



RECOMENDACIONES PARA LA INSTALACIÓN Y DE SEGURIDAD

Este documento contiene una serie de recomendaciones para la instalación y de seguridad en el uso e instalación del software. La primera parte contempla todo lo relacionado con la adecuada elección de un servidor web para instalar el software y la segunda, recomendaciones para hacer un uso seguro de la herramienta.

1-. Recomendaciones para la instalación

Una vez se haya decidido utilizar el software Internet para Rendición de Cuentas (<http://www.iprc.org.co>) requerirá un proveedor de servicios de Internet (ISP por sus siglas en inglés) con el fin de garantizar la disponibilidad del sitio las 24 horas del día siete días a la semana. Esta opción es la más recomendada ya que el proveedor se encarga de los detalles técnicos, lo que le permite concentrarse en el desarrollo del contenido del sitio.

El servidor web también puede ser una computadora ubicada en la entidad. Esto depende de las condiciones de conexión y de equipos con que cuente su organización. En algunos casos las organizaciones poseen una infraestructura adecuada de servidores, capacidad del personal para mantener el sistema en funcionamiento y una conexión dedicada a Internet de manera que no se presenta inconveniente en alojar los sitios web en sus propios servidores.

Para las entidades que hasta ahora empiezan a modernizar su infraestructura de comunicaciones, o que aún no hayan previsto contar con este tipo de infraestructura, puede ser mejor la opción de un ISP.

Se debe tener en cuenta que con un ISP no se tendrá que incurrir en gastos de hardware o software, ni tampoco en los gastos de personal calificado que administre el sitio, aunque podrá tener un asesor que le ayude con el mantenimiento necesario.

El costo de su conexión a Internet ser probablemente mucho menor con un proveedor externo, ya que no requerir de una conexión dedicada (conexión a Internet las 24 horas) y de un gran ancho de banda en su entidad.

Si se decide por un ISP tenga en cuenta que debe permitir instalar y configurar las siguientes aplicaciones requeridas por las Aplicaciones de Acción de APC (<http://www.apc.org/actionapps>), software con que trabaja el sistema:

- **Servidor Web Apache 2.0** o superior.
- **Php 4.3** o superior.



➤ **MySQL 4.1 o superior.**

A la hora de seleccionar un ISP pregunte por las características del servicio:

- ¿Qué ancho de banda ofrece? ¿Hay límite en su uso?
- ¿Qué capacidad en disco ofrece?
- ¿Ofrece soporte técnico?, ¿es personalizado? ¿En que horario?
- ¿Cuál es la disponibilidad del servicio?
- ¿Cuál es la política de copias de respaldo? ¿Cómo se restablecen las copias de respaldo?
- ¿Ofrece estadísticas de acceso?
- ¿Ofrece servidor seguro?

Es importante que su ISP esté conectado al NAP Colombia (www.nap.com.co) para garantizar que los visitantes del país sean quienes accedan más rápido al sitio ya que las conexiones no tienen que realizarse al extranjero. Igualmente tener un ISP en Colombia garantiza que Usted tenga una persona con quien hablar y saber qué sucede con la página si ésta deja de funcionar. Muchos ISP en Internet están tan automatizados que el apoyo humano se ofrece como último recurso y en oportunidades puede tomar mucho tiempo.

2.- Recomendaciones para hacer un uso seguro de la herramienta

Recuerde que la principal ventaja de utilizar este software es la posibilidad de editar los contenidos directamente desde cualquier navegador conectado a internet, de ahí la importancia de hacer un uso seguro de sus contraseñas de acceso. A continuación algunas recomendaciones tanto para administradores como para usuarios finales de la herramienta:

Recomendaciones para administradores en el momento de crear contraseñas:

- Evite el uso de claves obvias como repetir el mismo nombre de usuario como contraseña, por ejemplo:

Usuario: dmartinez

Clave: dmartinez

- Una buena clave reúne combinación de mayúsculas, minúsculas, números y símbolos. Además, es aconsejable que los números y/o símbolos aparezcan en medio de la clave, y no al principio o final.
- Nunca utilice su nombre ni letras de su nombre o de su organización en su clave.
- No utilice una palabra o nombre como clave (p.e. Cartagena, salud, vivienda, etc).
- Una buena clave puede basarse en una frase fácil de recordar, por ejemplo: "La



vaca que rie vía melgar - 9" corresponde a la clave LvqrvM-9. *NO utilice este ejemplo como clave*

Recomendaciones para usuarios del software:

- Su clave debe conocerla solamente Usted.
- No envíe su contraseña o nombre de usuario por correo electrónico. Trate de memorizarla, utilizando el ejemplo de la frase arriba descrito.

3-. Copias de seguridad

Para efectuar la copia de seguridad de su sitio ingrese a una herramienta como phpmyadmin y sitúese en la tabla que contiene las bases de datos en MySQL, por ejemplo, si la tabla se llama **aa-organizacion**, desde allí seleccione exportar y luego las opciones “estructura y datos” y “enviar”, luego pulse continuar:

Seleccione la ruta donde desea colocar el archivo **.SQL**. **Este archivo será la copia de su base de datos** tanto de la estructura como de los datos incluidos en el sistema. Si tiene acceso a la línea de comandos de su servidor utilice el comando mysqldump desde la línea de comandos:

```
mysqldump –h servidor.base.datos.gov.co –u usuario.base.datos base_de_datos > salida.sql
```

Para la copia de la carpeta de archivos del sistema sitúese en el directorio de su servidor web y cree una copia completa (o archivo comprimido) de la carpeta **apc-aa-organizacion**

Para Linux, (p.e. /var/www/html/) y cree un archivo comprimido con extensión tar.gz de la siguiente forma:

```
tar -zcvf apc-aa-organizacion.tar.gz apc-aa-organizacion/
```

Para Windows utilice una herramienta como Winzip (www.winzip.com).

Repita el proceso con el directorio **apc-aa-files-organizacions** para copiar todos los archivos asociados a los canales de las Aplicaciones de Acción de APC en el sistema.

De esta manera ya habrá realizado una copia de seguridad (backup) de las Aplicaciones de Acción de APC y de los datos que residen en el servidor.

Para recuperar una copia de seguridad siga las instrucciones del manual de instalación.



Es importante que las copias de seguridad se realicen de manera diaria e igualmente que se tengan copias semanales incrementales con al menos dos meses de periodicidad. Esto permitirá regresar a copias anteriores en caso de requerirse regresar en el tiempo. Igualmente se recomienda realizar una copia permanente una vez se haya rendido la cuenta por parte de las entidades sujetos de control.

4-. Protección antivirus

A través del sistema la única manera posible de propagar virus es a través de los archivos que se publican en el sitio.

Para evitar problemas con virus publique toda la información en el sitio en formato PDF. Consulte el manual de Autor y Editor para la instalación y uso de herramientas para generación de este tipo de archivos.

Si definitivamente requiere la publicación de archivos en formatos que son posibles portadores de virus utilice un antivirus actualizado para revisarlos antes de su publicación.

5-. Protección contra Hackers

Si su entidad administra su propio servidor en donde se encuentra alojado el sistema es importante que revise periódicamente las alertas de seguridad de los programas que utiliza el software y otros que pueden comprometer la seguridad del sitio:

- Aplicaciones de Acción de Apc: <http://ww.actionapps.org>
- Apache: <http://httpd.apache.org/>
- MySQL: <http://www.mysql.com>
- Php: <http://www.php.net>

Existen herramientas que pueden ayudarle a detectar fallas de seguridad en su sistema como por ejemplo Nessus (www.nessus.org).

Igualmente revise la configuración de sus dominios virtuales en Apache y restrinja la ejecución de *scripts* en php al usuario Apache con la opción *php_flag engine off* en el directorio donde se publican los archivos del sitio **apc-aa-files**:

```
<Location /apc-aa-files/>
```

```
Options FollowSymLinks Multiviews
```

```
AllowOverride None
```

```
Order allow,deny
```



```
Allow from all
php_flag engine off
</Location>
```

6-. Servidor Seguro

Con el fin de garantizar aun más la seguridad en las comunicaciones con los sujetos de control es conveniente considerar la posibilidad de instalar la herramienta en un servidor seguro que utilice SSL (Secure Socket Layer) para encriptar las comunicaciones con los entes sujetos de control.

A través de este mecanismo se protegerán las claves y la información que envían los entes sujetos de control mientras circulan por Internet, protegiéndolos contra herramientas que inspeccionan las comunicaciones.

Este sistema no puede utilizarse para la página de las contralorías, solamente para el Aplicativo de la Rendición de la Cuenta Fiscal en Línea.

Tenga en cuenta que si los Sujetos de Control poseen muy malas conexiones a Internet el uso de SSL puede demorar aun más las transferencias de archivos entre los clientes y el servidor.