



FILTRO DE CONTENIDOS DE INTERNET
MANUAL DE USUARIO

1. INTRODUCCIÓN

Este manual de usuario contiene toda la información necesaria para acceder al servicio de Filtro de Contenidos de Internet, un servicio innovador que garantiza una navegación segura.

Inicialmente se describirá la funcionalidad del servicio, para que usted pueda disfrutar del mismo con plenas garantías.

En el caso que esto no resuelva sus dudas o inquietudes, puede llamar a nuestro Centro de Atención al Cliente al teléfono fijo 702-1901 o entrar al sitio Web de la RCP (www.rcp.net.pe), Atención al cliente y llenar el formulario, donde le daremos una pronta respuesta a sus preguntas.

2. ¿QUÉ ES EL FILTRO DE CONTENIDOS DE INTERNET?

El Filtro de Contenidos de Internet es un servicio que utiliza tecnología proporcionada por Symantec, que es capaz de filtrar el acceso a Internet y las comunicaciones vía red IP orientado a usuarios que disponen de acceso ADSL basado en la infraestructura de Banda Ancha de Telefónica así como a los usuarios de Dial Up de cualquier ISP del mercado.

EL software utilizado es un servidor Proxy cuya función es proteger su red de virus y contenido inapropiado revisando el tráfico HTTP, HTTPS y FTP.

El servicio permite restringir el acceso a contenidos según una serie de categorías definidas que aseguran en el hogar una navegación segura y controlada desde las PC's asociados al servicio.

Al tratarse de una aplicación cliente servidor no requiere instalación en PC de cliente, facilitando así tanto las actualizaciones que requiera el servicio como su portabilidad.

3. ¿CÓMO SE BRINDA PROTECCIÓN?

3.1. Protección Antivirus:

El filtro de contenidos de Internet protege su red contra ataques del virus explorando todo el tráfico del HTTP y del FTP que pase de su browser a través de su cortafuego para los virus. Si se detecta un virus, el filtro de contenidos de Internet niega el acceso al sitio Web infectado.

La operación es transparente para el usuario.

3.2. Filtrado de Contenido:

- Listas de Filtrado (URLs): se usan listas de URLs para permitir o denegar el acceso a un sitio Web de acuerdo a las políticas establecidas por la empresa.

Estas listas de filtros URL nos permite filtrar los sitios Web mundiales en todo el sistema, en grupos, o en forma individual, utilizando categorías predefinidas, como por ejemplo, sexo, juegos de apuesta o intolerancia. Estas listas son actualizadas automáticamente de manera diaria.

Las principales categorías son las siguientes:

- Crime
- Drugs/Advocacy
- Drugs/Non-medical
- Gambling
- Intolerance
- Occult/New Age
- Sex/Acts
- Sex/Attire
- Sex/Nudity
- Sex/Personals
- Violence
- Weapons

Si el usuario intenta entrar a algún sitio Web que esté incluido en la lista de prohibidos, aparecerá el siguiente mensaje:



• Revisión Dinámica de Documentos (DDR)

1. Comparación de cada una de las palabras de una página Web contra diccionarios incluidos en el Symantec Web Security
2. Diccionario Multilingüe en 14 idiomas

La tecnología DDR va más allá de la simple búsqueda de palabras clave, ya que analiza relaciones de palabras sensibles al contexto. Funciona en tiempo real determinando al vuelo y con precisión la necesidad de bloquear un contenido de Web inapropiado, incluso si dicho contenido todavía no ha sido incluido en una lista de filtros. La tecnología DDR detecta y bloquea eficazmente nuevos sitios o sitios de acceso reciente, sitios anteriormente aceptados que han modificado su contenido, así como sitios bloqueados que contienen nuevos nombres de dominio.

Para determinar si el sistema va a bloquear o permitir el acceso a un sitio Web, el filtro de contenidos de Internet compara el texto en el sitio solicitado a los diccionarios predefinidos de DDR que contienen

palabras en idiomas múltiples. Cada ocurrencia de una palabra contenida en un diccionario activo recibe una puntuación. Si la puntuación total excede el nivel permitido, el acceso al sitio se bloquea.

El mensaje que aparecerá será el siguiente:



Acceso Denegado

El documento solicitado, <http://www.google.com.pe/search?q=sexo&hl=es&meta=>, no será mostrado.

Reason: **DDR score = 114**. This page will not be displayed because it contains prohibited words or it has exceeded its tolerance of questionable words.

4. ¿CÓMO SE ACCEDE AL FILTRO DE CONTENIDOS?

Para configurar el Proxy con Internet Explorer 5.01 o Superior, se debe realizar lo siguiente:

- Inicio: Panel de Control → Configuración → Opciones de Internet
- Elegir la pestaña Conexiones
- Ahora dependiendo si estamos conectados por MODEM o por TARJETA DE RED

4.1. Si es vía MODEM:

1. Seleccionar la Configuración de acceso telefónico que usa para conectarse a Internet. (Figura 1)
2. Hacer clic en el botón Configuración
3. Marcar la casilla Utilizar un servidor Proxy para esta conexión.
4. Típear en el recuadro Dirección: <http://websecure.rcp.net.pe> (IP Servidor Symantec Web Security asignado) y típear en el recuadro Puerto: 8002 (Puerto administración Symantec Web Security) (Figura 2)
5. Hacer clic en el botón Opciones Avanzadas
6. Quitar el Check de la casilla Usar el mismo Servidor Proxy para todos los protocolos.
7. Borrar el contenido de los recuadros Dirección IP y Protocolo del Servicio Gopher (Figura 3).
8. Pulsar el botón Aceptar
9. Pulsar el botón Aceptar
10. Pulsar el botón Aceptar

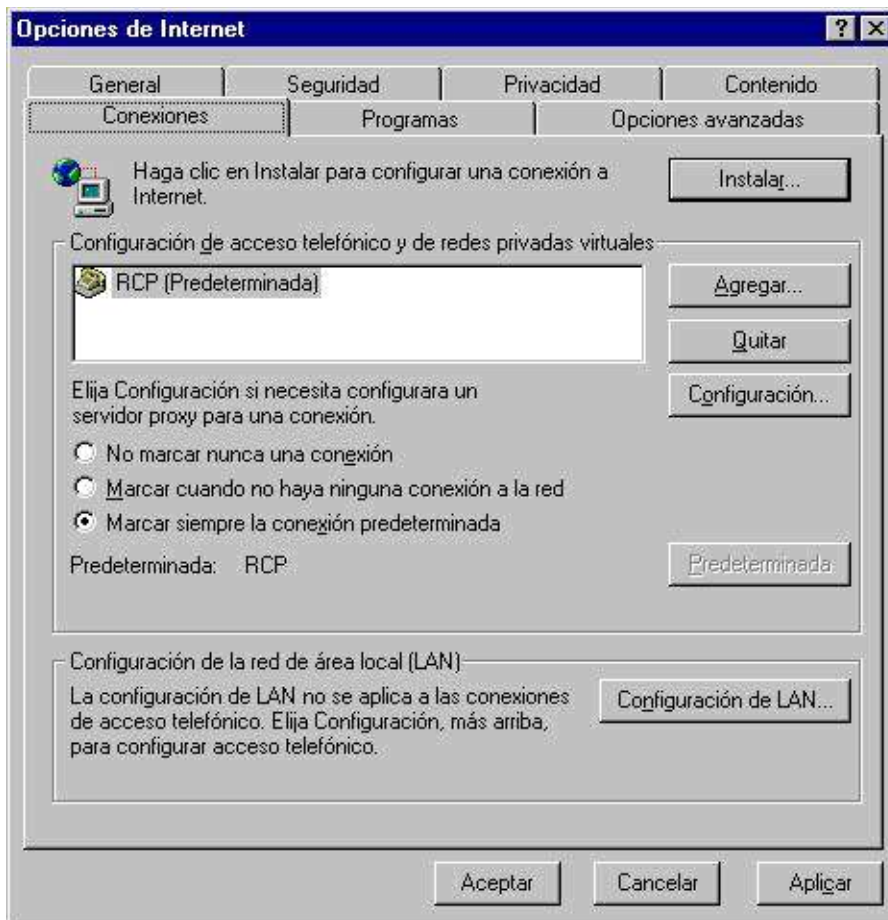


Figura 1: Conexión por MODEM

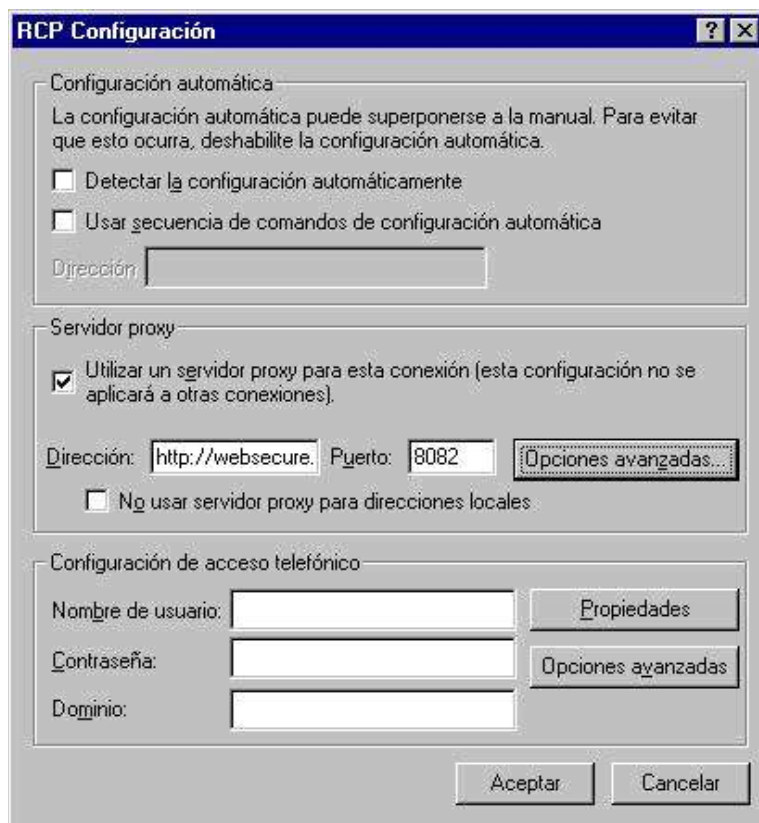


Figura 2: Servidor Proxy _Módem

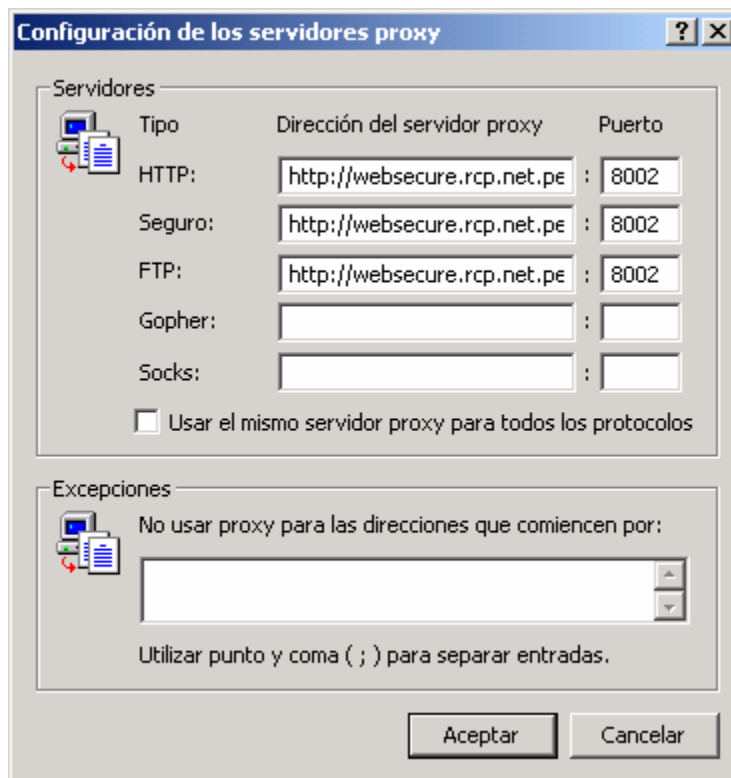


Figura 3: Configuración Servidores Proxy

4.2. Si es vía Tarjeta de RED

1. Hacer Clic en el botón Configuración de LAN (Ver Figura 1)
2. Marcar la casilla Utilizar un servidor Proxy para su LAN
3. Típear en el recuadro Dirección: http://websecure.rcp.net.pe (IP Servidor Symantec Web Security asignado) y típear en el recuadro Puerto: 8002 (Puerto administración Symantec Web Security) (Ver Figura 4 y Figura 5)
4. Hacer clic en el botón Opciones Avanzadas
5. Quitar el Check de la casilla Usar el mismo Servidor Proxy para todos los protocolos.
6. Borrar el contenido de los recuadros Dirección IP y Protocolo del Servicio Gopher (Ver Figura 3).
7. Pulsar el botón Aceptar
8. Pulsar el botón Aceptar
9. Pulsar el botón Aceptar

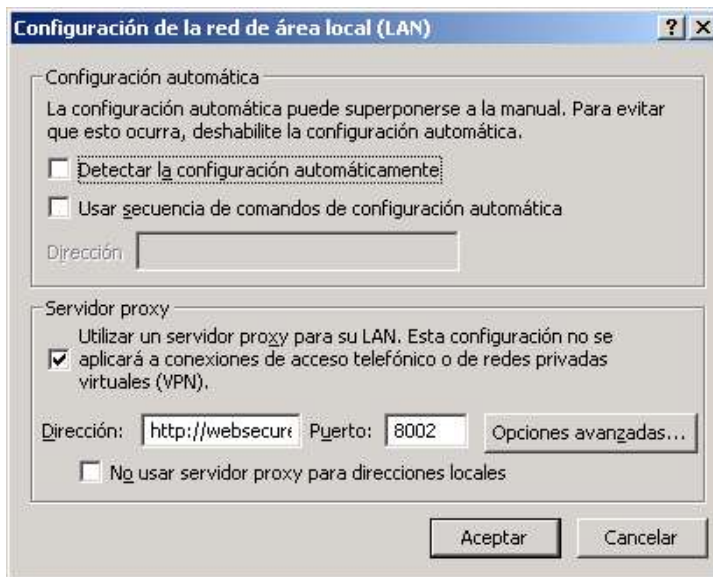


Figura 4 – Servidor Proxy LAN



Figura 5: Servidor Proxy LAN

NOTA 1:

Para evitar que estas opciones de configuración en el Internet Explorer sean modificadas y evitar que se pueda tener un acceso sin restricciones de navegación debe hacerse modificaciones a nivel del Regedit.

Es importante mencionar que solo se recomienda utilizar esta herramienta si el usuario es experimentado ya que si no lo es, podría ser riesgoso para la configuración del Windows.

Esta opción deberá ser configurada por el responsable de la cuenta, en los perfiles que considere necesarios. Solo Windows 2000, Windows NT y Windows XP (en sus diferentes versiones) permiten tener diferentes perfiles a los cuales se ingresan con contraseña.

A continuación se explica el proceso:

1. Inicio → Ejecutar
2. En el recuadro *Abrir* tipear REGEDIT
3. En el árbol mostrado en el lado izquierdo expandir HKEY_CURRENT_USER
4. Expandir SOFTWARE → POLICIES → MICROSOFT
5. Crear una nueva CLAVE con el nombre *Internet Explorer*
6. Estando sobre esta última crear una nueva CLAVE con el nombre *Control Panel* (Ver figura 6)
7. Dentro de *Control Panel* creamos un nuevo valor DWORD de nombre *Connections Tab* y a este le asignamos un valor de 1 (para poder volver a ver las opciones de configuración de *Conexiones de Internet Explorer* volver este valor a 0) (Ver figura 7)
8. Cerrar la ventana de Regedit

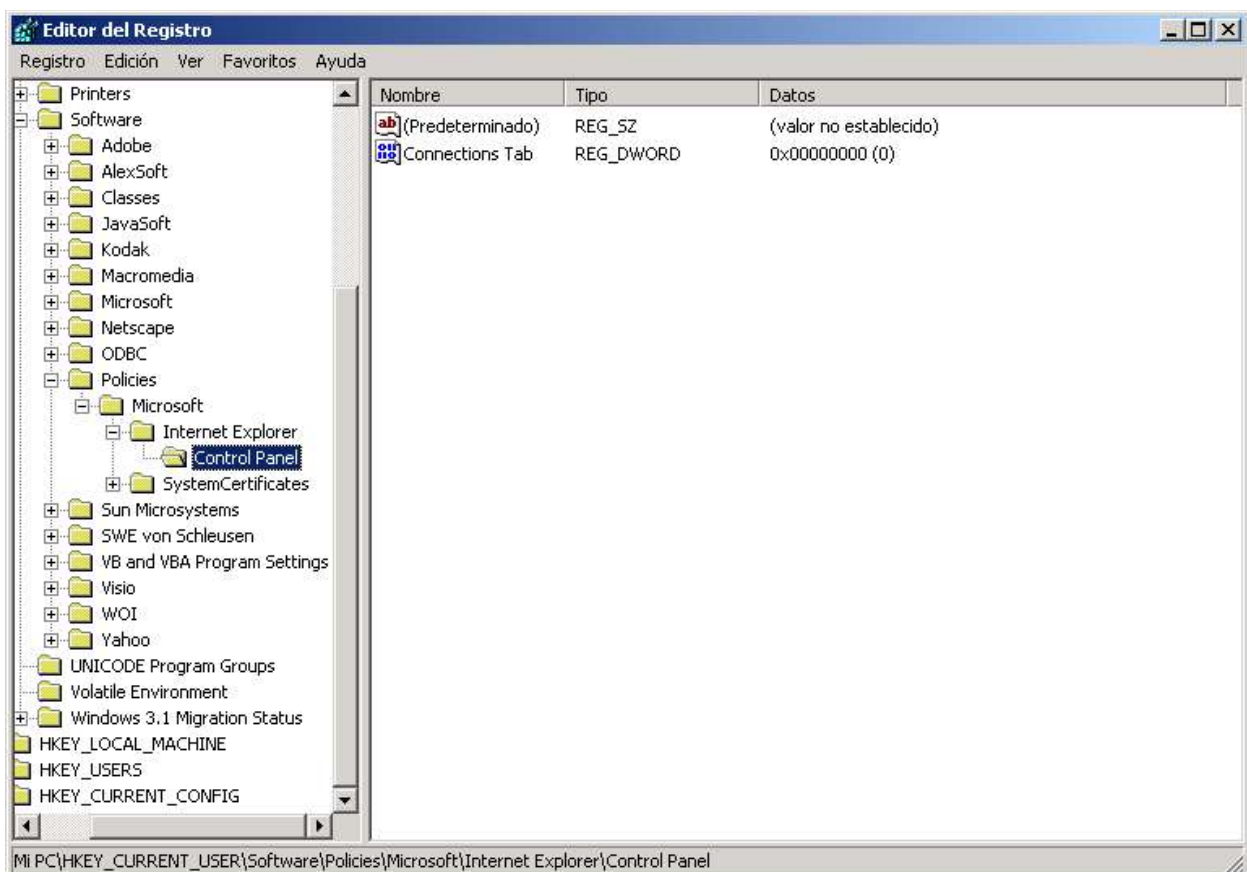


Figura 6 – Creación de nueva entrada en el REGEDIT

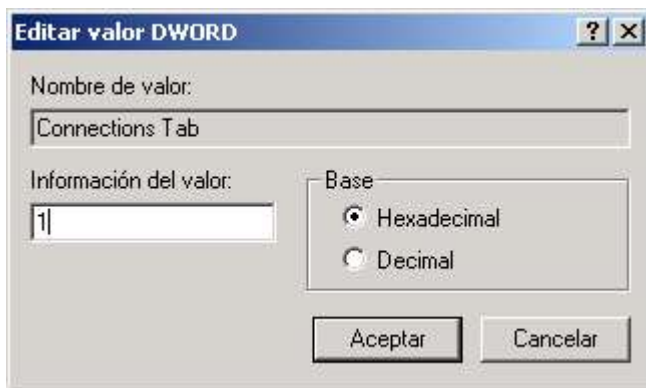


Figura 7 – Agregar el DWORD “Connections Tab” con valor 1

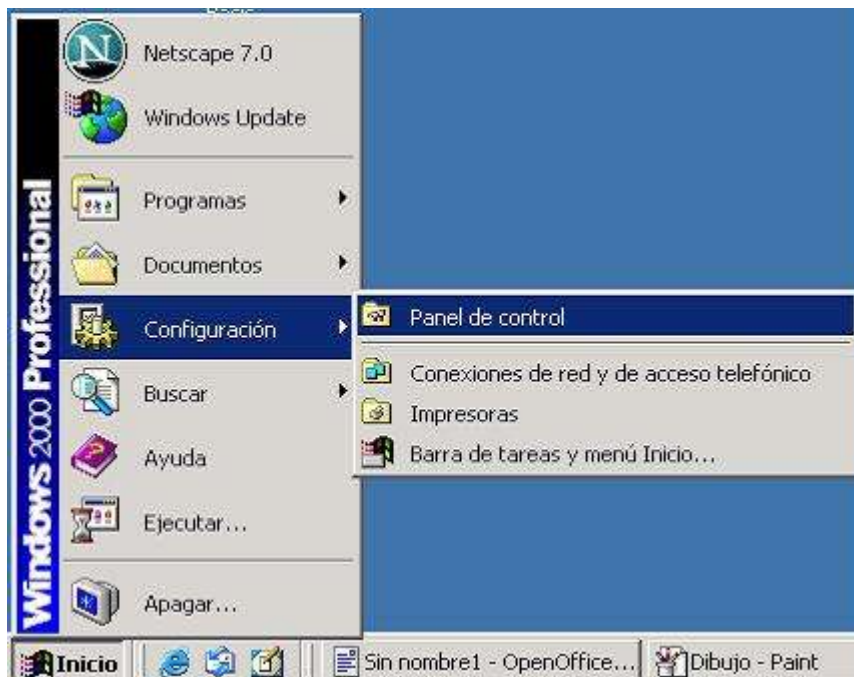
OBS:

1. No se olvide de contraer cada uno de los ramos del árbol que se expandieron y hacer clic finalmente en MI PC de esta manera nos aseguramos que no puedan seguirle el rastro de los cambios que hizo.
2. Este procedimientos fue probado sobre Windows 98, Me, 2000 Server y Professional y sobre Windows XP Professional.

NOTA 2:

Cómo configurar perfiles:

1. Inicio → Configuración → Panel de Control → Usuarios y contraseñas



2. Le aparecerá una ventana como ésta busque la opción **Usuarios y contraseña**.

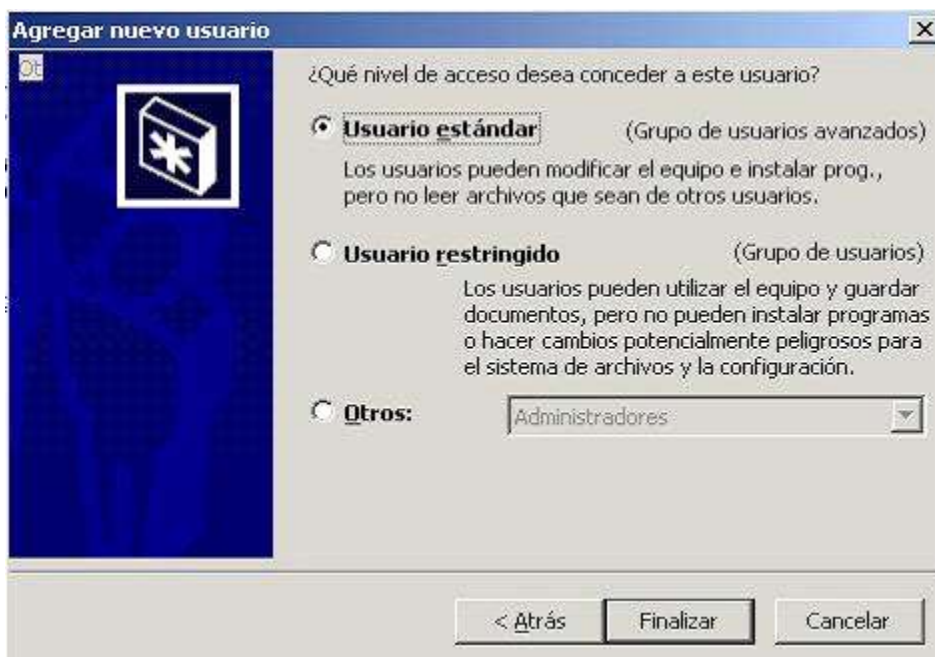


3. Luego de hacer clic, le aparecerá una ventana como ésta, haga clic en Agregar.





4. Haga clic en *Siguiente*



5. Haga clic en *Finalizar*.

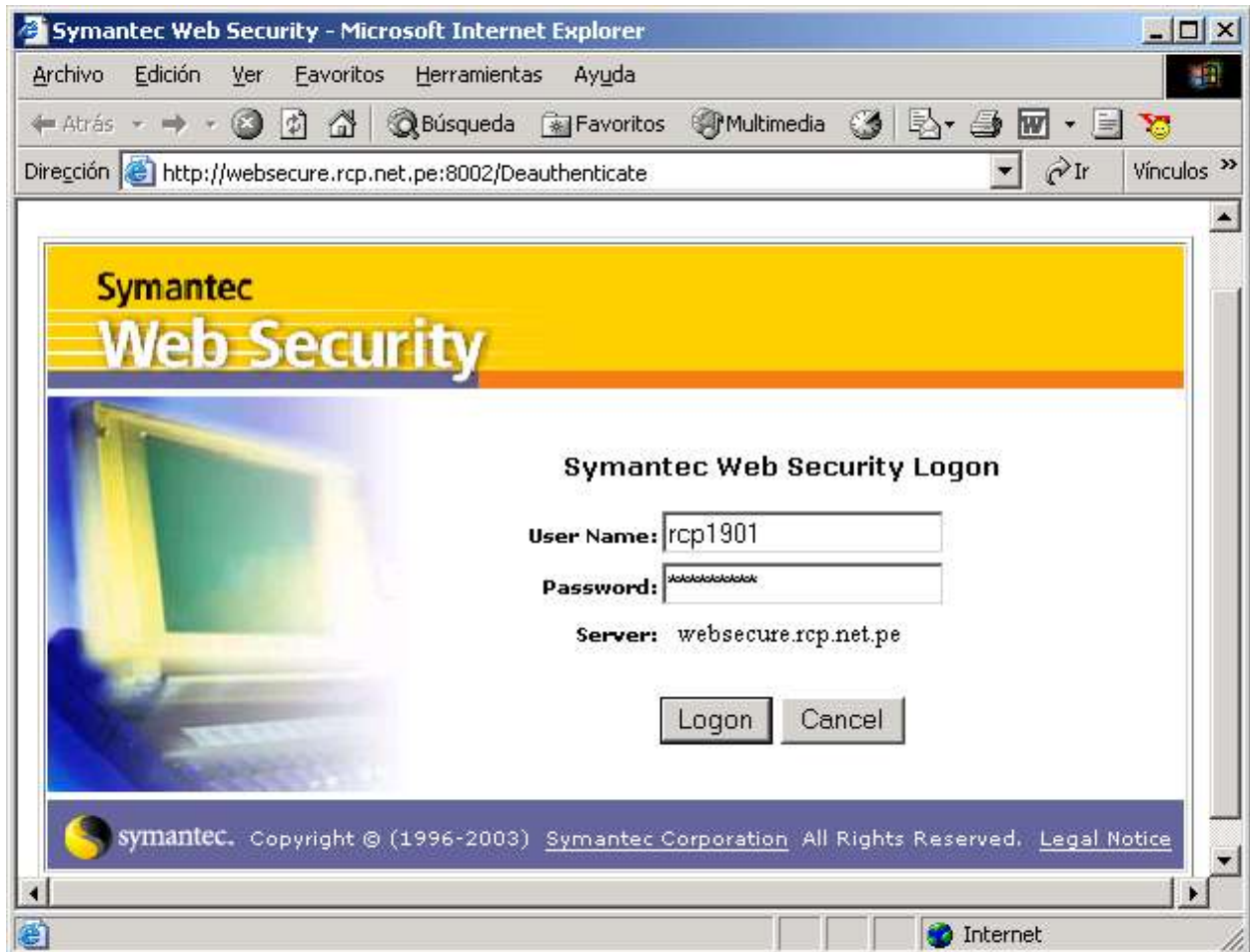
6. Para poder cambiar de sesión solo tiene que presionar las teclas Control + Alt + Supr.

Elija la opción *Cerrar la sesión*.

Ingrese con la nueva sesión después de pulsar Ctrl + Alt + Supr e ingresar el nuevo usuario creado. Aquí es donde tendrá que configurar el filtro.

NOTA 3:

Para verificar la correcta configuración del mismo, deberá abrir el navegador y empezar a acceder a la navegación vía un usuario y contraseña.



Es necesario dar Logout para evitar que una sesión que permanece activa interfiera en el correcto funcionamiento del servicio de filtrado.

Cuando el usuario ingrese a Internet, le aparecerá una ventana Web Security Button Bar donde tendrá que dar Logout al momento de terminar una sesión ya que si no lo hace se quedará "logeado" durante 60 minutos (después de ese tiempo el usuario se deshabilitará automáticamente) y no podrá acceder desde otra máquina (para las personas que utilizan el filtro en diferentes máquinas).

