centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Noviembre de 2022

MINISTERIO DE DEFENSA

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

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2023.01.03 14:57:06 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

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 y Servicios STIC (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)

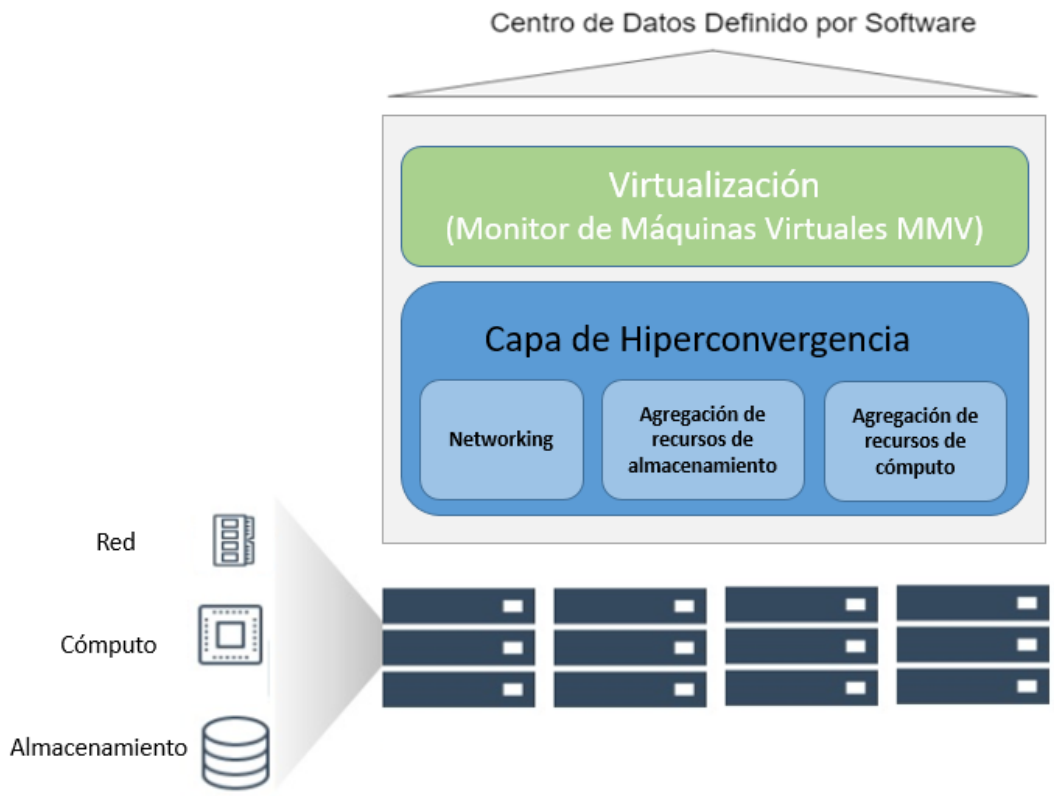

Figura 1: Centro de Datos Definido por *Software*

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 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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.** El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.

- **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *la capa de hiperconvergencia* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **Protección de las credenciales.** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

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

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

Complementaria que incluya las pruebas que no han podido ser encajadas en el mencionado periodo.

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS SENSIBLES A PROTEGER

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

- **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación**: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.
- **AC.PSC**. [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

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

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al 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.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

28. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.DISP
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	X									
IAU.5									X	

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.DISP
COM.1		X	X							
COM.2			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
PSC.1						X				
PRO.1							X			
CIF.1		X	X							
HCI.1										X
HCI.2							X			X
HCI.3										X
HCI.4										X
HCI.5						X				X

4. REQUISITOS DE SEGURIDAD

29. 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.

30. 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.

31. La convención utilizada en las descripciones de los RFS es la siguiente:

    - Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

      RFS: Administración del producto [**selección***: local; remota*]

      DS: Administración del producto local y remota

    - Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

      RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

      DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

32. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

33. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

34. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

    - Administración del producto [**selección**: *local; remota*].
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - [**asignación**: otras funcionalidades administrables del producto].

35. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

36. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

37. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

38. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

39. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.

    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “].

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

40. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

41. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [**selección***: cambio; establecimiento*] de credenciales en el siguiente acceso.

4.3 CANALES SEGUROS

42. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

43. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

44. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

45. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos

[***asignación**: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

4.4 CRIPTOGRAFÍA

46. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
47. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación**: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

48. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].
49. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
50. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 AUDITORÍA

51. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
52. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
    a) Al inicio y finalización de las funciones de auditoría.
    b) *Login* y *logout* de usuarios registrados.
    c) Cambios en las credenciales de usuarios.
    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].
    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].
    f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].

53. **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.

54. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:

    a) Lectura: usuarios autorizados.

    b) Modificación: ningún usuario.

    c) Borrado: [**selección**: solo administradores; ningún usuario]

55. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].

56. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

57. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

5.1 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

58. **PRO.1** El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.8 HIPERCONVERGENCIA

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: [***selección**: disco; nodo; módulo de memoria RAM; procesador; [**asignación**: otros componentes*]].

60. **HCI.2** 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.

61. **HCI.3** 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 [***selección**: localmente; de forma remota]*. En caso de ser almacenado remotamente deberá cumplir con los requisitos establecidos en COM.1.
62. **HCI.4** 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.
63. **HCI.5** 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: [***selección**: sobreescritura; [**asignación**: otros mecanismos]*].

4.9 NOTAS DE APLICACIÓN

64. 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.
65. 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 y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
EDR	*Endpoint Detection and Reaction*
ENS	Esquema Nacional de Seguridad
EPP	*Endpoint Protection Platform*
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*

PUBLICACIONES DE DEFENSA

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