Páez – Cauca, 16 de abril de 2026

Ingeniero
César Augusto Escobar Prada
Supervisor orden 22630009
Imprenta Nacional de Colombia
Bogotá D. C.

Asunto: Informe de ejecución de la orden 22630009

Cordial saludo,

el día de hoy se terminó la emisión y configuración de los archivos de los certificados TLS, la Autoridad de Certificación (CA) SSL.com realizó la verificación de la organización, y los certificados OV serían activados el día de mañana por parte de la CA. Se realizó la generación de las llaves y los CSR en cada uno de los servidores para los siguientes subdominios:

- suscriptores.imprenta.gov.co (RSA)

- svrpubindc.imprenta.gov.co (RSA) (Diario oficial)

- mesadeayuda.imprenta.gov.co (ECDSA)

- gpingindc.imprenta.gov.co (ECDSA) (cortafuegos Palo Alto)

- servsgdoc.imprenta.gov.co (RSA) (Orfeo), que está en el mismo servidor con pqrd.imprenta.gov.co, urnavirtual.imprenta.gov.co y facturacion.imprenta.gov.co[1]

También con el personal encargado de los servidores de la INC el señor Lorenzo Fuentes, se realizó la instalación del escáner de malware ClamAV en el servidor de Orfeo, no fue posible realizar la instalación en el servidor del diario oficial debido a la desactualización del sistema operativo. [2]

Así mismo ya se realizó el escaneo de vulnerabilidades asociadas con los certificados TLS, documento adjunto a esta comunicación.

1 Se generó una llave privada para cada servidor en el formato óptimo según las capacidades de cada uno de los servidores. Las llaves privadas solo reposan en el servidor que se van a usar.

2 El servidor se encuentra muy desactualizado, y solo funciona con la versión de TLS 1.0, que en este momento está fuera de soporte en la mayoría de los servicios en Internet, incluso en los servicios de descarga de actualizaciones, debido a que se encontró que los protocolos TLS 1.0 y 1.1. tienen graves debilidades de seguridad.

En un correo anterior se envió la invitación para crear el usuario en la CA, para manejar la suscripción del certificado OV WildCard. Esta invitación también se envió al correo del señor Lorenzo Fuentes. Solo es necesario que creen el usuario en las próximas 72 horas. Nosotros seguiremos manejando la suscripción y el proceso con la CA, solo es para que tengan el acceso si quieren verificar o realizar alguna modificación.

Como la validez máxima de los certificados a cambiado a 200 días a partir de marzo de 2026, y cambiará a 100 días a partir de marzo de 2027, y de la misma forma la validez de la validación de la organización cambió hasta un máximo de 398 días[3] este sería el cronograma aproximado de reinstalaciones y el nuevo proceso de validación que se debe realizar:

Actividad	**Fecha**
Reinstalación de certificados OV	Octubre 2026
Reinstalación de certificados OV (antes de que cambie la duración a 100 días)	Marzo 2027
Revalidación de la organización	Marzo - abril 2027
Reinstalación de certificados OV	Septiembre 2027
Reinstalación de certificados OV	Diciembre 2027
Reinstalación de certificados OV	Marzo 2028

En todo caso el soporte técnico para los certificados TLS contratados y la herramienta de escaneo de malware seguirá vigente hasta la vigencia de los certificados el 09 de abril de 2028.

Recomendaciones:

1. **Actualizar** en el **servidor del diario oficial svrpubindc.imprenta.gov.co la versión de Java** (y en los demás servidores que esté desactualizado) y por ende la versión del sistema operativo, dado que actualmente tiene una versión que salió de soporte en el año 2020 y esta versión tiene vulnerabilidades conocidas que aumentan el riesgo de ataques maliciosos en contra del servidor web, que nunca van a ser arregladas porque

3 “Preparing for 47 day SSL/TLS certificates”, SSL.com. https://www.ssl.com/article/preparing-for-47-day-ssl-tls-certificates/

ya no tiene soporte. Se recomienda pasar como mínimo a la versión 17 de OpenJDK, e idealmente a la versión 21.

2. Actualizar los sistemas operativos CentOS 7 (Orfeo), Oracle Linux 6.4 (Diario oficial) a Red Hat Enterprise Linux (RHEL) 9 o 10 (de pago con soporte técnico oficial) o Alma Linux 9 o 10 (Clon gratuito), **para asegurar el acceso a actualizaciones de seguridad del sistema operativo,** la posibilidad de usar llaves de encriptación más modernas (ECDSA) al actualizar con el sistema operativo el servidor web, así como las versiones más actualizadas de escaneo de malware.
3. Se recomienda poner **el acceso a servprodoc.imprenta.gov.co** (DVR HikVision marca de cámaras de seguridad) **detrás de una VPN,** o no permitir conexiones entrantes desde Internet (ej.: configurando una restricción en el cortafuegos), o de no ser posible, por lo menos detrás de un proxy reverso como Nginx y asegurar que todas las conexiones entrantes pasen por el servidor web que si es posible configurarle un certificado TLS.
4. Igualmente se recomienda **bloquear conexiones entrantes desde Internet a la página de administración del cortafuegos Palo Alto en gpingindc.imprenta.gov.co,** ya que el plano de gestión ("management plane", o sea la página de administración) debe estar siempre aislado del plano de datos ("data plane", o sea el tráfico que pasa a través del firewall). Aunque el riesgo es menor porque el cortafuegos permite la instalación de un certificado TLS válido y el contrafuegos es capaz de recibir actualizaciones de seguridad. Aún así hay algún nivel de riesgo de inyección de credenciales (“credential stuffing”) y fuerza bruta, por tener la página de inicio expuesta a Internet.

Anexos:

1. Documento de análisis de vulnerabilidades
2. Pantallazos del estado del certificado con SSL.com
3. Pantallazos del portal de scripts para la generación de llaves privadas, CSR y obtención de los certificados generados una vez que la CA los firme.
4. Pantallazos del portal de scripts para la instalación de ClamAV

Anexo 2: Pantallazos del estado del certificado con SSL.com

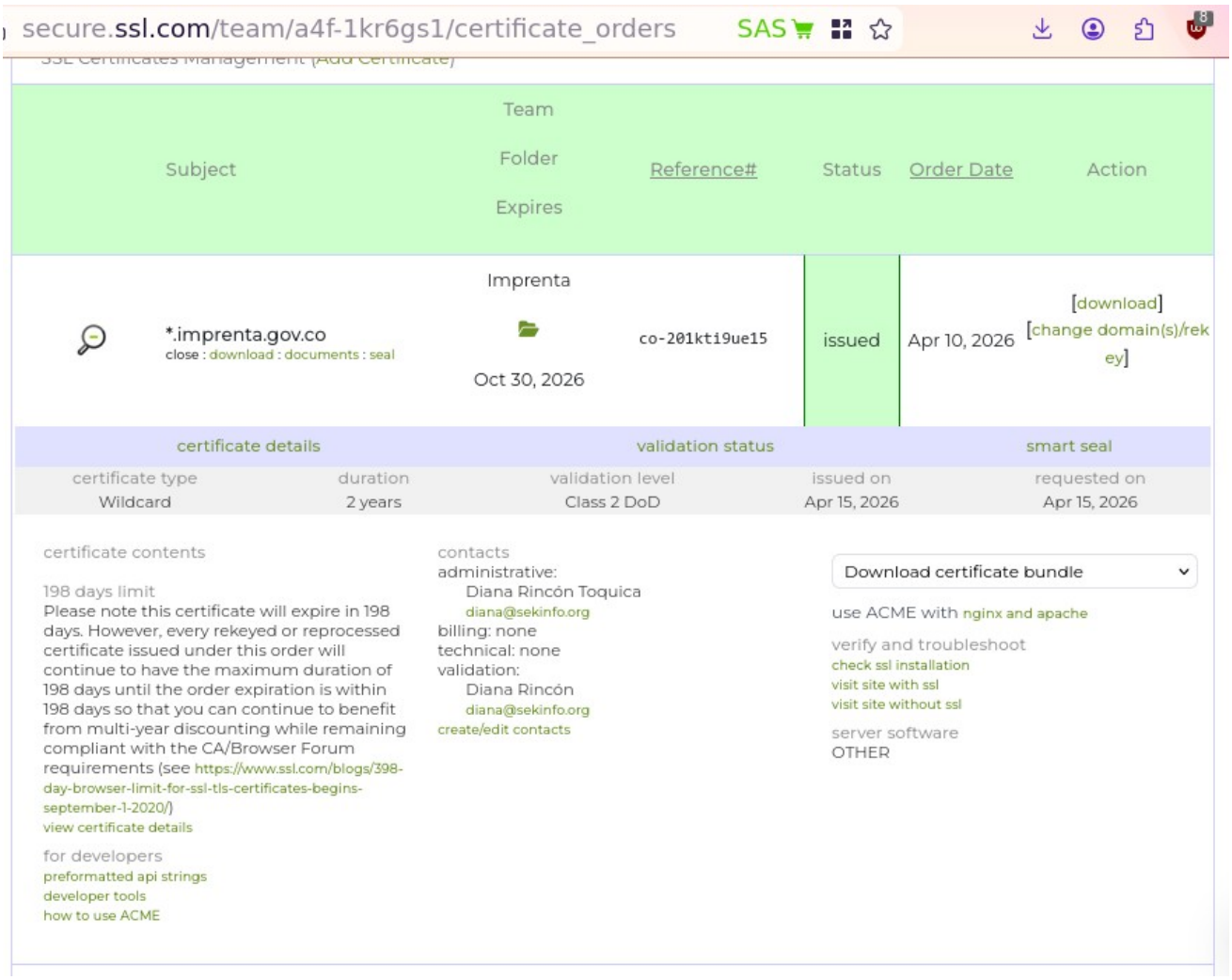


Figura 1: Estado del certificado WildCard OV por 2 años

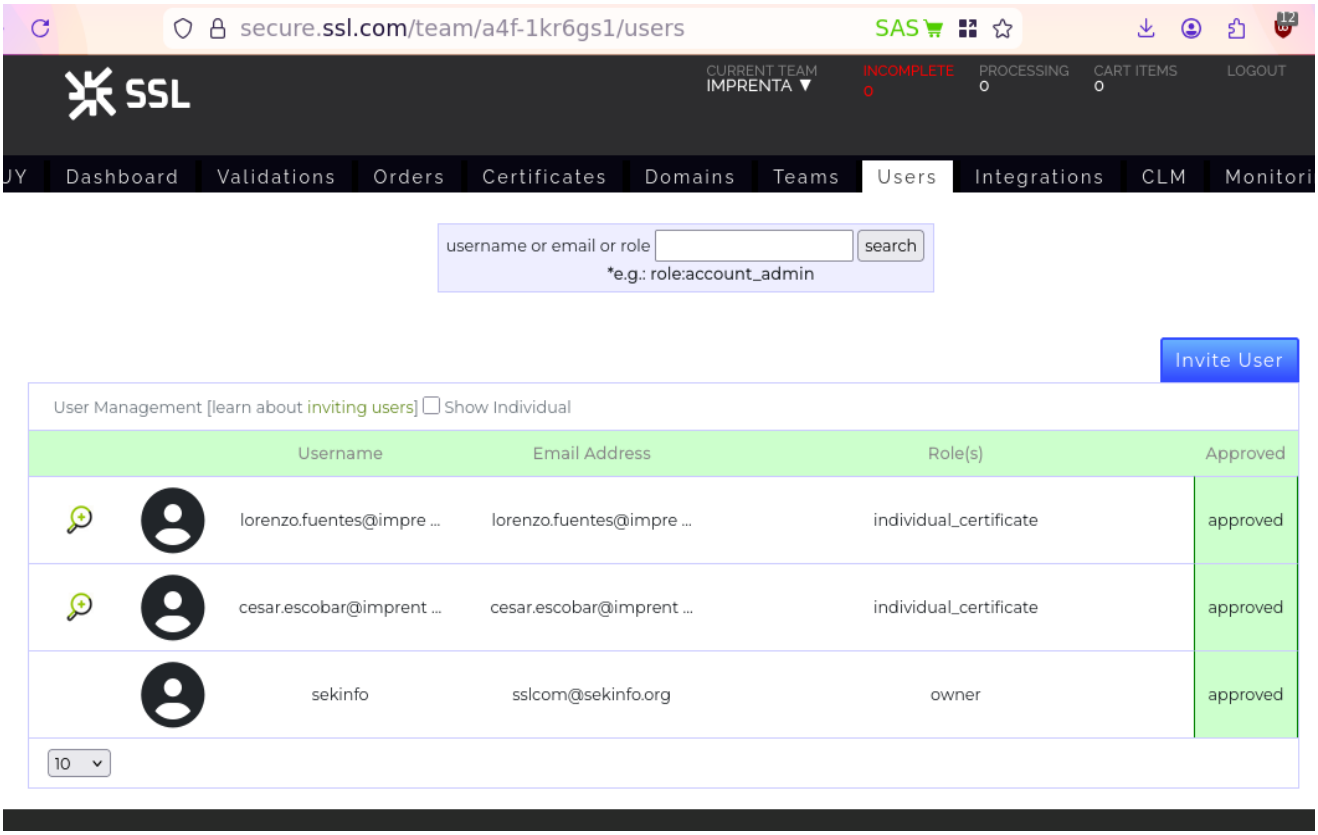
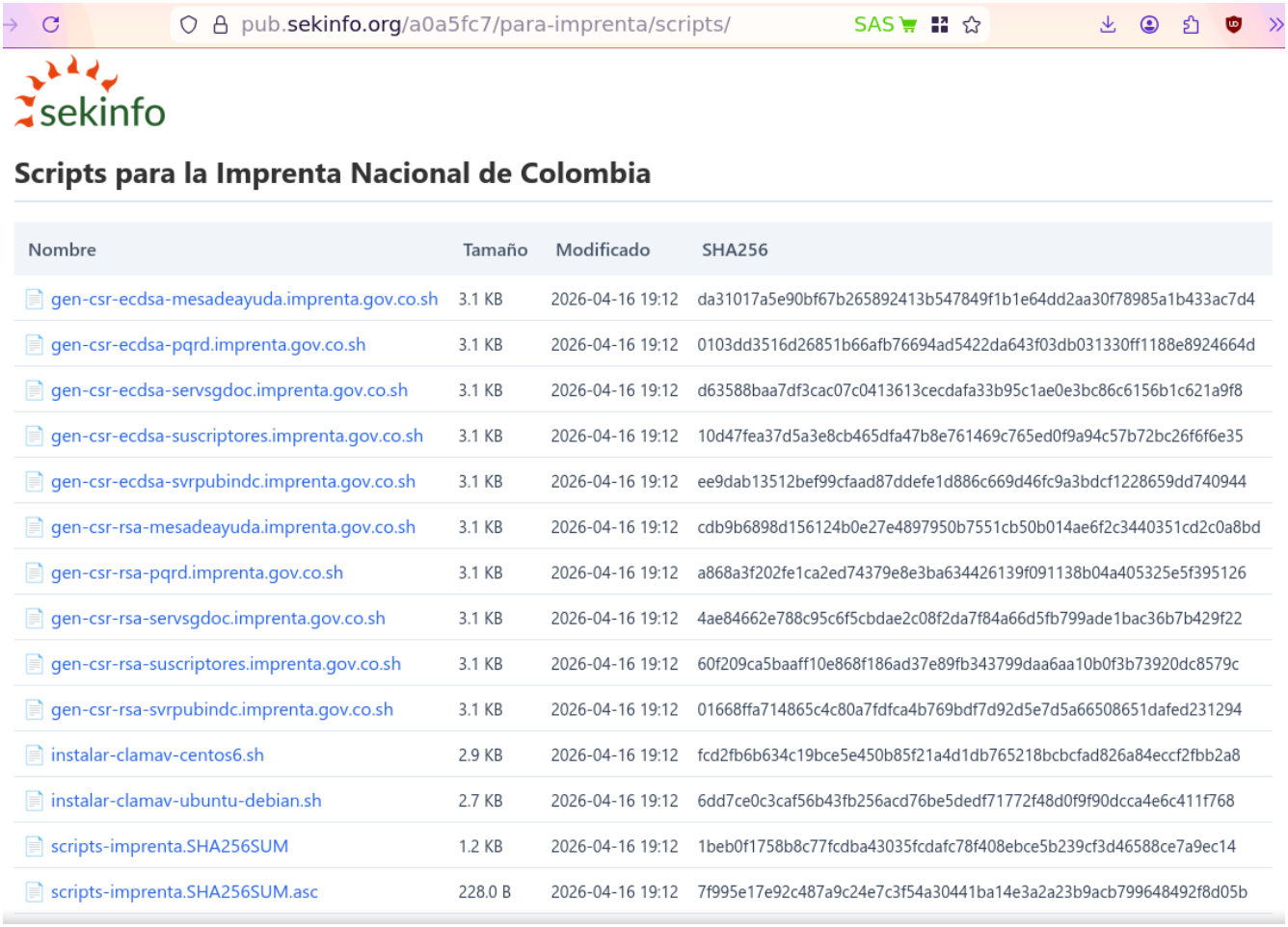


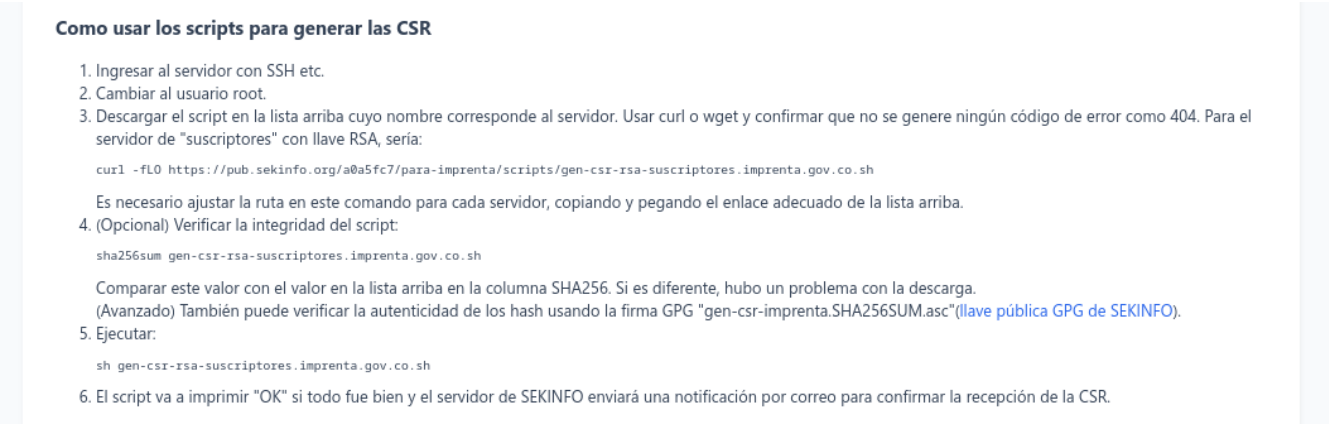
Figura 2: Usuarios autorizados para acceder a la configuración del Certificado OV WildCard

Anexo 3: Pantallazos del portal de scripts para la generación de llaves privadas, CSR y obtención de los certificados generados una vez que la CA los firme



Nombre	Tamaño	Modificado	SHA256
gen-csr-ecdsa-mesadeayuda.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	da31017a5e90bf67b265892413b547849f1b1e64dd2aa30f78985a1b433ac7d4
gen-csr-ecdsa-pqrd.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	0103dd3516d26851b66afb76694ad5422da643f03db031330ff1188e8924664d
gen-csr-ecdsa-servsgdoc.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	d63588baa7df3cac07c0413613cecdafa33b95c1ae0e3bc86c6156b1c621a9f8
gen-csr-ecdsa-suscriptores.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	10d47fea37d5a3e8cb465dfa47b8e761469c765ed0f9a94c57b72bc26f6f6e35
gen-csr-ecdsa-svrpubindc.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	ee9dab13512bef99cfaad87ddefe1d886c669d46fc9a3bdcf1228659dd740944
gen-csr-rsa-mesadeayuda.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	cdb9b6898d156124b0e27e4897950b7551cb50b014ae6f2c3440351cd2c0a8bd
gen-csr-rsa-pqrd.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	a868a3f202fe1ca2ed74379e8e3ba634426139f091138b04a405325e5f395126
gen-csr-rsa-servsgdoc.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	4ae84662e788c95c6f5cbdae2c08f2da7f84a66d5fb799ade1bac36b7b429f22
gen-csr-rsa-suscriptores.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	60f209ca5baaff10e868f186ad37e89fb343799daa6aa10b0f3b73920dc8579c
gen-csr-rsa-svrpubindc.imprenta.gov.co.sh	3.1 KB	2026-04-16 19:12	01668ffa714865c4c80a7fdfca4b769bdf7d92d5e7d5a66508651dafed231294
instalar-clamav-centos6.sh	2.9 KB	2026-04-16 19:12	fcd2fb6b634c19bce5e450b85f21a4d1db765218bcbcfad826a84eccf2fbb2a8
instalar-clamav-ubuntu-debian.sh	2.7 KB	2026-04-16 19:12	6dd7ce0c3caf56b43fb256acd76be5dedf71772f48d0f9f90dcca4e6c411f768
scripts-imprenta.SHA256SUM	1.2 KB	2026-04-16 19:12	1beb0f1758b8c77fcdba43035fcdafc78f408ebce5b239cf3d46588ce7a9ec14
scripts-imprenta.SHA256SUM.asc	228.0 B	2026-04-16 19:12	7f995e17e92c487a9c24e7c3f54a30441ba14e3a2a23b9acb799648492f8d05b

Figura 3: Scripts aportados para la configuración de los certificados TLS OV y herramienta de escaneo de malware ClamAV



Como usar los scripts para generar las CSR

1. Ingresar al servidor con SSH etc.
2. Cambiar al usuario root.
3. Descargar el script en la lista arriba cuyo nombre corresponde al servidor. Usar curl o wget y confirmar que no se genere ningún código de error como 404. Para el servidor de "suscriptores" con llave RSA, sería:

   ```
   curl -fLO https://pub.sekinfo.org/a0a5fc7/para-imprenta/scripts/gen-csr-rsa-suscriptores.imprenta.gov.co.sh
   ```

   Es necesario ajustar la ruta en este comando para cada servidor, copiando y pegando el enlace adecuado de la lista arriba.
4. (Opcional) Verificar la integridad del script:

   ```
   sha256sum gen-csr-rsa-suscriptores.imprenta.gov.co.sh
   ```

   Comparar este valor con el valor en la lista arriba en la columna SHA256. Si es diferente, hubo un problema con la descarga.
   (Avanzado) También puede verificar la autenticidad de los hash usando la firma GPG "gen-csr-imprenta.SHA256SUM.asc"(llave pública GPG de SEKINFO).
5. Ejecutar:

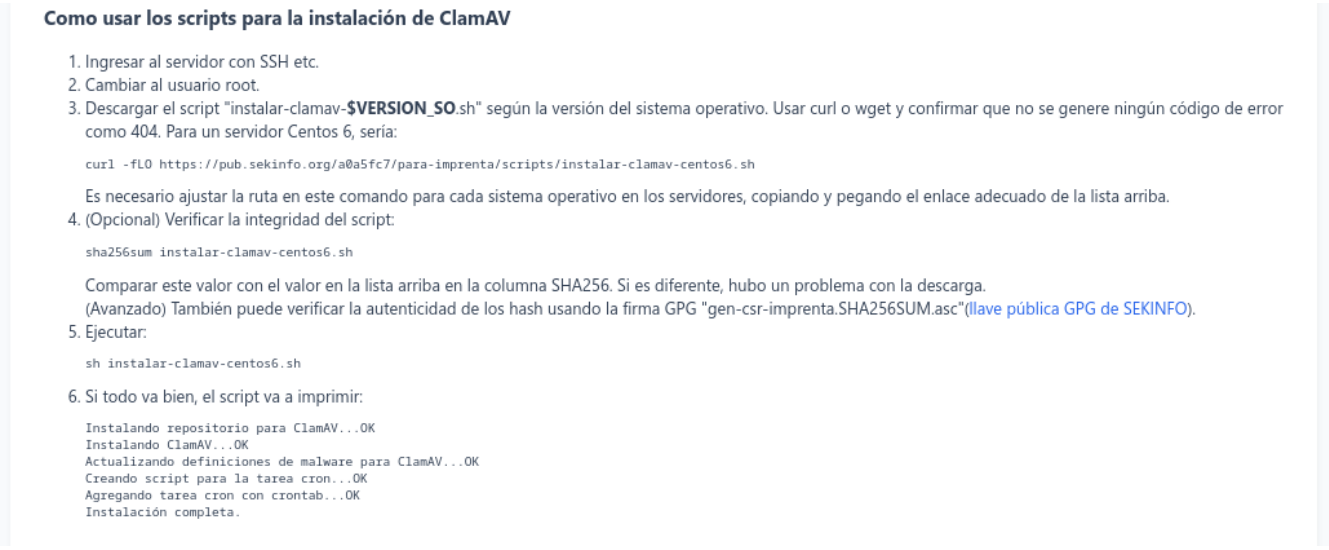
   ```
   sh gen-csr-rsa-suscriptores.imprenta.gov.co.sh
   ```

6. El script va a imprimir "OK" si todo fue bien y el servidor de SEKINFO enviará una notificación por correo para confirmar la recepción de la CSR.

Figura 4: Instrucciones para ejecutar los scripts de generación de llaves y CSR de los certificados TLS OV. En https://pub.sekinfo.org/a0a5fc7/para-imprenta/scripts/

.

Anexo 4: Pantallazos del portal de scripts para la instalación de ClamAV



Como usar los scripts para la instalación de ClamAV

1. Ingresar al servidor con SSH etc.
2. Cambiar al usuario root.
3. Descargar el script "instalar-clamav-**$VERSION_SO**.sh" según la versión del sistema operativo. Usar curl o wget y confirmar que no se genere ningún código de error como 404. Para un servidor Centos 6, sería:

   ```
   curl -fLO https://pub.sekinfo.org/a0a5fc7/para-imprenta/scripts/instalar-clamav-centos6.sh
   ```

   Es necesario ajustar la ruta en este comando para cada sistema operativo en los servidores, copiando y pegando el enlace adecuado de la lista arriba.
4. (Opcional) Verificar la integridad del script:

   ```
   sha256sum instalar-clamav-centos6.sh
   ```

   Comparar este valor con el valor en la lista arriba en la columna SHA256. Si es diferente, hubo un problema con la descarga.
   (Avanzado) También puede verificar la autenticidad de los hash usando la firma GPG "gen-csr-imprenta.SHA256SUM.asc"(llave pública GPG de SEKINFO).
5. Ejecutar:

   ```
   sh instalar-clamav-centos6.sh
   ```

6. Si todo va bien, el script va a imprimir:

   ```
   Instalando repositorio para ClamAV...OK
   Instalando ClamAV...OK
   Actualizando definiciones de malware para ClamAV...OK
   Creando script para la tarea cron...OK
   Agregando tarea cron con crontab...OK
   Instalación completa.
   ```

Figura 5: Instrucciones para ejecutar los scripts de generación de llaves y CSR de los certificados TLS OV. En https://pub.sekinfo.org/a0a5fc7/para-imprenta/scripts/