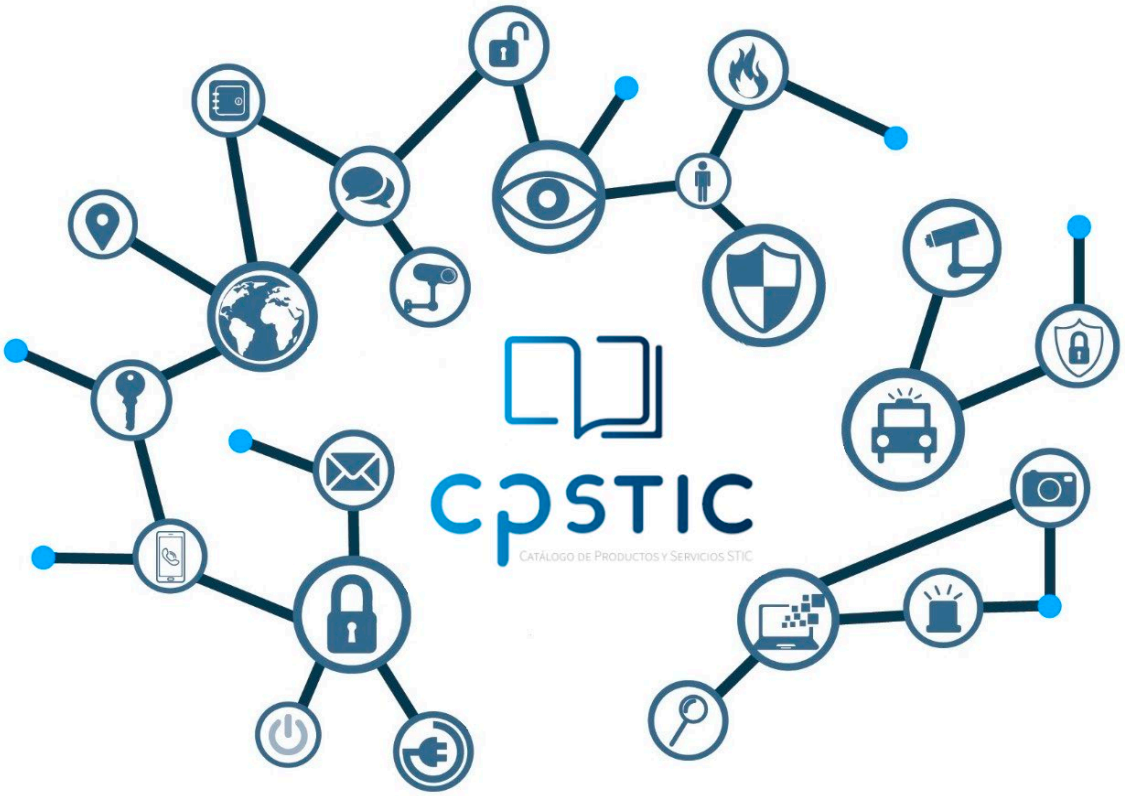
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1220

Procedimiento de Empleo Seguro
TrendMicro Tipping Point



Junio 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.06.06 15:25:12 +02'00'

NIPO: 083-23-157-2.
Fecha de Edición: junio de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. **Tipping Point TPS es una plataforma de seguridad red que permite monitorizar y detectar vulnerabilidades con alta precisión.**
2. Proporciona protección contra distintos vectores de ataque con una alta flexibilidad, ayudando a lograr resiliencia frente al *malware* y *phising*. Emplea una combinación de tecnologías, incluyendo *Deep packet inspection*, reputación de ataques, reputación de URLs, etc.

2. OBJETO Y ALCANCE

3. El objeto del presente documento es facilitar la instalación y configuración segura del producto **Tipping Point con la versión de software 5.4.1**, junto con el aseguramiento del entorno en el que se despliega.

3. ORGANIZACIÓN DEL DOCUMENTO

4. El documento ha sido estructurado de la siguiente manera:

   a) Apartado **4**. Fase de despliegue e instalación, describe todas las tareas necesarias para efectuar un despliegue seguro del producto.

   b) Apartado **5**. Fase de Configuración. Detalla las configuraciones a aplicar en el producto para que este opere de manera segura optimizando sus capacidades de protección y rendimiento.

   c) Apartado **6**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

   d) Apartado **7**. Listado de tareas a completar empleando la presente guía.

   e) Apartado **8**. Referencias externas a este documento de recomendada revisión.

   f) Apartado **9**. Abreviaturas empleadas en el documento.

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

5. El producto se compone de un *appliance* TPS (*Threath Prevention System*) y una consola de gestión SMS la cual puede ser en modo físico o virtual.
6. En caso de adquirir el producto en formato físico, se deberá verificar:
   a) Que el paquete se recibe correctamente precintado y no muestra señas de haber sido alterado.
   b) Que el número de serie del producto recibido corresponde con el indicado en el albarán de compra.
7. La descarga del software relativo a la solución vSMS, versiones de *firmware* tanto del IPS como de la consola de gestión SMS, vacunas digitales, firmas personalizadas, o firmas de detección de malware en red y base de datos reputacionales, se realiza desde el portal de TMC https://tmc.tippingpoint.com/TMC/

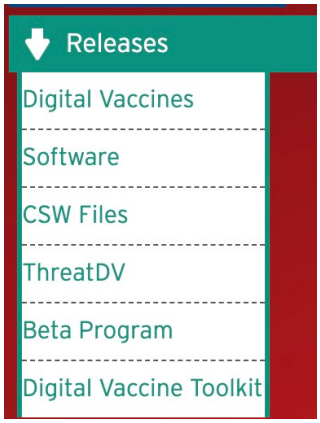


Ilustración 1. Página de descargas

8. Una vez descargado el software, se deberá realizar su *hash* y verificar que coincide con el mostrado en la página de descarga.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Se recomienda desplegar la consola SMS en el CPD de la organización y que los puertos de comunicación del producto (descritos en el apartado **4.4 CONSIDERACIONES PREVIAS**) estén limitados a recibir conexiones desde los entornos a proteger.
10. La única comunicación externa que realizará la consola SMS es hacia la URL del portal TMC, pudiendo ser esta parte opcional y descargar de manera manual las actualizaciones de las firmas.

4.3 REGISTRO Y LICENCIAS

11. Durante el proceso de compra de licencias, la organización recibirá un certificado de licenciamiento donde se listarán las claves de registro asociadas al producto.
12. La organización deberá acceder al portal https://tmc.tippingpoint.com/TMC/ para registrarse utilizando el *Customer ID* adjunto en el certificado de licencia. Este código se utilizará para crear la cuenta de cliente donde se podrán descargar: la descarga del software relativo a la solución vSMS, versiones de firmware tanto del IPS como de la consola de gestión SMS, vacunas digitales, firmas customizadas, o firmas de detección de malware en red y base de datos reputacionales.
13. Tipping point dispone de dos (2) tipos de licencias que se basan en *throughput* inspeccionado:
    a) Digital Vacine: Incluye firmas sobre vulnerabilidades, *exploits*, sanitización de tráfico, desviación de protocolos, DOS, etc.
    b) Threat Digital Vacine: Incluye firmas de Antimalware, reputación DNS/IP, C&C, Botnets y posibilidad de importar reglas snort, etc.
14. Se puede consultar la información sobre licenciamiento en detalle en el apartado *Licensing* de la guía *User Guide – REF1*.

4.4 CONSIDERACIONES PREVIAS

15. De cara a disponer de un rendimiento óptimo, se recomienda dimensionar correctamente las licencias de inspección, acorde al *throughput* que se va a inspeccionar por parte del IPS.
16. Se debe contemplar el espacio en RACK para el IPS y su consola de gestión SMS. En el caso de ser todo virtual, no debe contemplarse espacio en RACK.
17. Si el despliegue se realiza en formato virtual, se deben reservar diversos recursos. En la guía *vSMS Getting Started Guide – REFX*, se puede consultar el detalle de los requisitos necesarios.
18. Adicionalmente, en el apartado *Required ports* de la guía *User Guide – REF1*, se pueden consultar todos los puertos empleados en las comunicaciones del producto. Se recomienda verificar los puertos empleados para permitir todas las comunicaciones necesarias para la correcta operación del producto en los cortafuegos o proxys de la organización.

4.5 INSTALACIÓN

19. Configuración inicial de IPS o vIPS:
    a) La configuración inicial de TPS se realiza mediante puerto de consola, utilizando un terminal o un emulador como *PuTTY*. Para ello, se debe utilizar el cable de consola suministrado con el appliance, empleando los siguientes parámetros de conexión:

- *115200 baud, 8, None, 1.*

b) Una vez conectado y establecida la conexión aparecerá el siguiente mensaje:

```
Welcome to the TippingPoint Technologies Initial Setup wizard.
Press any key to begin the Initial Setup Wizard or use LCD panel.
```

c) Después se mostrará el siguiente mensaje para comenzar el *setup* inicial de configuración:

```
You will be presented with some questions along with default values in brackets[].
Please update any empty fields or modify them to match your requirements. You may
press the ENTER key to keep the current default value. After each group of
entries, you will have a chance to confirm your settings, so don't worry if you
make a mistake.
```

d) Se solicitará el nivel de seguridad de contraseñas, se debe mantener el valor por defecto, ya que se trata del más restrictivo (Nivel 2).

```
There are three security levels for specifying user names and passwords:
 Level 0: User names and passwords are unrestricted.
 Level 1: Names must be at least 6 characters long; passwords
 at least 8.
 Level 2: In addition to level 1 restrictions, passwords must
 contain:
  - at least 2 alpha characters
  - at least 1 numeric character
  - at least 1 non-alphanumeric character
Please specify a security level to be used for initial super-user name and
password creation. As super-user, you can modify the security level later on via
Command Line Interface (CLI) or Local Security Manager (LSM).
Security level [2]:
```

e) En el siguiente paso de la configuración, se solicitará cambiar la contraseña por defecto del Usuario administrador *SuperUser* y contraseña por defecto root—00. La nueva contraseña deberá cumplir con la política de contraseñas definida en el apartado 5.4.3 Parámetro de seguridad para administradores.

```
Please enter a user name that we will use to create your super-user account.
Spaces are not allowed.
Name: superuser
Do you wish to accept [superuser] <Y,[N]>:Y
Please enter your super-user account password: root--00
Verify password: root--00
Saving information...Done
Your super-user account has been created.
You may continue initial configuration by logging into your device.
After logging in, you will be asked for additional information.
```

f) Una vez activada y modificada la cuenta *SuperUser*, continuará el *setup* de configuración inicial para configurar su IPv4/IPv6, hostname, localización, etc.

g) A continuación, se muestra un ejemplo.

```
The host management port is used to configure and monitor this device via a
network connection (e.g., a web browser).
Enter Management IPv4 Address [none]: 10.252.0.71
Enter Network IPv4 Mask [255.255.255.0]:
Enable IPv6 [No]: y
Enable IPv6 Address Autoconfig [No]: y
Enter Host Name [myhostname]: device71
Enter Host Location [room/rack]: Lab

   Host IPv4: 10.252.0.71/24
IPv6 Enabled: Yes
 Host Link-Local IPv6: fe80::207:99ff:fe66:6999/64
   Host IPv6: Auto
   Host Name: device71
        Host Location: Lab
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a
```

h) Una vez configurada la IP, *hostname* y localización, se solicitará el *Gateway*, DNS y reloj de sistema.

i) Después de ingresar las opciones de reloj de sistema, introducir No para finalizar la configuración inicial.

20. Configuración inicial de SMS o vSMS:

a) La configuración inicial de SMS es muy similar a la configuración inicial del IPS. Según el dispositivo de SMS que esté implementando, llegar al punto del asistente de configuración inicial variará ligeramente.

- Para el SMS en formato *hardware*, basta con conectar un teclado y un monitor VGA. Alternativamente, la consola serie también se puede utilizar para realizar la configuración inicial, utilizando una aplicación de emulación como PuTTY. Los ajustes de la consola serie son: 9600, 8, N, 1.
- Para vSMS, la configuración inicial se realizará a través de la consola de *vCenter* o KVM después de implementar OVF.

b) La primera vez que se inicia un SMS, deberá proporcionar el nombre de usuario y la contraseña predeterminados de fábrica.

- *SuperUser* (*Case Sensitive*) y contraseña <en blanco>.

c) Después de ingresar el nombre de usuario y la contraseña predeterminados de fábrica, se solicitará aceptar el acuerdo de licencia.

d) El resto del asistente de configuración inicial de SMS es casi idéntico al asistente de configuración inicial de NGIPS. Por lo tanto, usar los mismos valores.

e) Una vez completado el asistente, es posible que se solicite reiniciar el servidor.

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

21. **Se deberá configurar el producto para operar en modo seguro. Para ello, se debe ejecutar el siguiente comando mediante la interfaz CLI de TPS: *fips-mode-enable*.**
22. Una vez activado, no se podrá desactivar a no ser que se reseteen los parámetros de fábrica. Ejecutar el comando *show fipsmode* para verificar que ha sido activado correctamente.
23. También se debe habilitar el modo seguro en SMS, para ello es necesario realizar los siguientes pasos:
    - Ir a Admin > Server Properties y seleccionar la pestaña Management.
    - Hacer clic en *Edit* sobre *FIPS Mode.*
    - Revisar el modo configurado actualmente. Desde el desplegable se puede comprobar si está activado el modo *FIPS Crypto Core*. Seleccionar *Enabled* en el desplegable.
    - Hacer clic en *OK*, cuando se cambia a modo FIPS el servidor SMS reiniciará automáticamente.
24. Una vez que el proceso se ha completado, el SMS operará en modo seguro y se aplicarán las siguientes restricciones:
    - No se permitirá hacer un *upgrade* de la clave de certificados.
    - El SMS no comunicará con el agente de Identidad.
    - Las acciones de respuesta *Custom Responder Actions* no podrán importarse o ejecutarse.
    - El acceso externo la base de datos no está permitido.
    - La replicación externa de la base de datos no está permitida.

5.2 AUTENTICACIÓN

25. El producto requiere la autenticación de los usuarios para acceder a la configuración. Los mecanismos disponibles son los siguientes:
    - Credenciales locales mediante usuario/contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver apartado **5.4.2 CONFIGURACIÓN DE ADMINISTRADORES**.
    - Servidores de autenticación externos. Mediante la integración con distintos servidores de autenticación. Para la configuración y gestión de los mismos, ver apartado **5.3 SERVIDORES DE AUTENTICACIÓN**.
26. El producto empleará aquellos servidores de autenticación externos configurados para llevar a cabo la autenticación de usuarios. Para emplear únicamente la

autenticación local, se deberá activar la casilla *Local Authentication Only*, durante la creación de usuarios.

5.3 SERVIDORES DE AUTENTICACIÓN

27. El producto permite efectuar la autenticación de usuarios empleando Active Directory, RADIUS, TACACS+ y CAC. El detalle de configuración de los servidores de autenticación, se puede consultar en el apartado *Authentication configuration* de la guía *User Guide – REF1.*
28. En caso de emplear alguna de las opciones disponibles, se recomienda seguir las siguientes indicaciones:
    - En caso de emplear RADIUS, seleccionar *PEAP/EAP-MSCHAPv2* como método de autenticación.
    - En caso de emplear Active Directory, seleccionar *Enable SSL*, seguido de *Using LDAPS.*

5.4 ADMINISTRACIÓN DEL PRODUCTO

5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

29. El producto dispone de las siguientes interfaces para su administración:
    - Administración remota a través de LSM (*Local Security Manager*). Mediante HTTPS/TLS y empleada principalmente para ver logs en tiempo real. Accesible desde https://<IP del IPS>/
    - Administración remota a través de SMS (*Security Management System*). Cliente pesado que conecta con el producto, permitiendo una gestión centralizada de varios IPS de tipo GUI. Mediante protocolo HTTPS.
    - Administración remota de tipo CLI mediante SSHv2. El producto solo permite el empleo de la versión 2 de SSH.
    - Administración local mediante consola.
30. Se recomienda realizar la configuración y gestión del producto mediante SMS o la interfaz de tipo CLI.

5.4.2 CONFIGURACIÓN DE ADMINISTRADORES

31. Por defecto el producto dispone de los siguientes roles:
    - *SuperUser*: dispone de permisos de lectura/escritura para todas las configuraciones del producto. Es el único rol con la capacidad de modificar la contraseña de otros usuarios.
    - *Operator*: dispone de permisos de lectura sobre todas las configuraciones del producto. Se trata de un rol de monitorización.

- *Admin*: dispone de permisos de lectura/escritura para todas las configuraciones salvo la gestión de usuarios, grupos y roles.

32. Adicionalmente, se pueden crear roles personalizados ajustándose a las necesidades de la organización. Para ello, ir a *Admin > Authentication and Authorization > Roles* y seleccionar *New*. Se pueden seleccionar los permisos deseados de forma granular.
33. El producto dispone también de la funcionalidad de "grupos". Se pueden emplear para agrupar usuarios y gestionar los recursos a los que pueden acceder de forma conjunta.
34. El detalle de configuración de Roles y Grupos se puede consultar en el apartado *User roles and capabilities* de la guía *User Guide – REF1.*
35. Para la creación de un nuevo usuario, ir a *Admin > Authentication and Authorization > Users* y seleccionar *New*. Se deberá introducir la contraseña, que deberá cumplir con la política de contraseñas definida a continuación, así como el rol de usuario. Seleccionar la casilla *Change password on next login*, de tal forma que el usuario deba modificar su contraseña en el primer acceso.
36. El detalle de configuración de Usuarios se puede consultar en el apartado *Create or edit a user account* de la guía *User Guide – REF1.*

5.4.3 PARÁMETROS DE SEGURIDAD PARA AMINISTRADORES

37. Una vez creados los administradores, se deben configurar los parámetros de sesión de los administradores del producto, desde *Edit > Preferences > Security*:
    - Seleccionar el nivel dos (2) de seguridad de contraseñas (nivel máximo), el cual exige:
        - Las contraseñas deben ser distintas de la anterior.
        - Deben contener al menos una minúscula y una mayúscula.
        - Deben contener al menos un número.
        - Deben contener al menos un carácter especial.
        - Longitud mínima de 15 caracteres.
    - Seleccionar *Lock user after failed login attempts*, configurando un valor de 3 intentos fallidos. Configurar el valor de *Lockout Time* en 5 minutos.
    - Seleccionar *Require new password to be different from previous passwords*, con un valor de 5.
    - Activar *Show previous login details when a user logs in*, para mostrar a los usuarios el historial reciente de accesos.
    - Activar *Require user to reauthenticate*, con el valor deseado para fijar un tiempo máximo de sesión.

- Seleccionar *Timeout client session after inactivity*, con un valor de 5 minutos. Tras 5 minutos de inactividad, los usuarios deberán iniciar sesión de nuevo.
- Seleccionar *Enforce a mínimum password lifetime*, con un valor de 60 días, tras el cual los usuarios deberán modificar sus contraseñas.

38. Por último, los administradores deberán asegurar de forma procedimental que no se puedan volver a modificar las nuevas contraseñas hasta pasados 7 días.
39. El detalle de configuración de los parámetros de sesión, se puede consultar en el apartado *Preferences > Security* de la guía *User guide – REF1.*

5.4.4 CONFIGURACIÓN DEL BANNER DE ACCESO

40. **Se debe configurar el mensaje de aviso antes de la autenticación** en el producto, para ello ir a *Edit > Preferences > Banner Message* y seleccionar las interfaces empleadas para el acceso de usuarios. Finalmente introducir el mensaje deseado y guardar.

5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

41. Para evitar el uso de interfaces y servicios inseguros en TPS, **se deben desactivar manualmente los servicios no empleados, y aquellos considerados inseguros**. Para ello, seguir los siguientes pasos:
    - Ir a *Edit > Preferences > Services*.
    - Desmarcar la casilla correspondiente a HTTP para deshabilitarlo.
    - Desmarcar la casilla correspondiente a SNMP para deshabilitarlo.
    - TPS soporta SNMP v1, v2 y v3. En caso de emplearse, **deberá ser utilizando SNMP v3 con autenticación vía SHA y cifrado AES.**

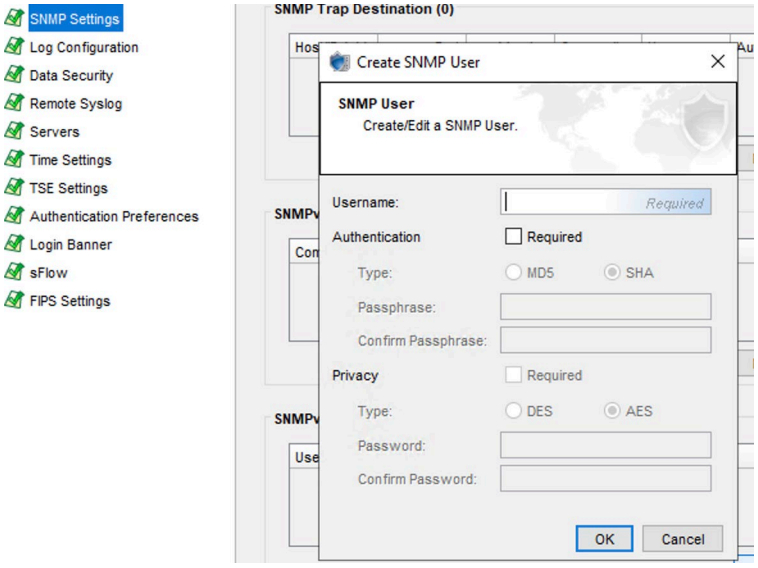


Ilustración 2. Versión SNMP

- En el apartado *TLS Settings*, se debe verificar que no se encuentren marcadas casillas correspondientes a versiones inferiores a TLSv1.2.

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

42. Tal como se ha mostrado en el apartado **5.1 MODO DE OPERACIÓN SEGURO**, se debe activar el modo seguro, el cual fuerza el empleo de protocolos y algoritmos seguros en el producto:
    - Los protocolos SSH, HTTPS, y el cliente de SMS negociarán usando solo algoritmos seguros.
    - La versión usada por defecto será TLSv1.2.
    - *External DB replication* no está permitido.
    - El contador de intentos fallidos de bloqueo permanecerá activado para todos los usuarios.
43. Para deshabilitar SNMP, ir a *Admin > Server Properties > SNMP* y desactivar la casilla *Enable SNMP Requests.* En caso de requerir su uso, se deberá emplear únicamente la v3 del protocolo, por lo que sería necesario marcar únicamente la casilla *v3* en el apartado *version*.
44. También se deben configurar las comunicaciones TLS de SMS con los distintos componentes del producto. Para ello, desde *Admin > Server Properties > TLS*, verificar que solo se encuentra activada la casilla *TLSv1.2* para los distintos tipos de comunicación.

5.7 GESTIÓN DE CERTIFICADOS

45. El detalle de configuración de los certificados se puede consultar a partir del apartado *Certificate management* de la guía *User Guide – REF1.*
46. Deberán seguirse los siguientes pasos generales:
    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor, así como los correspondientes a los servidores de autenticación o servidores de auditoría (*syslog*) en caso de ser empleados.
    - Crear un CSR (*Certificate Signing Request*) para el certificado de servidor empleado por SMS. Ver apartado *Create a new signing request* de la guía *User Guide – REF1.* **Se deberá emplear el siguiente parámetro para la creación del certificado**: tipo de clave RSA, con una longitud de clave de 4096 bits o superior.

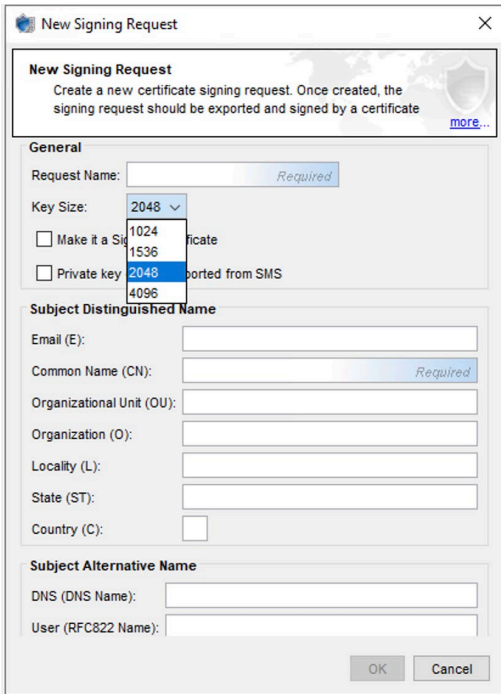


Ilustración 3 . Creación de un CSR.

- Importar el certificado de servidor una vez recibido.

5.8 SINCRONIZACIÓN HORARIA

47. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

48. El producto permite el empleo de servidores NTP para obtener la hora. Ir a *Admin > Server Properties* y seleccionar la pestaña *Network*. Seleccionar *Enable Time Protocol (NTP)* bajo *Date/Time*. Introducir los datos del servidor NTP deseado y hacer clic en *Apply*.

49. No se permite el uso de claves de autenticación para el servicio NTP. Debido a esto**, se recomienda utilizar sólo servidores de tiempo ubicados en la red interna** de la organización para evitar posibles ataques.

50. También es posible definir manualmente la hora y fecha en el producto. Para ello, desde *Admin > Server Properties > Network,* con la casilla *Enable Time Protocol (NTP)* deshabilitada, hacer clic en el icono *New Date/Time* e introducir los valores.

5.9 ACTUALIZACIONES

51. El producto requiere la actualización tanto de la consola de gestión SMS, cómo del *IPS Tipping Point*. También se recibirán actualizaciones de las firmas y reglas del IPS.

52. Las actualizaciones de la consola SMS se pueden descargar desde la misma consola o comprobando la página del fabricante:

    https://tmc.tippingpoint.com/TMC/

53. Tal como se ha indicado en el apartado **4.1 ENTREGA SEGURA DEL PRODUCTO**, **se deberá realizar su hash y verificar que coincide con el mostrado en la página de descarga.**
54. Antes de realizar una actualización, se recomienda llevar a cabo una copia de seguridad, ver apartado **5.14 COPIAS DE SEGURIDAD**.
55. Las actualizaciones de Tipping Point se pueden realizar desde SMS en *Devices* > *Tipping Point OS*, o desde la interfaz de comandos del propio dispositivo. En el siguiente enlace se puede consultar el proceso detallado.
56. La actualización del paquete de reglas de IPS, se realiza desde el menú: *Profiles/Digital Vacine o Profiles/auxiliary DV*. El paquete puede descargarse, activarse y distribuirse a los IPS de forma automática o manual. Para el modo automatico, el SMS debe tener acceso a internet y llegar a la URL del TMC: https://tmc.tippingpoint.com/TMC/
57. En caso de emplear el modo manual, se deberá realizar la verificación de la integridad tal como se indica anteriormente.
58. Una vez descargada la nueva versión, se recomienda revisar las *release notes* para comprobar qué reglas han cambiado y cuáles se han añadido nuevas. Tras dicha comprobación hay que activar el paquete descargado en el SMS para que se reflejen las nuevas reglas en la búsqueda del perfil. Una vez activado el paquete nuevo de *Digital Vacine*, hay que distribuirlo a los IPSs que se quieran actualizar.

5.10 AUTO-CHEQUEOS

59. Tanto *Tipping point IPS* como el SMS, realizan comprobaciones de integridad de los servicios en el arranque, incluyendo también el sistema operativo. También se realiza un chequeo automático de integridad a nivel de *checksum* cuando se carga un nuevo sistema operativo o reléase, siendo homologado por el SMS antes de realizar el *upgrade* de versión tanto a nivel de SMS como IPS.
60. TPS realiza test de integridad del *software* y tests criptográficos de “respuesta conocida” durante el arranque. Si alguno de los test fallase, el producto entra en estado de error y muestra un mensaje de restauración del sistema. Mientras permanezca en estado de error, no realiza ninguna operación criptográfica.

5.11 SNMP

61. El producto permite el envío de eventos (alertas) utilizando el protocolo SNMPv1, SNMPv2 y SNMPv3.
62. **Se debe emplear únicamente SNMPv3 por el mayor nivel de seguridad** que aporta el protocolo ya que permite usar autenticación MD5 o SHA y cifrado con DES o AES. **En caso de usarse, deberá configurarse para utilizar únicamente SHA y AES.**

5.12 ALTA DISPONIBILIDAD

63. Existen varios servicios que pueden disponer de alta disponibilidad:

    - IPS – tarjetas con bypass en hardware. Los IPS disponen de tarjetas con bypass incluidas en placa, con el fin de no interrumpir el servicio de comunicación si el *appliance* tiene un fallo. También conocido como Layer2 Fallback (L2FB). El detalle se puede consultar en el siguiente enlace.
    - IPS - HA Transparente. Es posible implementar el modo HA transparente en una configuración de red redundante para que un dispositivo asociado se haga cargo en caso de falla del sistema teniendo una copia de sesiones a la unidad secundaria. La información que se comparte entre ambos nodos es información (flujos bloqueados, flujos confiables y hosts en cuarentena). El detalle de configuración se puede consultar en el apartado *Device High Availability* de la guía *User Guide – REF1.*
    - SMS – *clustering*: El SMS se puede desplegar de forma redundada, formando un cluster activo/pasivo. El detalle se puede consultar en el apartado *SMS High Availability* de la guía *User guide – REF1*.

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

64. Los eventos relativos al sistema y a auditoria se pueden consultar desde *Device > Selección del dispositivo > Events.* Todos los eventos incluyen un identificador, la hora del evento, el usuario en caso de aplicar y una descripción. Son de tres tipos:

    - Eventos del sistema (*System Events*): Relativos a actividades relacionadas con el funcionamiento del producto.
    - Eventos de auditoría.
    - Eventos de seguridad. Relativos a actividades registradas en la inspección de tráfico por parte del IPS.

5.13.2 ALMACENAMIENTO LOCAL

65. Toda la información de eventos y configuraciones se almacena en la BBDD interna del SMS. La BBDD se puede externalizar siguiendo el siguiente procedimiento:

    https://success.trendmicro.com/dcx/s/solution/TP000088865-How-do-I-enable-external-access-to-the-SMS-database?language=en_US&sfdcIFrameOrigin=null

66. Una vez alcanzado el límite de retención, el producto comenzará a sobrescribir eventos antiguos. La sobre escritura quedará definida por antigüedad de datos o por número de registros. Es posible modificar los periodos de retención desde *Admin > Maintenance Settings*.

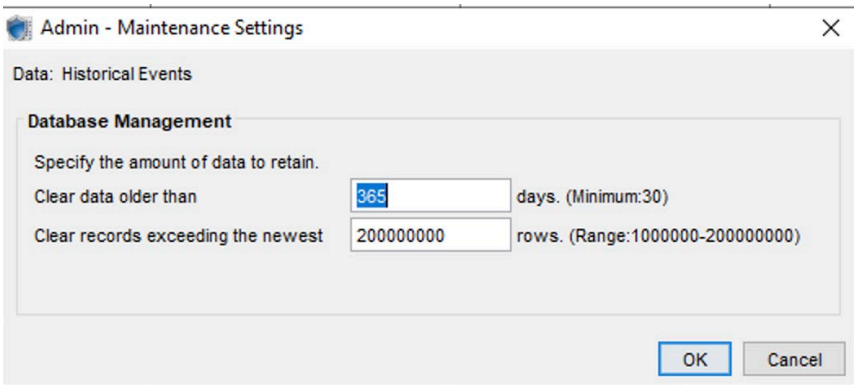


Ilustración 4. Retención de registros de auditoría

5.13.3 ALMACENAMIENTO REMOTO

67. El producto permite el envío de eventos a un sistema de almacenamiento remoto empleando el protocolo *Syslog*. Debido al espacio limitado de almacenamiento local, **se recomienda configurar el envío de eventos a un servidor externo de auditoría**.

68. Para ello, ir a *Devices > All devices > device* y hacer clic en *Device configuration*. Seleccionar *Remote Syslog* y hacer clic en *New*. Introducir los siguientes datos para realizar el envío cifrado de los registros:

    - Dirección del servidor.
    - En protocolo seleccionar *Encrypted TCP*.
    - Importar el certificado del servidor Syslog.
    - Finalmente hacer clic en *OK*.

5.14 COPIAS DE SEGURIDAD

69. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto**. Para realizar la copia de la Base de Datos de SMS, ir a *Admin > Database > Backup* y hacer clic en:

    - *New* si se desea programar una copia de seguridad.
    - *Backup now* si se desea realizar una copia manual en el instante.

70. Finalmente se deberá seleccionar qué información desea incluirse en la copia de seguridad, desde SMS se puede salvar la configuración de todas las máquinas. El detalle de las copias de la base de datos de SMS se puede consultar en el apartado *Backup and restore de la guía User Guide – REF1.*

5.15 SERVICIOS DE SEGURIDAD

71. Los servicios de seguridad proporcionados por *Tipping Point* se dividen en los descritos a continuación:

- Servicio de inspección IPS: se implementa mediante paquetes de reglas de IPS, llamados *Digital Vacine*. Se publica un nuevo paquete cada martes del año.
- Servicio de Inspección Antimalware-IPS: Se implementa mediante paquetes de reglas de Antimalware, llamados *Auxiliary DV*, suscrito mediante la licencia de inspección (*Threat DV*). Se publica un nuevo paquete cada martes del año.
- Servicio de reputación: Se implementa mediante paquetes de reputación, suscrito mediante la licencia de inspección (*Threat DV*). Se publica un nuevo paquete cada martes del año.

72. La configuración y definición de estos servicios se realiza a través de la creación de los *Protection Profiles:*
    - Para crear un nuevo perfil, ir a *Profiles > Inspection Profiles > New*.
    - Desde el apartado de *search* se pueden buscar los filtros que correspondan a los servicios que se desea proteger. En la búsqueda de filtros se permite definir la criticidad, categoría, estado y tipo.
    - Una vez seleccionado los filtros hacer clic en *Edit > State: Enabled*, y cambiar la acción a realizar por el filtro.
    - Para la definición de la base de datos reputacional seleccionar *Reputation Filter* desde el menú de *Protection Profile > Create New.*
    - Definir la acción a tomar cuando coincida una de las acciones seleccionadas. Es posible habilitar filtros reputacionales para direcciones IPv4/v6, Dominios DNS y URL's. Posteriormente se debe definir el servicio reputacional correspondiente. Por defecto se recomienda activar *Reputation DV Score* para toda reputación igual o superior a 80.
73. El detalle de configuración de los Perfiles se puede consultar en el apartado *Profiles* de la guía *User Guide – REF1*. Adicionalmente se dispone de los siguientes enlaces con información adicional:

    https://docs.trendmicro.com/all/tip/sms/v5.5.3/en-us/sms_urlrep_filter_dg.pdf
74. Los IPS de *Tipping Point* pueden trabajar en dos modos: IDS e IPS.
    - IPS – *Inline mode*: el tráfico debe pasar por el dispositivo para realizar la labor de IPS.
    - IDS – mediante *Port Mirror* o *TAP device*": Se envía una copia del tráfico para ser analizado por *Tipping point*. En circunstancias especiales en las que no sea posible una implementación en línea, el IPS se puede implementar fuera de línea, utilizando un puerto SPAN. Sin embargo, se debe tener cuidado para configurar el puerto SPAN correctamente, ya que es muy fácil sobre dimensionar un enlace, lo que provoca la pérdida de paquetes.

  - Al implementar en un puerto SPAN, tener en cuenta que solo se debe conectar una conexión SPAN por segmento.
  - Se recomienda que el "Modo IDS" esté habilitado en la configuración del dispositivo.

- Para configurarlo ir a la sección de configuración del SMS Dispositivos -> [nombre_dispositivo] -> Configuración del dispositivo -> [hacer clic en Editar] -> Configuración de TSE.

6. FASE DE OPERACIÓN

75. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

- El producto debe contar con las últimas actualizaciones de seguridad para preservar al mismo de amenazas y vulnerabilidades conocidas.
- Se deben mantener y analizar los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- Se deben gestionar correctamente los certificados utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
- Se deben realizar copias de seguridad de manera periódica.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad de la descarga	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de usuarios	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
Configuración del banner de acceso	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Configuración de servicios no empleados	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Deshabilitación de los protocolos no seguros	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
SINCRONIZACIÓN			
Configuración de un servidor de hora NTP	☐	☐	
SNMP			
Configuración de la v3 de SNMP en caso necesario	☐	☐	
COPIAS DE SEGURIDAD			
Creación de los *backups*	☐	☐	
AUDITORÍA			
Configuración del envío de los logs a un servidor Syslog	☐	☐	

8. REFERENCIAS

REF1 *User Guide*
https://docs.trendmicro.com/all/tip/sms/v5.4.0/en-us/sms_5.4.0_ug.pdf

REF2 vSMS Getting Started Guide
https://docs.trendmicro.com/all/tip/sms/v5.4.0/en-us/vsms_5.4_ug.pdf

9. ABREVIATURAS

CA	*Certification Authority*
CLI	*Command Line Interface*
CPD	Centro de Procesado de Datos
CSR	*Certificate Signing Request*
DB	*DataBase*
DNS	*Domain Name Service*
DV	*Digital Vacine*
ENS	Esquema Nacional de Seguridad.
HTTPS	*HyperText Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
LSM	*Local Security Manager*
NGIPS	*New Generation Intrusion Prevention System*
NTP	*Network Time Protocol*
SMS	*Security Management system*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TMC	*Threat Management Center*
TLS	*Transport Layer Security*
TPS	*Threat Protection System*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL