Rentas
Dirección General de Rentas
Provincia de Misiones

Recomendaciones de Seguridad

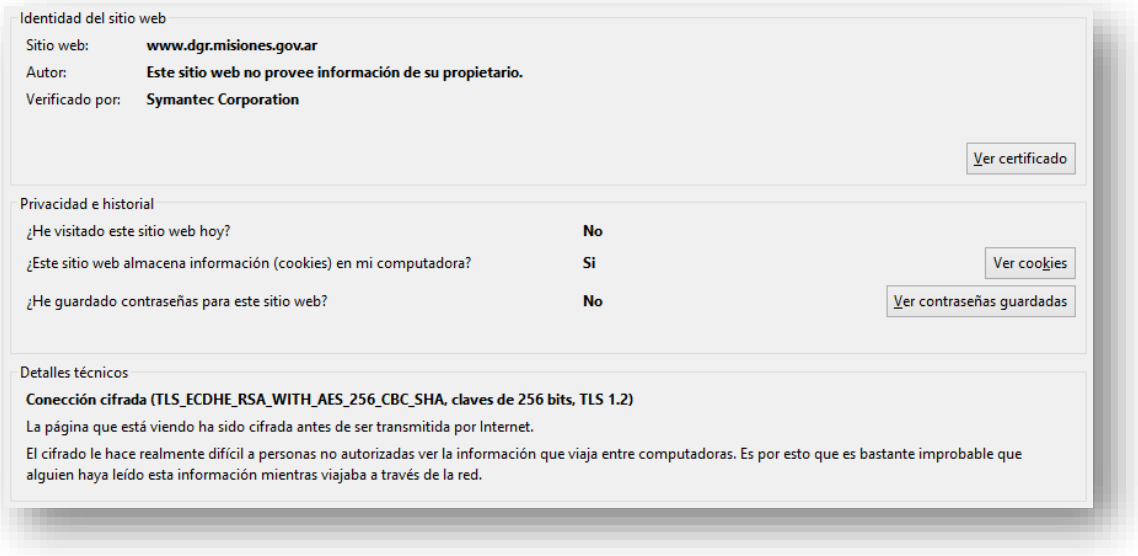
Con motivo de aumentar el nivel de protección y prevenir ante la probabilidad de algún tipo de incidente, la educación del usuario logrará que este se exponga menos a las amenazas existentes y así evitar ser víctimas de virus, fraudes, hackers, malwares y otras amenazas de la red.

Proteja sus datos:

- **Evita el uso del sitio de Rentas en lugares públicos (Cyber cafés, locutorios, etc)**
  Esto evitará que alguien pueda copiar tu información desde el equipo que utilizó.

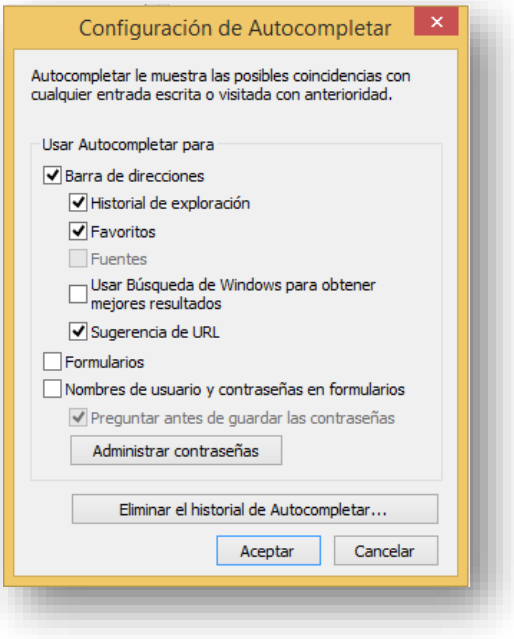
- **No divulgues tus datos personales a terceros.**

- **Visualiza el candado cerrado en la parte superior del Navegador.**
  Haciendo clic en el candado podrás comprobar la vigencia/validez del Certificado Digital y el tipo de encriptación.

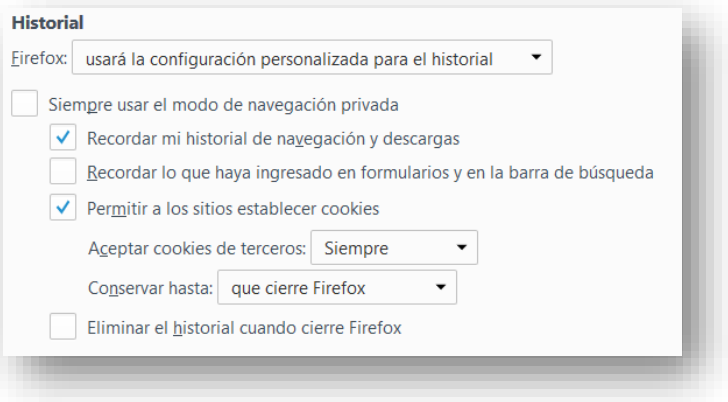


- **Compruebe el acceso a sitios seguros**
  Cuando la comunicación se realiza en un entorno seguro la dirección de Internet (URL) de la página es " https", en vez de "http". La dirección de Rentas es *https://www.dgr.misiones.gov.ar/*

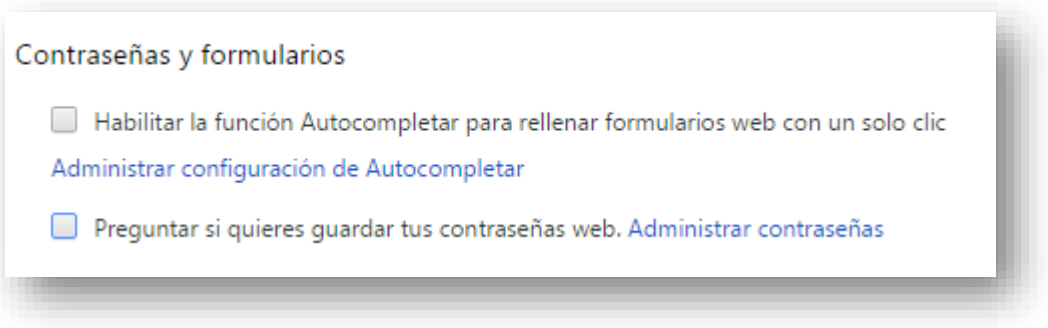
- **Deshabilite la función de Auto completado**
  Puede acceder a esta opción ingresando en:
  - Explorer: Herramientas > Opciones de Internet > Contenido > "Autocompletar". Configuración recomendada:



  - Mozilla: Herramientas > Opciones > Privacidad. Configuración recomendada:



- Chrome: Configuración > Contraseñas y formularios. Configuración recomendada:



➢ **Cierre su sesión al finalizar.**

Proteja su computadora:

Tenga en cuenta las siguientes herramientas y prácticas para protegerla de virus y gusanos informáticos:

- **Utilizar tecnologías de seguridad**
  Las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante la principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

- **Actualizar el sistema operativo y aplicaciones**
  El usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

- **Descargar aplicaciones desde sitios web oficiales**
  Muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema. Por eso, es recomendable que al momento de descargar aplicaciones lo haga siempre desde las páginas web oficiales.

- **Actualización de Contenidos**
  Con el fin de que la información que se despliega en el sitio se encuentre siempre actualizada, comprobá que tu navegador esté configurado de la siguiente manera:
  - Explorer: Herramientas > Opciones de Internet > General > Archivos temporales de Internet > Configuración > seleccione "Cada vez que se visite la página".

- Mozilla Firefox: Herramientas > Opciones > solapa Privacidad > Datos Privados, seleccionar Opciones, seleccionar datos que se desean borrar (entre ellos Caché).

- **Evitar los enlaces sospechosos**
  Uno de los medios más utilizados para direccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Los enlaces pueden estar presentes en un correo electrónico , una ventana de chat o un mensaje en una red social: la clave está en analizar si son ofrecidos en alguna situación sospechosa (una invitación a ver una foto en un idioma distinto al propio, por ejemplo), provienen de un remitente desconocido o remiten a un sitio web poco confiable.

- **No acceder a sitios web de dudosa reputación**
  A través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario – como descuentos en la compra de productos (o incluso ofrecimientos gratuitos), primicias o materiales exclusivos de noticias de actualidad, material multimedia, etc. Es recomendable para una navegación segura que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características.

- **Aceptar sólo contactos conocidos**
  Tanto en los clientes de mensajería instantánea como en redes sociales, es recomendable aceptar e interactuar sólo con contactos conocidos. De esta manera se evita acceder a los perfiles creados por los atacantes para comunicarse con las víctimas y exponerlas a diversas amenazas como malware, phishing, cyberbullying u otras.

- **Evitar la ejecución de archivos sospechosos**
  La propagación de malware suele realizarse a través de archivos ejecutables. Es recomendable evitar la ejecución de archivos a menos que se conozca la seguridad del mismo y su procedencia sea confiable (tanto si proviene de un contacto en la mensajería instantánea, un correo electrónico o un sitio web). Cuando se descargan archivos de redes P2P, se sugiere analizarlos de modo previo a su ejecución con un una solución de seguridad.

Proteja su clave y usuario:

- Cambie su clave de acceso con frecuencia.

- Utilizar contraseñas fuertes: muchos servicios en Internet están protegidos con una clave de acceso, de forma de resguardar la privacidad de la información. Si esta contraseña fuera sencilla o común (muy utilizada entre los usuarios) un atacante podría adivinarla y por lo tanto acceder indebidamente como si fuera el usuario verdadero. Por este motivo se recomienda la utilización de contraseñas fuertes, con distintos tipos de caracteres y una longitud de al menos 8 caracteres.

- No divulgues ni compartas tu clave y usuario con nadie y bajo ninguna circunstancia.

- No utilices información personal en tu clave tal como: nombre, apodo, nombres de familiares o mascotas, tampoco teléfonos o direcciones.

- Su clave debe ser fáciles de recordar pero difíciles de suponer.

Rentas
Dirección General de Rentas
Provincia de Misiones

- No guardes tu clave y usuario, ni los anotes.
- Utiliza usuarios y claves únicas y no las repitas para otros servicios.
- No utilices para tus operaciones online las mismas claves que utilizas para operar en otros servicios de Internet, tales como e-mail, newsletters, portales y otros.

Ante cualquier consulta, comunícate con la Mesa de Ayuda Especializada de lunes a viernes de 06:45 a 18:00 hs. al 0810-444-5505 o por e-mail a mesadeayuda@rafsa.com.ar