SEGURIDAD EN LOS ACCESOS A LA INTERNET Y EN EL USO DE REDES INALÁMBRICAS

Ver. 1.4. – Abril de 2009

I. OBJETIVO

Incrementar los niveles de seguridad en la Red Provincial de Transmisión de Datos, asegurando la convivencia de las distintas áreas de gobierno en una sola red, minimizando los riesgos que puedan afectar la integridad, disponibilidad y rendimiento de la red y/o la integridad, confidencialidad y disponibilidad de la información que en ella reside o circula.

II. ALCANCE

La presente Directiva es de aplicación y cumplimiento de todos los Organismos Centralizados y Descentralizados dependientes del Poder Ejecutivo provincial y de todas aquéllas áreas de Estado que participen o planifiquen participar como integrantes de la Red Provincial de Transmisión de Datos.

III. BASE NORMATIVA

- Política Provincial de Informática, Decreto N° 0405/1991.
- Política de Seguridad de la Información para los Organismos de la Administración Pública Provincial. Decreto Nº 2223/2008..
- Ley Orgánica de Ministerios 2571, articulo 24°, funciones de la Secretaria de la Gestión Pública y Contrataciones del Estado (SGPyCE). 2007.

IV. FUNDAMENTACION

La Red Provincial de Transmisión de Datos es un ambiente protegido que cumple con las normas más estrictas de seguridad en lo que respecta a su conexión con la Internet.

Aunque se han tomado medidas rigurosas para asegurar su protección en cuanto a la integridad, confidencialidad y disponibilidad de la información que por ella circula o reside, es extremadamente importante que los usuarios que forman parte de esta red también tomen precauciones para asegurar que su información permanezca segura y protegida y que la Red Provincial de Transmisión de Datos mantenga un desempeño aceptable en cuanto a su rendimiento.

Existen “vulnerabilidades” y riesgos asociado cuando se tiene una computadora conectada directamente a la Internet por un período de tiempo extendido. Esto se aplica a todos los usuarios, pero es de extrema importancia para aquéllos que tienen acceso a la Internet mediante módem, ADSL (“Asimetric Digital Subscriber Line”), cable u otro medio. Estos métodos de conexión no requieren marcar un número telefónico para conectarse a la Internet, por lo cual a veces se los describe como conexiones “siempre activadas”.

Cuando una computadora permanece encendida y conectada a la Internet, queda abierta una ventana de oportunidad para terceros maliciosos de atacar la computadora personal de usuario y a través de ésta, al resto de la Red Provincial, desvirtuando de esta forma todos los esfuerzos por mantener segura la Red Provincial y atentando directamente la convivencia de las distintas áreas de Gobierno en una sola red.

En tal sentido, la Secretaría de Estado de la Gestión Pública y Contrataciones del Estado, en cumplimiento del Decreto Nº 2223/08 que establece la “Política de Seguridad de la Información para los Organismos de la Administración Pública Provincial”, considera necesario la sanción de la presente **Directiva de Seguridad**

destinada a las distintas áreas del Estado que cuenten o planeen contar con conexiones del tipo ADSL, Cable u otro y que a su vez participan o planean participar de la Red Provincial de Transmisión de Datos.

V. DISPOSICIONES GENERALES Y ESPECÍFICAS

1. De las conexiones ADSL, Cable u otros:

   Aquéllos organismos que cuenten con conexiones locales vía módem, ADSL, Cable u otras para acceso a la Internet y que compartan dicha conexión con otros equipos de su red local deberán poseer un equipo que administre dichos accesos con las siguientes características mínimas:

   - Sistema Operativo licenciado con capacidad de recibir actualizaciones del proveedor en línea.
   - Cortafuegos o barrera de seguridad (Firewall) tipo corporativo.
   - Antivirus licenciado con capacidad de recibir actualizaciones del proveedor en línea.
   - Protección contra software malicioso licenciado con capacidad de recibir actualizaciones del proveedor en línea.
   - IDS (Sistema de Detección de Intrusiones).
   - Manejo de usuarios.
   - Manejo de equipos o direcciones IP.
   - Filtro de contenidos.
   - Capacidad de administración remota.

2. De las conexiones inalámbricas:

   Aquéllos organismos que cuenten con equipamiento tipo router inalámbrico o “Access point” para usufructuar las conexiones vía módem, ADSL, Cable u otro para acceso a la Internet o para acceso a su red local deberán cumplir con las siguientes medidas de seguridad adicionales:

   - Instalar el router o AP en el ambiente más alejado de la calle y las ventanas.
   - Muchos routers permiten controlar la intensidad de la señal, en tal caso disminuir la intensidad para restringir la propagación fuera del edificio.
   - Cambiar la contraseña por defecto (de fábrica) del usuario administrador del router inalámbrico y utilizar una de construcción robusta.
   - Cambiar el SSID (Identificación de la red inalámbrica) por defecto (de fábrica) del router inalámbrico y deshabilitar el broadcast del SSID. En lo posible, no se permitirá acceder a su red local a través de su red inalámbrica sino solamente a través de la red cableada conectada a uno de los puertos del router.
   - Utilizar seguridad tipo WPA para establecer la conexión inalámbrica. En caso de no estar disponible, utilizar WEP con una contraseña de 128 bits.

- Habilitar la opción Firewall del router y configurar el rechazo de ping entrante (bloqueo de requerimientos desde la WAN) en la mayoría de los routers, esta opción también oculta los puertos de red con lo que se incrementa la protección contra accesos anónimos desde la Internet.

- Deshabilitar la función de servidor DHCP.

- Las funciones UPnP generalmente vienen deshabilitadas por defecto (valor predeterminado de fábrica) debido a que esto puede representar un riesgo para la seguridad; de no ser necesario verifique que quede deshabilitado.

- Mantener actualizado el firmware del router inalámbrico (cuando las actualizaciones estén disponibles por el fabricante).

- Desconectar el router o deshabilitar la red inalámbrica cuando no se utilice.

3. De los equipos que participen y/o usufructúen las conexiones vía módem, ADSL o Cable:

   Aquéllos equipos independientes que posean una conexión vía módem, ADSL, Cable u otro, o aquéllos equipos que formen parte de una red local y que usufructúan una conexión como la descripta en el punto 1 y que por otra parte integran o está planeado que integren la Red Provincial de Transmisión de Datos deberán cumplir con las siguientes características mínimas:

   - Sistema Operativo licenciado con capacidad de recibir actualizaciones del proveedor en línea.

   - Cortafuegos o barrera de seguridad (Firewall) tipo personal.

   - Antivirus licenciado con capacidad de recibir actualizaciones del proveedor en línea.

   - Protección contra software malicioso licenciado con capacidad de recibir actualizaciones de proveedor en línea.

4. Generales:

   Se establece un plazó máximo de 180 días para el cumplimiento de la presente directiva, transcurridos los cuales, la SEGPyCE podrá disponer de inspecciones y de constatar el no cumplimiento de la misma podrá proceder a desconectar de la Red Provincial de Transmisión de Datos al área donde se constate el incumplimiento.

   Queda excluido el uso de antivirus en sus versiones “free” para lo cual deberán ser bloqueados los accesos a los sitios oficiales de descarga.

   Toda área de gobierno que posea un acceso a la Internet vía módem, ADSL o Cable y/o que posean equipamiento de red inalámbrica (router o Access point) deberá estar cubierta o asistida por un área de Tecnología de la Información (TICs) propia o de otra área de gobierno.

   Los equipos que participen de la Red Provincial y/o del usufructo de conexiones a la Internet vía módem, ADSL o Cable deberán mantener “Vigencia Tecnológica” en cuanto a la versión del Sistema Operativo y los programas de protección contra software malicioso.