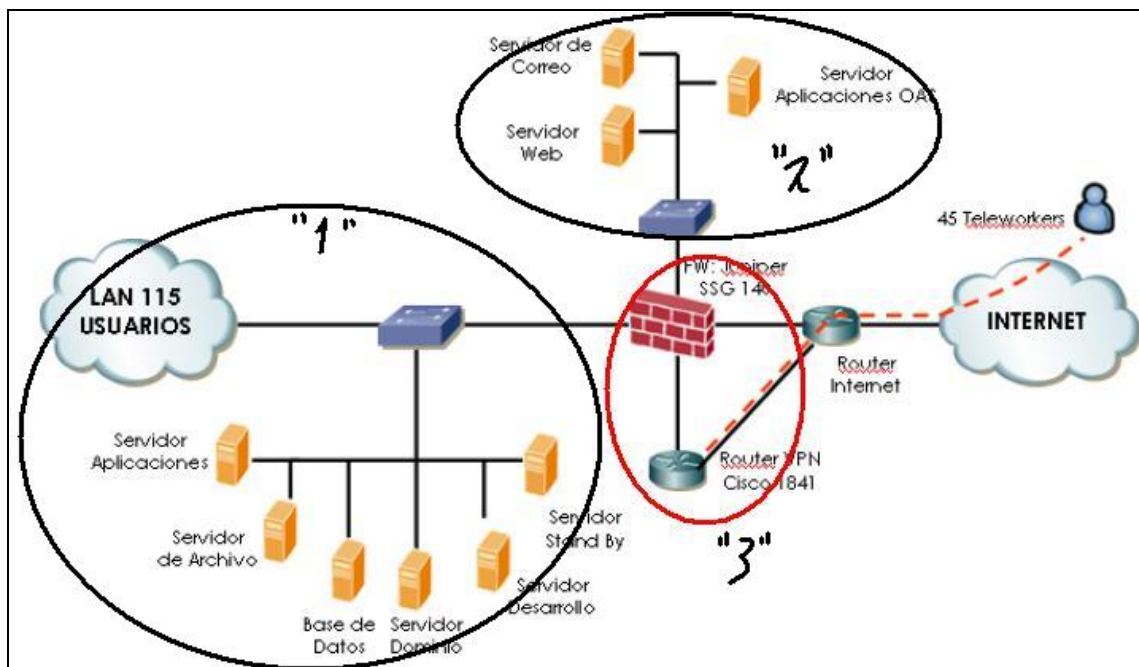
Es una funcionalidad que permite monitoreo en tiempo real los servicios públicos implementados (Internet) por la Institución, proporcionando alarmas que permiten conocer en forma preactiva las amenazas a los servicios indicados, con lo cual se tiene elementos para verificar la gravedad de



la alarma y desarrollar acciones preventivas o correctivas sobre la configuración actual, según sea requerido por la situación.

Considerando la limitada cantidad de recursos con la que se dispone, el programa no cuenta con personal que pueda realizar un monitoreo 24x7 (24 horas los 7 días de la semana) ni se cuenta con herramientas de software para realizarlo.

### 3. DISEÑO DEL SERVICIO DE SEGURIDAD PERIMETRAL REQUERIDO



Donde:

"1" Red Local Interna del programa

"2" Red de servicios públicos del programa

"3" Solución integral para seguridad Perimetral (Firewall, antivirus perimetral, IDP, router-VPN y otros)

#### 4. ALTERNATIVAS DE SOLUCION

- 1) **Alternativa 1:** Solución por adquisición de equipo y administración por personal especialista contratado por Programa JUNTOS. Para un periodo de 5 meses (setiembre a enero 2008) se requiere un total de S/. 151,297, detalle en cuadro siguiente:

Descripción	Cantidad	Costo Unitario	TOTAL S/.
Costo estimado de Firewall	1	61.297	61,297
Administración de los equipos de comunicación y seguridad por personal especialista en seguridad y comunicaciones (para cubrir 3 turnos por 5 meses)	3	6000	90,000
<b>TOTAL S/.</b>			<b>151.297</b>

- 2) **Alternativa 2:** Solución por contratación de servicio de terceros se requiere S/.19.956:

Descripción	Cantidad	Costo Unitario	TOTAL S/.
Costo estimado de Firewall			
Administración de los equipos de comunicación y seguridad por personal especialista en seguridad y comunicaciones (para cubrir 3 turnos por 5 meses)			
<b>Servicios:</b> Instalación, configuración y Puesta en Marcha <b>Gestión 24x7</b> (todos los días las 24 horas) Firewall+IDP Perimetral SSG-140, servicio de Webfilter, servicio de Antivirus Gateway. 45 Teleworkers. <ul style="list-style-type: none"> <li>• Costo al instalar = S/. 5,676</li> <li>• Pago mensual = S/. 3,570</li> </ul>			
<b>TOTAL S/.</b>			<b>19,956</b>



## 5. CONCLUSIONES Y RECOMENDACIONES

---

- 1) La seguridad perimetral de la red de datos es de vital importancia ya que con el acceso a Internet los servicios del programa se ven expuestas a ataques y accesos no autorizados por parte de usuarios externos e internos.
- 2) La información de los beneficiarios es crítica y por tanto es necesario darle todos los niveles de seguridad a fin de resguardarla de accesos no autorizados.
- 3) El programa JUNTOS no cuenta con los recursos necesarios para la implementación de una solución de seguridad perimetral adecuada a los requerimientos de confidencialidad y alta disponibilidad de la información. Tampoco dispone de ambientes adecuados para alojar a los equipos de comunicación y seguridad necesarios, ni el personal que garantice su adecuada administración.
- 4) La terciarización de los servicios de seguridad, surge como la alternativa mas adecuada, dado que existe una amplia oferta de servicios disponibles, los cuales permiten configurar un entorno seguro para el programa durante las 24 horas de todos los días.
- 5) Las empresas que ofrecen servicios en este rubro son altamente especializadas, garantizando un nivel de seguridad adecuado para el Programa.