centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.10-M: Hiperconvergencia

Agosto 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
2020.08.10 09:40:50 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto 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 **Hiperconvergencia** 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 para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS), 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 **Hiperconvergencia** 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. La **infraestructura hiperconvergente (HCI)** es un enfoque de arquitectura basada en *software*, que proporciona recursos de almacenamiento, cómputo y redes de forma transparente al *hardware* que se utilice, con grandes capacidades de escalado horizontal y todo ello gestionado desde un único punto centralizado.
7. En general se trata de productos *software* que gestionan una infraestructura *hardware* estándar. Pero también hay algunos productos que se presentan en *formato appliance* con un *hardware* específico y con el *software* de hiperconvergencia integrado.
8. Los productos de hiperconvergencia integran, por lo tanto, las capacidades de cómputo, de almacenamiento y de red en una misma capa de funcionamiento, centralizando todas las tareas de gestión propias de los centros de datos, a nivel *software*.
9. Estos productos se despliegan empleando nodos que consisten en servidores que combinan capacidades de procesamiento, memoria y almacenamiento. Los nodos permiten una extensión y gestión simplificada del almacenamiento disponible en la infraestructura. En caso de que se desee aumentar los recursos disponibles, únicamente será necesario añadir un nuevo nodo a la infraestructura (escalado horizontal).
10. Estos productos proporcionan alta disponibilidad, por lo que en caso de que cualquiera de sus componentes falle (nodos, procesadores, discos, etc.), la infraestructura hiperconvergente permite que los servicios continúen proporcionándose sin pérdida de datos o funcionalidad. Para ello se utilizan los siguientes mecanismos:
    - Monitorización continua de los componentes de la infraestructura.
    - Monitorización continua del estado de las Máquinas Virtuales.
    - *Backups* locales y remotos de las Máquinas Virtuales y de sus almacenes de datos.
    - Configuraciones de alta disponibilidad (*high availability*).
11. También proporcionan mecanismos de protección de los datos almacenados:
    - Monitorización continua de la integridad de los datos. En caso de que se detecte un fallo en la integridad, estos productos ofrecen mecanismos para poder recuperar la información.
    - En algunos casos, permiten cifrado de los datos almacenados (at *rest*) cuando sean datos sensibles cuya confidencialidad debe ser protegida.

- Borrado seguro, haciendo irrecuperables los datos tras el borrado. Sólo podrán recuperarse en caso de regresar al estado anterior o al backup de las máquinas virtuales.

12. Otra de las ventajas que ofrecen estos productos es un único punto de gestión y control. Permiten que las operaciones de gestión y control sobre la infraestructura y los servicios disponibles, sean gestionadas desde un único panel de control.
13. Estos productos ofrecen mecanismos de control de acceso de terceras partes a los recursos ofrecidos por la infraestructura. Por ejemplo, listas blancas de aplicaciones y servicios que pueden acceder a determinados recursos.
14. Permiten la instalación de nodos en distintas ubicaciones geográficas (distintos CPDs). La información y datos intercambiados entre los distintos CPDs irán protegidos utilizando mecanismos de cifrado y mecanismos que aseguren que se envían a su auténtico destino y no a ninguna entidad que intente suplantarlo.
15. Permiten monitorizar y establecer configuraciones automáticas de seguridad, mediante la comparación y evaluación automática de parámetros básicos de seguridad, con estándares y buenas prácticas de la industria.

2.2 CASOS DE USO

16. Dada la naturaleza y el objetivo de este tipo de productos, se contempla un único caso de uso para esta familia tal y como se indica a continuación.

2.2.1. CASO DE USO 1 – DESPLIEGUE COMO CENTRO DE DATOS DEFINIDO POR SOFTWARE (SDDC)

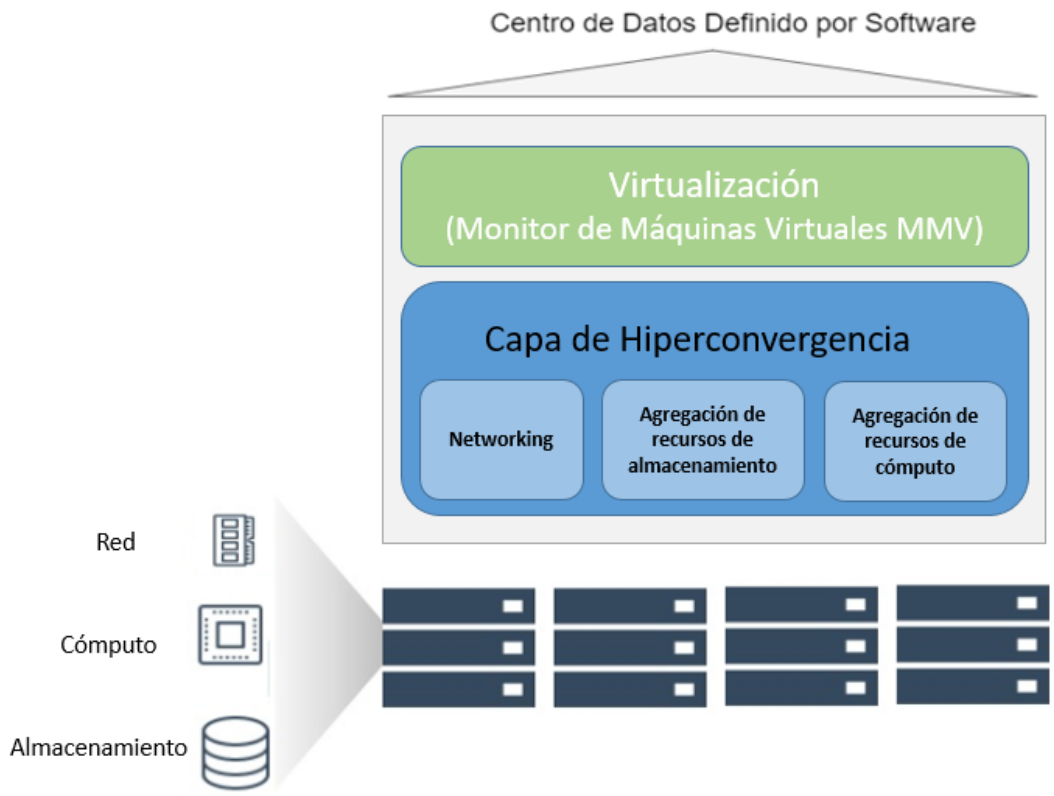

Figura 1: Centro de Datos Definido por *Software*

17. En un Centro de Datos Definido por *Software* toda la infraestructura del CPD ha sido virtualizada y se entrega como servicio.
18. Las funciones de gestión y control se ejercen a **nivel *software***, que ofrece una interfaz única de monitorización y administración, mientras el *hardware* actúa como un banco común de recursos, que son asignados en base a las necesidades y cargas de trabajo.

2.3 ENTORNO DE USO

19. Para la utilización en condiciones óptimas de seguridad de las herramientas de hiperconvergencia, es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física:** Los recursos *hardware* gestionados por la capa de hiperconvergencia, deberán instalarse en áreas 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 al administrar el producto.

- **Integridad de la plataforma**: La plataforma *hardware* no debe haber sido comprometida con anterioridad a la instalación del producto de hiperconvergencia.
- **Actualizaciones periódicas:** El *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

20. Generalmente este tipo de productos se presenta en formato *software*, integrando y gestionando los recursos de computación, de almacenamiento, y red de cualquier hardware estándar.
21. En algunos casos también se puede presentar en formato *appliance* con un *hardware* específico y con el *software* de hiperconvergencia integrado.
22. En ambos casos, el producto puede incorporar la función de Hipervisor o Monitor de Máquinas Virtuales (VMM), o utilizar una solución de terceros.

2.5 CERTIFICACIÓN LINCE

23. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Medio, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
24. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.
25. En caso de estimarse que el esfuerzo de evaluación de los requisitos incluidos en el apartado 4 excede de los días de esfuerzo determinados dentro de la metodología LINCE, se contempla la posibilidad de realizar una Evaluación STIC Complementaria que incluya las pruebas que no han podido ser encajadas en el mencionado periodo.

[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

26. Los recursos que deben protegerse mediante el uso de estos productos incluyen:

- Información almacenada. Deberá protegerse la integridad y la disponibilidad de la información almacenada, permitiendo recuperar la información frente a cualquier fallo, sin pérdida de datos.
- Recursos de la infraestructura, de forma que únicamente usuarios, aplicaciones y servicios autorizados puedan acceder a ellos.
- Servicio ofrecido a la organización, de forma que el fallo de cualquier componente de la infraestructura será transparente a la organización, continuando la operativa del servicio ofrecido.
- Comunicaciones del producto, establecidas entre sus propios componentes o con otras entidades autorizadas.
- Datos de configuración del producto.
- Actualizaciones del producto susceptibles de afectar a la configuración y funcionalidad.

3.2 AMENAZAS

27. 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 el producto y otras entidades autorizadas o modificar 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 sensible 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. SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.

- **A.DISP. Indisponibilidad de la información o servicios.** Un fallo en la infraestructura podría comprometer la disponibilidad de la información almacenada y de los servicios prestados a la organización.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

28. 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.

29. **Los requisitos que se incluyen en los siguientes apartados son los que aplican a la capa de hiperconvergencia del producto. Para aquellos productos que incluyan, además, el componente Hipervisor o Monitor de Máquinas Virtuales (VMM), este componente deberá cumplir los RFS indicados en el Anexo F.7 de la familia Virtualización.**

4.1 AUDITORÍA

30. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET). **Podrán ser cubiertas por el producto o por su entorno operacional.**

31. **AUD.1** El producto deberá 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 personal autorizado.

    b) Cambios en las credenciales de usuarios.

    c) Cambios en la configuración del producto.

    d) Eventos relativos a la funcionalidad del producto.

32. **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).

33. **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: solo Administradores.

34. **AUD.4** El producto deberá ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.

35. **AUD.5** El producto deberá ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

36. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**

37. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.

38. **IAU.2** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
39. **IAU.3** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
40. **IAU.4** El producto deberá 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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
41. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 ADMINISTRACIÓN CONFIABLE

42. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
43. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
44. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - Otros parámetros de configuración del producto.
45. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2).

4.4 CANAL SEGURO

46. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
47. **COM.1.** El producto deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas, o entre las 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.).
48. **COM.2.** El producto debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

49. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
50. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *firmware/software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
51. **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.
52. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

53. Estas funcionalidades de seguridad mitigan la amenaza (A.REST).
54. **CRD.1** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con CIF.1.

4.7 REQUISITOS CRIPTOGRÁFICOS

55. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
56. **CIF.1** El producto permitirá exclusivamente el empleo de protocolos, funciones y algoritmos criptográficos que estén incluidos entre los autorizados para Categoría MEDIA del ENS, de acuerdo con lo establecido en la guía CCN-STIC-807.
57. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 HIPERCONVERGENCIA

58. Esta funcionalidad de seguridad mitiga la amenaza (A.DISP).
59. **HCI.1** El producto deberá mantener la operación de forma segura (es decir, con el mismo nivel de seguridad y sin menoscabo de ninguna de las medidas de seguridad) y generar un mensaje de alerta, cuando se produzca un fallo en el funcionamiento de cualquiera de los componentes gestionados por la capa de hiperconvergencia (disco, nodo, módulo de memoria RAM, procesador, etc.).
60. **HCI.2** El producto deberá poder realizar *tests* y comprobaciones periódicas del correcto funcionamiento de sus diferentes funcionalidades y servicios, así como la integridad de los datos almacenados.

61. **HCI.3** En caso de detectar un fallo en la integridad de la información almacenada, el producto debe generar un mensaje de alerta y ser capaz de recuperar dicha información.

62. **HCI.4** El producto debe ofrecer mecanismos que permitan guardar el estado de datos de una Máquina Virtual en un instante determinado (por ejemplo, mediante *snapshots*). Estos estados, podrán almacenarse localmente y/o remotamente. En caso de ser almacenado remotamente deberá cumplir con los requisitos establecidos en COM.1.

63. **HCI.5** El producto debe ofrecer mecanismos para retroceder a un estado específico de Máquina Virtual, sin pérdida de datos. Debe permitir la recuperación de todas las Máquinas Virtuales, incluso aunque estas y los almacenes de sus datos (*data stores*) hayan sido borrados.

64. **HCI.6** El producto deberá asegurar que cualquier información almacenada en un dispositivo de almacenamiento se volverá inaccesible/irrecuperable antes de la reutilización de dicho dispositivo. Para ello, deberá emplear algún mecanismo de borrado seguro como, por ejemplo, la sobreescritura.

4.9 NOTAS DE APLICACIÓN

65. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente.

    Todos los requisitos indicados en la tabla anterior deberán formar parte de la declaración de seguridad o *Security Target* asociada a la certificación.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
EPP	*Endpoint Protection Platform*
EDR	*Endpoint Detection and Reaction*
HCI	*Hyper-Converged Infrastructure*
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol security
MCF	Revisión de Código Fuente
MEC	Módulo de Evaluación Criptográfica
MMV	Monitor de Máquinas Virtuales
NIAP	*National Information Assurance Partnership*
RAM	*Random Access Memory*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
SSH	*Secure SHell*
TLS	*Transport Layer Security*
TOE	*Target of Evaluation*