centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo C.4-M: Herramientas de *Sandbox*

Enero 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.02.13 17:38:31 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: enero 2020

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 Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de ***Herramientas de Sandbox*** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el **Esquema Nacional de Seguridad (ENS) para categoría MEDIA**. Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia de ***Herramientas de Sandbox*** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

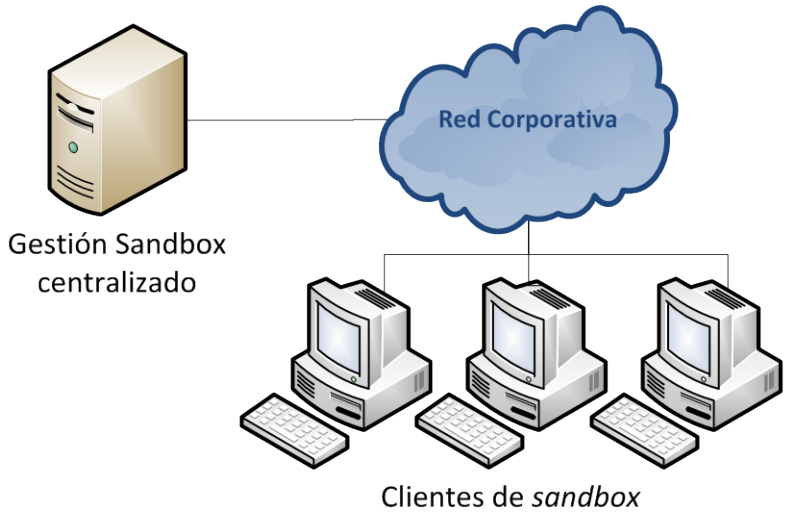
6. Las herramientas de S*andbox* están orientados a la ejecución de aplicaciones en entornos virtuales aislados y controlados, principalmente para el análisis y detección de *malware*.
7. Permiten la ejecución de programas sin que la plataforma en la que se ha desplegado la herramienta de *Sandbox* se vea afectada.

2.2 CASOS DE USO

8. Se contemplan dos (2) casos de uso.

2.2.1. CASO DE USO 1 – GESTIÓN CENTRALIZADA

9. Se realiza una gestión centralizada, que permite monitorizar, gestionar y controlar las instancias de *sandbox* almacenadas en un servidor cuya petición de creación es lanzada desde equipos cliente de diversa índole.



2.2.2. CASO DE USO 2 – GESTIÓN INDIVIDUALIZADA

10. La gestión, monitorización y control de los entornos virtuales de *sandbox* es realizada de forma autónoma en cada equipo.

2.3 ENTORNO DE USO

11. Este tipo de dispositivos son de uso generalizado en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, que busque disponer de capacidad de análisis de *malware* o de mecanismos de protección con un nivel alto de madurez.

12. Para la utilización en condiciones óptimas de seguridad de las herramientas de *sandbox*, es necesaria su integración en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Acceso:** El producto tiene acceso todos los datos del sistema necesarios para llevar a cabo todas sus funciones.
    - **Administración confiable**: El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará altamente capacitada y carecerá de cualquier intención dañina al administrar los dispositivos. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.
    - **Actualizaciones periódicas**: El *firmware* y el *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos son herramientas que suelen presentarse en formato de *software* que se instala en un sistema de ficheros proporcionado por un sistema operativo. Se ejecuta en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.5 CERTIFICACIÓN LINCE

14. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría Media, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, evaluados considerando el problema de seguridad definido en el presente documento.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

15. Los recursos que deben protegerse mediante el uso de estos productos son:

    - **AC.Comunicación**. Comunicaciones del producto.
    - **AC.Datos**. Información contenida en la plataforma sobre la que se instala y ejecuta el producto.
    - **AC.Actualizaciones**. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

16. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    - **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red entre la plataforma en la que se instala y ejecuta el producto y otras entidades autorizadas a acceder a sus comunicaciones.
    - **A.LOCAL. Ataque local.** Un atacante puede actuar a través de *software* no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
    - **A.REST. Acceso a información almacenada.** Un atacante podía acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
    - **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
    - **A.MAL. Malware**. Un agente dañino podría intentar introducir un virus vía red o medios removibles que comprometa el sistema.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

17. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia para categoría ENS Media.

4.1 CANALES DE COMUNICACIÓN CONFIABLE

18. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
19. **COM. 1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas (auditoría, administración, etc.) o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).
20. **COM.2** El producto debe permitir comunicaciones, a través de canales seguros, iniciadas por sí mismo o por entidades autorizadas.
21. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.2 REQUISITOS CRIPTOGRÁFICOS

22. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
23. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
24. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.3 ADMINISTRACIÓN CONFIABLE

25. Estas funcionalidades de seguridad mitigan la amenaza (A. REST).
26. **ADM.1** El producto debe definir al menos el rol de administrador y ser capaz de asociar usuarios a roles.
27. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades del producto:
    - Administración de producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - Otros parámetros de configuración del producto.

28. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas.

4.4 IDENTIFICACIÓN Y AUTENTICACIÓN

29. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
30. **IAU.1** El producto debe identificar y autenticar a cada usuario antes de permitir acciones que modifiquen la configuración del producto.
31. **IAU.2** El producto debe implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
32. **IAU.3** El producto debe proteger de lectura y modificación no autorizada las credenciales de autenticación, claves o información sobre las claves.
33. **IAU.4** El producto debe disponer de la capacidad de gestión de las contraseñas:
    a) La contraseña debe poder configurarse con una longitud mínima o igual a 9 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
34. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE

35. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
36. **ACT.1** El producto debe ofrecer la posibilidad de consultar la versión actual del *firmware/software*.
37. **ACT.2** El producto deberá ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de firmware/software antes de instalarlas.
38. **ACT.3** La actualización del firmware/software se permitirá únicamente a usuarios con rol de administrador.
39. **ACT.4** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual y de comprobar si existen nuevas actualizaciones disponibles.

4.6 AUDITORÍA

40. Esta funcionalidad de seguridad mitiga la amenaza (A.NODET).

41. **AUD.1** El producto debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) *Login* y *logout* de usuarios registrados.
    b) Cambios en la configuración del producto.
    c) Generación, importación, cambio o eliminación de claves criptográficas.
    d) Otros eventos relacionados con la funcionalidad de seguridad del sistema.
42. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica).
43. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: Sólo usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: Administradores.
44. **AUD.4** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo.
45. **AUD.5** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.7 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

1. Esta funcionalidad de seguridad mitiga la amenaza (A.RED) y (A.LOCAL).
2. **PRO.1** El producto deberá ser capaz de realizar un test (durante el arranque o encendido del producto, periódicamente durante la operación normal del producto y a petición de un usuario autorizado) para demostrar el funcionamiento correcto del producto determinado previamente.

4.8 SANDBOX

3. Esta funcionalidad de seguridad mitiga la amenaza (A.MAL).
4. **SAN.1** El producto hará uso de un entorno aislado y seguro (*sandbox*) para llevar a cabo un análisis detallado de los objetos analizados, proporcionando información adicional al administrador o a otra herramienta que lleve a cabo las decisiones necesarias para mitigar una posible amenaza.
5. **SAN.2** El entorno aislado y seguro que utiliza el producto para realizar un análisis en profundidad de una posible amenaza debe disponer de las medidas de protección necesarias para garantizar que la ejecución/análisis detallado no

suponga un riesgo en sí mismo para la ejecución normal del producto, así como para el sistema en el que se encuentre desplegado.

6. **SAND.3** Los informes generados por el producto dispondrán de las medidas de protección necesarias para evitar cualquier tipo de fallo en la integridad de la información que genera y comunica a un administrador o a otra herramienta.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
TLS	*Transport Layer Security*