GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
CENTRO CRIPTOLÓGICO NACIONAL

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo F5: Copias de seguridad

Julio 2018

Edita:

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2018.07.10 12:17:35 +02'00'

NIPO: 785-18-034-0.
Publicación incluida en el programa editorial del suprimido Ministerio de la Presidencia y para la Administraciones Territoriales (de acuerdo con la reestructuración ministerial establecida por Real Decreto 355/2018, de 6 de junio).

Fecha de Edición: julio 2018
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de **Copias de Seguridad** 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). 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 **Copias de Seguridad** 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. Los productos asociados a esta familia se utilizan para realizar copias de seguridad, no solo de información contenida en dispositivos de almacenamiento sino también de sistemas o plataformas completos. La realización de copias de seguridad periódicas constituye una parte esencial de la política de seguridad que cualquier administrador de sistemas debe tener en cuenta.
7. Antes de implementar un sistema de copias de seguridad, es necesario haber definido una **política de copias de seguridad**, para lo que deberán tenerse en cuenta las distintas limitaciones que imponen los recursos y la tecnología disponibles (velocidad, capacidad de almacenamiento, etc.), aspectos que serán determinantes a la hora de elegir y configurar las herramientas.
8. Toda política de copias de seguridad deberá definir, entre otras cosas:
    a) **Qué** necesito replicar, cuales son los datos críticos en mi sistema que no debo perder.
    b) **Cuándo** debo realizar la copia. Para ello, deberán tenerse en cuenta parámetros como el tiempo que tarda en realizarse una copia de seguridad, cuánto varían mis datos a lo largo del tiempo, cual es el máximo coste por pérdida de datos que puedo asumir y cuál es el coste de almacenamiento, y encontrar un compromiso entre ellos.
    c) **Dónde** debo guardar mis copias y **hasta cuándo**. A la hora de definir donde se guardan las copias de seguridad, una buena práctica consiste en mover periódicamente una copia completa de los datos fuera del sistema, de cara a protegerlas de posibles fallos de hardware, robos de información y otras amenazas. Esto es bastante habitual cuando el soporte físico es en cinta y a día de hoy se utiliza cada vez más el almacenamiento cifrado en la nube.
9. Además, es importante tener en cuenta que los datos son guardados para poder ser restaurados ante una pérdida de datos del sistema principal. Por ello, a la hora de elegir nuestro sistema, es necesario tener en cuenta el tiempo máximo que el servicio puede estar caído o RTO (*Recovery Time Objective*) y el tiempo máximo que se pueden perder los datos de un servicio RPO (*Recovery Point Objective*).

2.2 CASOS DE USO

10. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1 – BACKUP EN RED PRIVADA

11. En este caso todas las copias de seguridad se guardan en dispositivos de almacenamiento que pertenecen y se gestionan desde la misma red de la empresa u organismo al que pertenecen los datos.

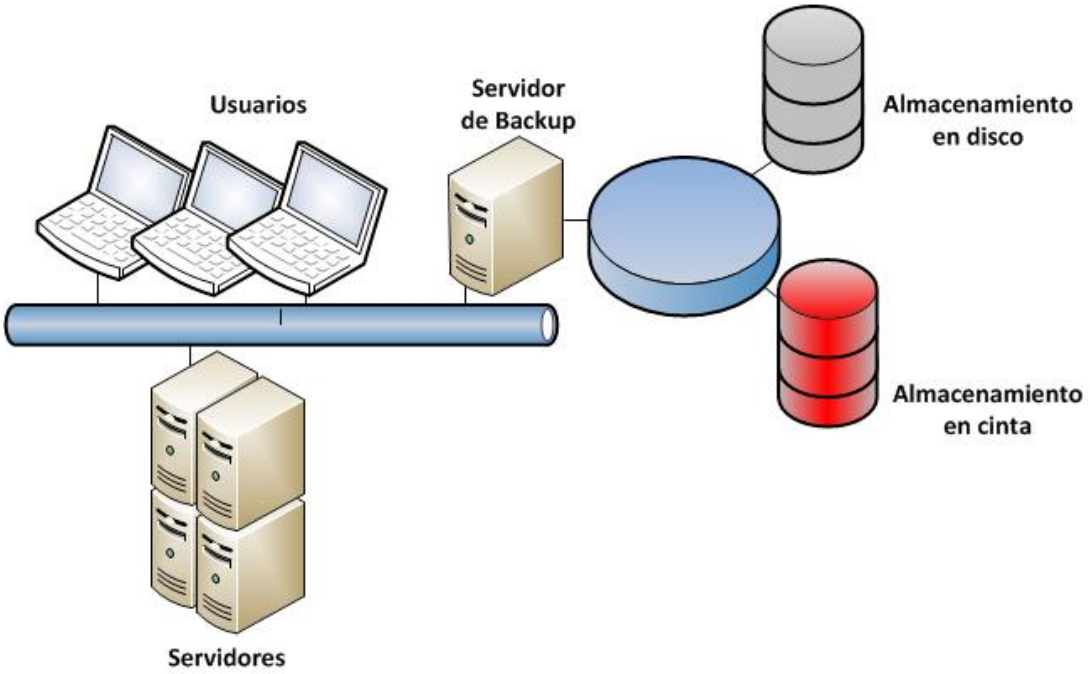

Figura 1-Caso de uso 1-Ejemplo de esquema de almacenamiento en red

2.2.2. CASO DE USO 2- BACKUP EN LA NUBE

12. En este caso las copias de seguridad se guardan en dispositivos de almacenamiento que pertenecen y se gestionan desde una red externa a la empresa u organismo al que pertenecen los datos.
13. Este caso de uso es compatible con el anterior, siendo una funcionalidad añadida que se explota en determinados entornos con la intención de optimizar los recursos de almacenamiento y flexibilizar el acceso a las copias de seguridad.

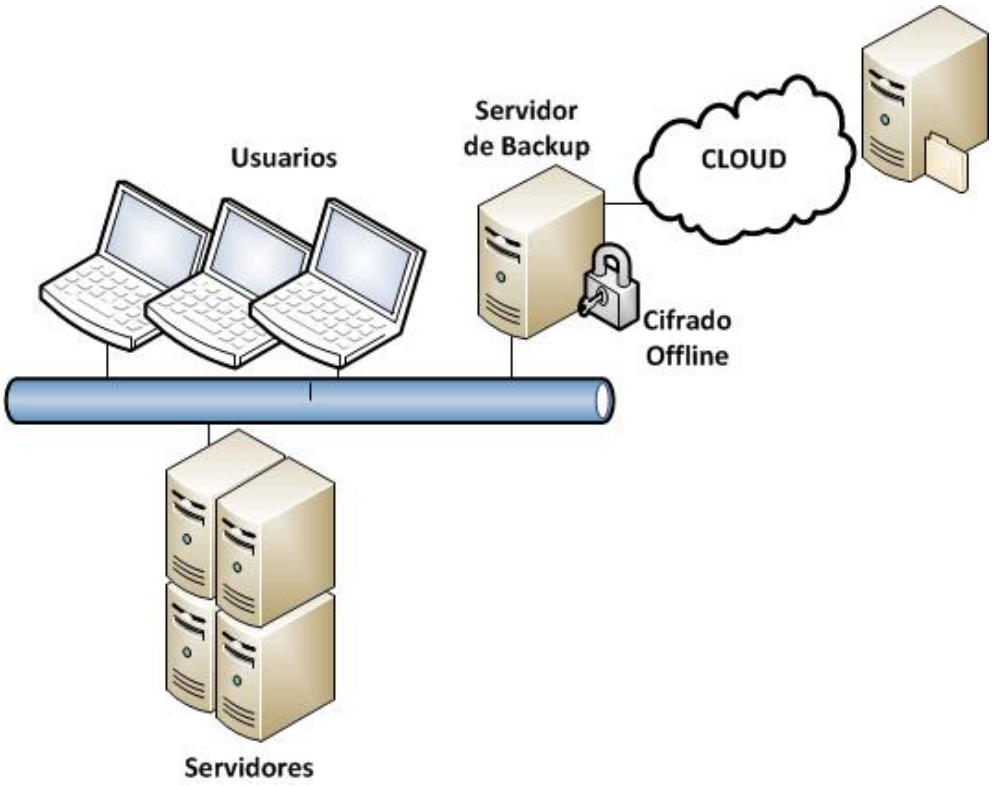

Figura 1 – Caso de Uso 2-Ejemplo de esquema de almacenamiento en nube.

2.3 ENTORNO DE USO

14. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física**: El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **Administración confiable**: El 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 capacitada, formada y carecerá de cualquier intención dañina.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

15. Podrán tenerse en cuenta los siguientes tipos de herramientas de *backup*:
16. **Herramientas de sincronización**. Son herramientas que duplican el contenido de una serie de directorios. Los directorios de *backup* podrán situarse en la misma máquina o en máquinas distintas.
17. **Copias**. Son herramientas que realizan copias periódicas de una serie de archivos en un espacio aparte, específicamente diseñado para ello.

18. **Instantáneas *(Snapshots)***. Las instantáneas son copias de todo un sistema o parte de un sistema que permiten recuperarlo en un estado que se sabe que es correcto. Pueden duplicarse sistemas de ficheros, máquinas virtuales, volumen de disco, etc.
19. ***Continuous data protection*.** Son herramientas que guardan automáticamente una copia de todas las modificaciones que se realizan en los datos, manteniendo una copia de un número de versiones determinado por la política de seguridad..

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

20. El estándar Common Criteria (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
21. El nivel de confianza EAL (Evaluation Assurance Level) conforme a CC, al que deben ser evaluados los Requisitos Fundamentales de Seguridad descritos en este documento debería ser EAL2 o superior.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

22. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

    - Datos de usuario (copias de seguridad de usuario almacenadas dentro del propio producto e información relativa a éstas).
    - Datos de configuración del producto y de auditoría generados por éste.
    - Material criptográfico.

3.2 AMENAZAS

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

    - **Compromiso de datos de usuario** (copias de seguridad de usuario almacenadas dentro del propio producto e información relativa a éstas). Un atacante recupera, accede o modifica datos de usuario guardados en la plataforma y protegidos por ésta.
    - **Compromiso de la funcionalidad del dispositivo**: Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad y la modifica o la desactiva de manera no conforme a las políticas de seguridad (p.ej. instalación de actualizaciones maliciosas o administración no autorizada del producto).
    - **Compromiso de material criptográfico.** Un usuario del sistema (no legitimado para estas acciones) o atacante consulta o modifica el material criptográfico almacenado y gestionado por el producto. Esto incluye la posible modificación de los mecanismos criptográficos.
    - **Canales de comunicación inseguros**. Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
    - **Cifrado débil**: Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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.

4.1 REQUISITOS CRIPTOGRÁFICOS

25. **REQ. 1** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).
26. **REQ. 2** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[1]) determinísticos, el producto deberá:
    - Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
    - Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.
27. **REQ. 3** Algoritmos HASH. Las funciones resumen o HASH que utilice el producto deberán utilizar los algoritmos SHA-2[2] y SHA-3 de longitud mayor o igual a 256.
28. **REQ. 4** Firma digital. Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:
    - *Digital Signature Algorithm* (DSA) con una longitud de clave de 3072 bits o superior.
    - *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
    - RSA con una longitud de clave de 3072 o superior.
29. **REQ. 5** Cifrado de datos y claves con AES[3]. El producto implementará cifrado de datos de acuerdo con el algoritmo AES los modos CBC[4], GCM[5], CTR[6], CCM[7] O XTS (para cifrado de disco) y longitud de claves 128 bits o superior.

[1] *Random Bit Generator*
[2] *Secure Hash Algorithm*
[3] *Advanced Encryption Standard*
[4] *Cipher Block Chaining*
[5] *Galois/Counter Mode*
[6] Counter mode
[7] Counter with CBC-MAC

30. **REQ. 6** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar:
    - HMAC-SHA-2 o HMAC-SHA-1[8].
    - AES-XCBC-MAC-96, AES-XCBC-MAC-128.
    - CMAC-AES-96, CMAC-AES-128.
    - GMAC-AES-128.
31. **REQ. 7** El producto deberá implementar los siguientes métodos de borrado de claves:
    - Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
        - Un patrón de sobrescritura de una pasada utilizando un patrón pseudoaleatorio generado por el RBG del producto, ceros, unos, un nuevo valor de clave o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        - Apagado de la alimentación de la memoria.
        - Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.
    - Para memoria no volátil:
        - Que emplee un algoritmo de *wear-leveling*[9], la destrucción deberá consistir en alguno de los siguientes métodos:
            1. Un patrón de sobrescritura de una pasada consistente en ceros, unos, un nuevo valor de clave de la misma longitud o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
            2. Borrado de bloque.
        - Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:
            1. Una o más pasadas de sobrescritura consistente en ceros seguidos de una lectura de verificación.
            2. Una o varias pasadas de sobrescritura consistente en todos unos seguidos de una lectura de verificación, sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una lectura de verificación.
            3. Una o varias pasadas de sobrescritura consistente en algún valor que no contenga ningún CSP seguidos de una

[8]Solamente para el caso de autenticación de mensajes con HMAC se permitirá el uso de SHA-1.
[9]Algoritmos de nivelación del desgaste que se utilizan para prolongar la vida útil de algunos dispositivos de memoria

verificación de lectura, sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una verificación de lectura.

4. Borrado de bloque.

Y si la lectura de verificación de los datos sobrescritos falla, el proceso deberá ser repetido de nuevo hasta un número mayor que cero de intentos en el cual se devuelva un error.

32. **REQ. 8** Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.

4.2 AUDITORÍA Y REGISTROS DE SEGURIDAD

33. **REQ. 9** Por cada evento auditable, el producto generará un registro de auditoría que contenga, como mínimo, la siguiente información:
    a) Tipo de evento.
    b) Resultado del evento.
    c) Hora y fecha.
    d) Identidad del usuario, en los casos en los que el evento sea producido por un usuario.
34. **REQ. 10** Se generará un registro de auditoría, al menos en los siguientes casos:
    a) Inicio y finalización de las funciones de *backup*.
    b) Cambios en las políticas de *backup*. (Creación, modificación, eliminación…)
35. **REQ. 11** La gestión de los registros (modificación, borrado) sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de auditor/administrador del sistema).
36. **REQ. 12** En el caso de que permita almacenamiento remoto de los registros de auditoría, el producto deberá utilizar los protocolos IPsec, TLS (1.2 o 1.3) o TLS/HTTPS para establecer un canal de comunicaciones seguro con la entidad remota.

4.3 IDENTIFICACIÓN Y AUTENTICACIÓN

37. **REQ. 13** La gestión de usuarios, incluyendo su creación y asignación de privilegios, así como la baja o supresión de aquellos, sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador).
38. **REQ. 14** El producto implementará políticas de control de acceso basadas en roles de usuario, grupos, identificadores de usuario y permisos de usuario, de

forma que solo se permita el acceso a un objeto controlado si el usuario es administrador o tiene permisos de acceso.

39. **REQ. 15** El producto requerirá un proceso de autenticación e identificación positivo previo a la realización de cualquier tarea.

4.4 ADMINISTRACIÓN DEL PRODUCTO

40. **REQ. 16** El producto presentará al menos dos tipos de perfiles: administradores del Sistema y usuarios, a los que se asociarán diferentes permisos.
41. **REQ. 17** La administración del producto y los datos de usuario sólo podrá ser realizada por un perfil de usuario privilegiado (p.ej.: rol de administrador).
42. **REQ. 18** En el caso de que permita administración remota, el producto deberá utilizar los protocolos IPsec, TLS/HTTPS o SSH para establecer un canal de comunicaciones seguro.

4.5 PROTECCIÓN DE LA FUNCIONALIDAD DE SEGURIDAD DEL PRODUCTO Y LOS DATOS DE USUARIO

43. **REQ. 19** El producto será capaz de generar sellos de tiempo fiables que utilizará en sus operaciones. Para ello podrá servirse de las actualizaciones de reloj generadas de un servidor NTP.

5. REQUISITOS OPERATIVOS ADICIONALES

44. Los requisitos que se describen a continuación, si bien no se incluyen en la certificación del producto deberán ser tenidos en cuenta a la hora de elaborar los procedimientos de empleo seguro:

45. **REQ OP. 20.** En el caso de los datos de *backup* se guarden en una nube pública o que pertenezca a otro sistema con una categoría de seguridad inferior, éstos deberán enviarse cifrados, utilizando para ello un dispositivo de cifrado offline que cumpla los requisitos establecidos para la familia de productos cifrado offline..

46. **REQ OP. 2.** En ningún caso deberá guardarse claves de cifrado o parámetros sensibles de seguridad del sistema en la nube.

47. **REQ OP. 3.** En el caso de que el producto permita administración remota, ésta deberá realizarse desde el interior de la red o sistema al que pertenezca o del que dependa.

6. ABREVIATURAS

AES	*Advanced Encryption Standard*
CBC	*Cipher Block Chaining*
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
GCM	*Galois/Counter Mode*
HTTPS	*Hypertext Transfer Protocol Secure*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
NTP	*Network Time Protocol*
RBG	*Random Bit Generator*
RFS	Requisitos Fundamentales de Seguridad
SHA	*Secure Hash Algorithm*
SSH	*Secure Shell*
TLS	*Transport Layer Security*