Declaración de Seguridad del producto KATUA SDI Platform para hiperconvergencia.

Cuadro de control de firmas

EDICIÓN	FECHA	ELABORADO	REVISADO	APROBADO
1	17/03/2020	Dep. tecnico KRC Española		
1.0.1	19/11/2020		JMDR	
1.0.2	30/11/2020		JMDR	
1.0.3	21/12/2020		JMDR	JSDA
1.0.4	15/01/2021		JMDR	JSDA
1.0.5	18/01/2021		JMDR	JSDA
1.0.6	25/01/2021		JMDR	JSDA
1.0.7	28/01/2021		JMDR	JSDA
1.0.8	28/01/2021		JMDR	JSDA
1.0.9	26/02/2021		JMDR	JSDA
1.0.10	11/03/2021		JMDR	JSDA
1.0.11	24/03/2021		JMDR	JSDA
1.0.12	24/03/2021		JMDR	JSDA
1.0.13	05/04/2021		JMDR	JSDA
1.0.14	27/04/2021		JMDR	JSDA
1.0.15	02/06/2021		JMDR	JSDA
1.0.16	26/07/2021		JMDR	JSDA

Tabla de contenido

1. INTRODUCCIÓN

El presente documento es la Declaración de Seguridad para Hiperconvergencia (HCI), una solución de hiperconvergencia. En el mismo se abordarán los siguientes puntos:

1. Información acerca de este documento
2. Descripción de la funcionalidad de la solución y casos de uso, que permite a las organizaciones o servicios públicos hacer frente a las amenazas y riesgos que se describen en el documento.
3. Descripción del entorno de ejecución
4. Análisis de amenaza y riesgos de los dispositivos móviles.
5. Requisitos fundamentales de seguridad que esta solución cubre y cómo los cubre para implementar cada función de seguridad.

1.1. INFORMACIÓN DEL PATROCINADOR, TOE Y EVALUACIÓN

Datos del Patrocinador (Nombre y Dirección)	KRC ESPAÑOLA S.A. C/BARBASTRO 5, LOCAL, 28022
Datos del Desarrollador (Nombre y Dirección)	KRC ESPAÑOLA S.A. C/BARBASTRO 5, LOCAL, 28022
Datos de contacto del Desarrollador (Nombre de contacto y e-mail)	JULIA SAGASTUME info@krc.es
Nombre del TOE	KATUA SDI PLATFORM
Versión del TOE	1.0.6
Hash de versión	d728352d025bce56fb06c19bd1e8e68debdb682259ce93b38cdeca2a47728619
Tipo de evaluación (incluir los módulos opcionales)	LINCE + MEC
Manuales de uso del producto y su versión	La documentación de instalación y configuración hay que solicitarla al fabricante y se proporcionará al usuario a demanda.
Taxonomía del producto según CCN-STIC-140	HIPERCONVERGENCIA

1.2. METODOLOGÍA Y CRITERIOS DE EVALUACIÓN

CCN-STIC-2001	CCN-STIC-2001 – Definición de la Certificación Nacional Esencial de Seguridad

CCN-STIC-2002	CCN-STIC-2002 – Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad

2. DESCRIPCIÓN DEL TOE

2.1. DESCRIPCIÓN FUNCIONAL DEL TOE

El TOE propuesto consiste en una solución hiperconvergente, donde todos los elementos necesarios para el uso del sistema se encuentran unificado en un solo nodo. La configuración propuesta permite el despliegue de todos los servicios necesarios para la implementación.

Las funcionalidades esenciales del TOE son:

- Gestión centralizada del nodo a través de un dashboard web desde donde se controlan todas las operaciones de administración, gestión de recursos y seguridad. Desde este dashboard se pueden realizar las siguientes operaciones:
    - Gestión de usuarios, grupos y proyectos (conjuntos de recursos)
    - Gestión de instancias de máquinas virtuales
    - Gestión de imágenes de máquinas virtuales
    - Gestión del almacenamiento persistente y efímero
    - Gestión de snapshots de las instancias de máquinas virtuales.
    - Gestión de las topologías de red definidas por software
    - Gestión de los grupos de seguridad (firewall)
- Seguridad de acceso centralizada para todos los servicios que conforman el TOE.
- TOE securizado, implementando los scripts publicados con el CCN-CERT para sistemas ENS en entornos CentOS CCN-STIC-619
- Orquestador WSGI de todos los servicios, interconectando los “endpoints” de cada uno de ellos mediante el uso de TLS/SSL.
- Hardware publicado en guía CCN-104 para catalogación zoning referencia 2018-224

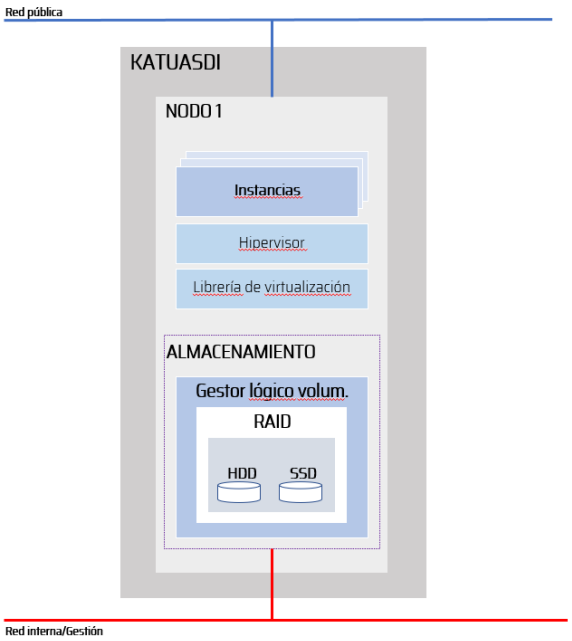
El hardware que forma parte del TOE se basa en el equipo SEG-2 de KRC Española al encontrarse publicado en la guía CCN-STIC-104 para zoning. Las características básicas del hardware son:

- Procesador Intel Xeon Scale
- 32 GB RAM
- Sistema RAID Hardware configurado con 1 unidad lógica conformada por tres discos físicos.
- 4 conexiones de red 1Gbe
- 1 conexión IPMI 100Mb
- 1 conexión de red en FO 100/1000

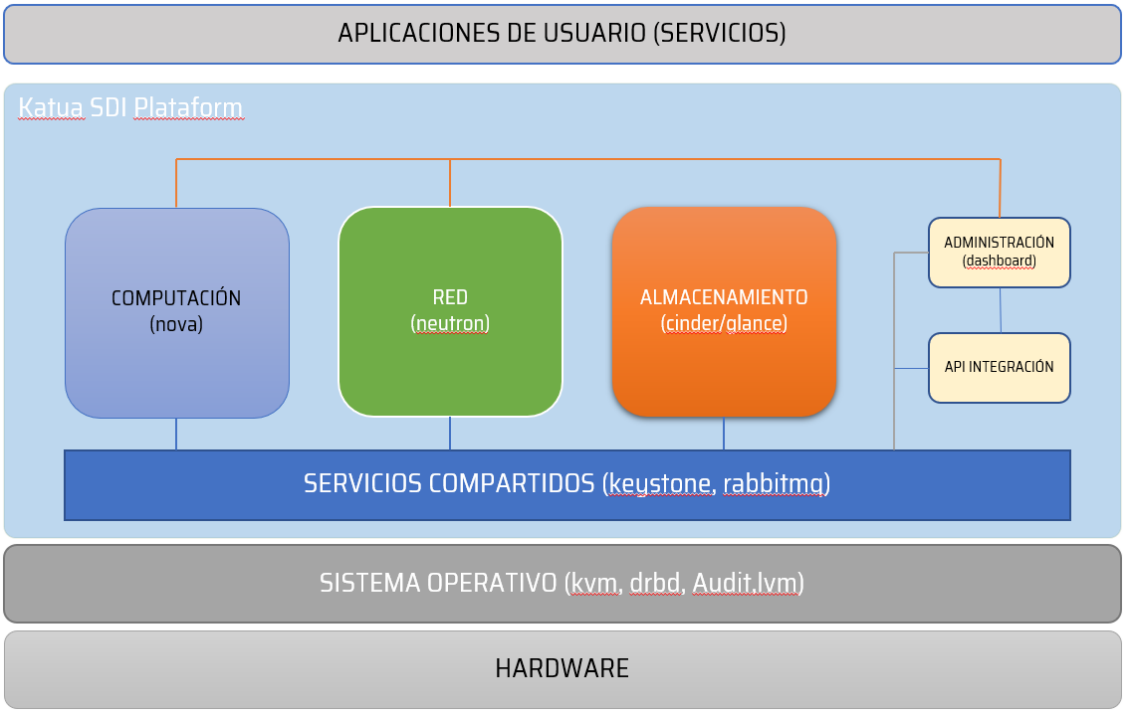
No entran dentro del ámbito de esta evaluación los siguientes elementos:

- Herramienta hipervisora KVM
- Sistema de replicación de bloques DRBD

La descripción gráfica del sistema completo sería la siguiente:



Más detalladamente, en el siguiente gráfico se muestra el TOE separado del entorno operacional y los componentes que lo forman:



Como ya se ha indicado, queda **fuera de la evaluación** el hipervisor KVM y el sistema de replicación de bloques DRBD.

2.2. IDENTIFICACIÓN DE LAS GUÍAS DE USO, INSTALACIÓN Y CONFIGURACIÓN SEGURAS DEL TOE

Nombre	Versión	Fecha emisión
Manual de Usuario	1.0.5	21/04/2021
Manual de Usuario CLI	1.0	01/01/2020

2.3. DESCRIPCIÓN DEL MODO DE USO DEL TOE

El TOE no requiere que se realice ninguna configuración previa o forma de uso especial para obtener las funciones de seguridad descritas en el apartado 5 del presente documento.

La evaluación se realizará conforme al TOE especificado, quedando fuera del ámbito de la misma las conexiones de cualquier tipo a almacenamientos externos de la configuración propuesta.

3. ENTORNO DE EJECUCIÓN

3.1. DESCRIPCIÓN DEL ENTORNO DE EJECUCIÓN

El entorno necesario para la ejecución del TOE lo confirman el hipervisor KVM, las instancias que se despliegan y las conexiones de red necesarias.

Como ya se indicó en el apartado 2.1, la herramienta utiliza como hipervisor el software KVM. Esta herramienta queda **fuera del ámbito** de la evaluación.

4. PROBLEMA DE SEGURIDAD

4.1. HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

En este apartado se incluyen las hipótesis sobre el entorno en el que se ejecutará el producto.

Código	Descripción
Actualizaciones periódicas	El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
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.
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.

4.2. ACTIVOS SENSIBLES A PROTEGER

En esta sección se describen los activos que las funciones de seguridad del TOE protegen.

Código	Descripción
AC. Actualizaciones	Actualizaciones del producto susceptibles de afectar a la configuración y funcionalidad. Se protege la integridad y autenticidad de las actualizaciones en cuanto a configuración y funcionalidad.
AC. Comunicaciones	Comunicaciones del producto, establecidas entre sus propios componentes o con otras entidades autorizadas.

	Las dimensiones de seguridad aplicables a la protección de este activo son la confidencialidad, integridad y disponibilidad.
AC. Datos de configuración	Datos de configuración del producto. Se protege la confidencialidad y la integridad de estos datos.
AC. 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. Se protege la integridad y la disponibilidad de esta información.
AC. Recursos de la infraestructura	Únicamente usuarios, aplicaciones y servicios autorizados puedan acceder a ellos. Se protege la confidencialidad y la integridad de este activo.
AC. Servicio ofrecido a la organización	El fallo de cualquier componente de la infraestructura será transparente a la organización, continuando la operativa del servicio ofrecido. Las dimensiones de seguridad aplicables a la protección de este activo son la integridad y la disponibilidad.

4.3. DESCRIPCIÓN DE LAS AMENAZAS

En esta sección se describen las amenazas mitigadas por las funciones de seguridad del TOE.

Actor	Acción Adversa	Activos afectados	Descripción
Atacante externo	A.RED. Ataque a la red	AC. Actualizaciones AC. Comunicaciones	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.
Usuario Malintencionado	A. LOCAL. Ataque Local	AC. Comunicaciones AC. Datos de configuración	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.
Usuario autorizado	A. REST. Acceso a información sensible almacenada	AC. Actualizaciones AC. Datos de Configuración	Un atacante podía acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
Usuario autorizado	A. NODET. Actividad no detectada	AC. Datos de Configuración	Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
Usuario autorizado	A. SEG. Acceso a las funciones de seguridad	AC. Recursos de la Infraestructura AC. Datos de Configuración	Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.
-	A.DISP. Indisponibilidad de la información o servicios	AC. Información Almacenada AC. Servicio ofrecido a la organización	Un fallo en la infraestructura podría comprometer la disponibilidad de la información almacenada y de los servicios prestados a la organización.

5. FUNCIONES DE SEGURIDAD

5.1. ESPECIFICACIÓN DE LAS FUNCIONES DE SEGURIDAD DEL PRODUCTO

Las funciones de seguridad que se especifican a continuación siguen los requisitos establecidos por [CCN-STIC-140-F10M] para hiperconvergencia. En la descripción de cada uno de ellos se hace una referencia indicando qué requisito se está tratando. Quedando indicado el requisito al que se hace referencia, se omiten las definiciones por cuestiones de claridad.

En aquellos casos en los que la redacción del requisito haya sido refinada, esta se reproduce en cursiva.

5.1.1. FS. Auditoría

Esta función de seguridad cubre los requisitos definidos en la sección 4.1 de [CCN-STIC-140-F10M] y mitiga la amenaza (A. NODET) en lo que respecta a datos de auditoría generados por el TOE.

El TOE tiene la capacidad de generar registros de eventos de auditoría.

Los registros de auditoría del sistema operativo del TOE son aquello del sistema de auditoría de Linux, *Linux Auditing System*, que permite realizar un seguimiento de los eventos relevantes en seguridad, así como grabar los eventos en ficheros de log, y detectar actividades no autorizadas o de uso impropio cuando se inspeccionan los ficheros de log de auditoría.

La configuración establecida para el sistema de auditoría "*Audit*" (el cual guarda información sobre las llamadas al sistema que se producen) en relación con la política de retención es la siguiente:

- Número máximo de logs generados: 12
- Tamaño máximo del log generado: 12 MB
- Rotación automática al alcanzar estos límites.

El resto de archivos de auditoría por defecto contienen la siguiente política:

- Rotación semanal
- Mantiene 4 archivos de log
- Los archivos de log se sobrescriben para evitar el llenado del espacio de almacenamiento.

A excepción de algunos módulos de la capa hiperconvergente los cuales siguen el siguiente criterio:

- Rotación semanal
- Mantiene 14 archivos de log
- Los archivos de log se sobrescriben para evitar el llenado del espacio de almacenamiento.

El acceso al TOE está permanentemente auditado, tanto en el acceso mediante consola SSH, Dashboard y las diferentes operaciones y acciones que se realizan en la capa hiperconvergente. Cada componente que conforma la capa hiperconvergente mantiene su propio fichero de log con el registro de las operaciones realizadas, especialmente en los aspectos de (***AUD.1)***:

- Acceso y desconexión del sistema por cualquier método (ssh, dashboard, login local).
- Cambios de contraseñas y permisos de los usuarios.
- Cambios en la configuración del sistema.
- Eventos que afecten a la funcionalidad del sistema, como son eventos relacionados con la gestión de volúmenes, conexión o desconexión física de tarjetas de red, eventos de kernel del sistema, escalado de privilegios, etc.

La estructura básica del log generado para estos apartados son los siguiente ***(AUD.2)***:

- Fecha y hora del acceso
- Nivel (WARNING-INFO-ERROR)
- Mensaje descriptivo del evento
- Usuario implicado en el evento
- Dirección IP

El acceso a los ficheros de auditoría está limitado a los usuarios autorizados, conforme a la política siguiente ***(AUD.3)***:

- Lectura, para los usuarios autorizados
- Modificación, ningún usuario
- Borrado, sólo el usuario administrador

Los logs se almacenan de forma local en el TOE y en ningún caso se exportan hacia el exterior. (***AUD.4***).

Como se ha comentado anteriormente, las políticas establecidas para los ficheros de log son ***(AUD.5)***:

Para el sistema de auditoría "*Audit*":

- Número máximo de logs generados: 12
- Tamaño máximo del log generado: 12 MB
- Rotación automática al alcanzar estos límites.

Para el resto de archivos de auditoría por defecto:

- Rotación semanal
- Mantiene 4 archivos de log
- Los archivos de log se sobrescriben para evitar el llenado del espacio de almacenamiento.

Excepcionalmente algunos módulos de la capa hiperconvergente:

- Rotación semanal
- Mantiene 14 archivos de log
- Los archivos de log se sobrescriben para evitar el llenado del espacio de almacenamiento.

5.1.2. FS. Identificación y Autenticación

Esta función de seguridad mitiga la amenaza (A. REST).

Los usuarios del TOE se autentican a través del panel de acceso del portal de administración, antes de que el acceso al TOE sea permitido (requisito ***IAU.1***). Una vez autenticado el usuario, el TOE solo permite el acceso a una funcionalidad determinada si el usuario ha sido identificado correctamente y si el rol que le ha sido asignado se lo permite.

En caso de realizar la autentificación mediante línea de comandos se establecen dos escenarios:

- Operaciones sobre la capa hiperconvergente: el TOE solicitará doble factor de autenticación. Por un lado, solicitará un usuario de acceso a la consola SSH y una vez dentro, se solicitará un usuario/clave adicional para realizar actuaciones sobre la capa hiperconvergente.
- Resto de operaciones: Para el resto de operaciones sólo se solicitará la autenticación a la consola por SSH.

El TOE limita el acceso de cuentas de usuario después de un número de intentos fallidos de acceso, ya que suelen ser un patrón indicador de ataques de fuerza bruta (requisito ***IAU.2***.). La configuración establecida para este requisito es:

- Bloqueo a través de la interfaz web durante 1800 segundos tras 6 intentos fallidos.
- Los usuarios del sistema (no root) se bloquean indefinidamente tras 8 intentos.
- El acceso por SSH bloquea durante 1 hora la dirección IP de los clientes que realicen 6 intentos de conexión fallidos en un corto período de tiempo.

En el proceso de autenticación, las credenciales utilizadas para la gestión y operación del TOE son protegidas por el componente KeyStone del propio TOE, y como se indica en el requisito ***IAU.3***: no se puede acceder a ellas si no se dispone de permiso.

Las contraseñas que gestiona el TOE siguen las pautas marcadas por el requisito ***IAU.4***: mínimo 9 caracteres y pueden incluir mayúsculas, minúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “]. Concretamente, para el servicio SSH se establece una longitud mínima de 11 caracteres y para el servicio web de 12, teniendo que incluir ambas al menos una letra minúscula, una letra mayúscula, un número y caracteres especiales.

Además, el TOE cierra la sesión de un usuario después de un periodo de tiempo sin actividad, tal y como marca el requisito ***IAU.5***.

El tiempo de actividad configurado por defecto, para la consola CLI es de 300 segundos y para el Dashboard es de 1800 segundos.

5.1.3. FS. Administración Confiable

Esta función de seguridad mitiga (A. SEG).

El TOE define el rol administrador, y es capaz de asociar usuarios a otros roles (***ADM.1***).

Únicamente un usuario administrador será capaz de administrar el TOE de forma local y remota, haciendo uso del *dashboard* a través de navegador web, una conexión remota por protocolo seguro *ssh* o conexión local en consola. Sólo un usuario con privilegios de administración puede desbloquear a un usuario bloqueado por intentos de acceso incorrectos, o por inactividad. De igual forma, sólo un usuario administrador puede cambiar parámetros de configuración del producto, como son direccionamientos IP, configuración de certificados digitales asociados al *dashboard*, configuración de los parámetros de funcionamientos de los diferentes módulos que conforman el producto (identificación, almacenamiento, etc.) ***(ADM.2)***

Como ya se indicó en el párrafo anterior, SOLO un usuario con privilegios de administración conectado por cualquiera de los métodos disponibles puede realizar cambios sobre la configuración del producto. (***ADM.3***).

5.1.4. FS. Canal Seguro

Esta función de seguridad mitiga la amenaza (A. RED).

El TOE establece canales de comunicación seguros para el intercambio de información sensible con entidades autorizadas y entre sus diferentes componentes, haciendo uso de HTTPS/TLS 1.2, protocolo incluido en la guía [CCN-STIC-807], según lo marcado en el requisito ***COM.1***.

Los canales de comunicación seguros pueden ser iniciados únicamente por el propio TOE o por los usuarios autorizados. La utilización de los canales se ve restringida por medio de SSH y HTTPS, y por la configuración de diferentes niveles de seguridad:

- Nivel físico, con posibilidad de asegurar mediante contraseñas BIOS el acceso al hardware.
- Sistema operativo base (CentOS), *securizado* conforme a las guías de aplicación CCN-STIC-619
- Núcleo del TOE, implementada mediante el uso de HTTPS/TLS 1.2 y SSH
- Propio de cada instancia.

El sistema permite que los canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas, considerando como tal, a los usuarios autorizados explícitamente. (***COM.2***)

5.1.5. FS. Instalación y Actualización Confiables

Esta función de seguridad mitiga la amenaza (A. LOCAL).

Las actualizaciones de los componentes del TOE está divididas en tres básicos: las actualizaciones del hardware (actualizaciones de BIOS), actualizaciones del sistema operativo (CentOS) y actualizaciones de la capa hiperconvergente en cualquier de sus componentes.

Las actualizaciones del software del TOE se llevarán a cabo mediante el uso de paquetes RPM firmados, realizando la aplicación de los mismos de forma manual por un usuario autorizado. El sistema permite conocer la versión instalada del producto en cualquier momento a través del dashboard usando la opción *"About"* del menú (***ACT.1.***).

El repositorio hace uso del gestor de paquetes "rpm", que permite la firma digital de los mismos antes de su distribución. Las actualizaciones desplegadas tanto del entorno operacional como los relativos a los componentes del TOE están firmados utilizando GPG. (***ACT.2***)

Asimismo, las actualizaciones solo pueden ser instaladas por usuarios con rol administrador (***ACT.3.***).

5.1.6. FS. Protección de Credenciales y Datos Sensibles

Esta función de seguridad mitiga la amenaza (A. REST).

CRD.1: *En el caso en que el producto almacene credenciales, éstas no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con CIF.1.*

Las credenciales utilizadas para la autenticación son previamente hasheadas, antes de ser almacenadas en una base de datos. El mecanismo utilizado para el hashing es bCrypt con un round de 12, 128 bits para la parte “salt” y 192 bits para el resto.

El mecanismo empleado para la generación de los tokens de seguridad es Fernet, el cual utiliza AES como algoritmo de encriptado, y que está incluido entre los autorizados para Categoría ALTA del ENS, de acuerdo con lo establecido en la guía CCN-STIC-807 (***CRD.1.***).

5.1.7. FS. Requisitos Criptográficos

Esta función de seguridad mitiga las amenazas (A. RED, A. REST).

CIF.1: *En la implementación de las funcionalidades de seguridad requeridas, el TOE empleará 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. Únicamente podrán emplearse algoritmos no autorizados en aquellos casos en los que se pueda satisfacer la funcionalidad de seguridad sin necesidad de utilizar dichos protocolos, funciones y algoritmos criptográficos y su utilización no suponga una reducción del nivel de seguridad ofrecido.*

CIF.2: *El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas). Para aquellos parámetros críticos del sistema que se almacenen sin utilizar protocolos / funciones y algoritmos autorizados de acuerdo a lo establecido en la guía CCN-STIC-807, deberá justificarse que se implementan mecanismos de protección que impiden el acceso no autorizado a dichos parámetros y que éstos se encuentran almacenados en claro únicamente durante su ciclo de vida útil.*

El TOE de forma predeterminada hace uso de mecanismos criptográficos basado en la librería de código abierto *openssl versión FIPS*.

Todas las contraseñas del sistema operativo se encuentran hasheadas. Estas contraseñas son utilizadas por *sshd* como primer factor de autentificación. Las contraseñas utilizadas por los componentes del TOE para el acceso a la capa hiperconvergente, tanto en su modalidad como segundo factor de autentificación en el modo CLI, como en el dashboard, se encuentran centralizadas en el módulo *KeyStone*. Las contraseñas, como ya se indicó en el punto 5.1.6 se encuentras hasheadas con bcrypt y la generación de los tokens de seguridad están cifrados utilizando *Fernet*, que utiliza *AES-128 + HMAC* como algoritmo principal de encriptado.

El acceso al TOE, tanto por línea de comando como a través del portal de administración se encuentra securizado utilizando en el primer caso *SSH* como protocolo de conexión con claves de *RSA-4096* bits y *https* en el segundo caso con certificados digitales autofirmados de *4096* bits.

Para la generación de los certificados autofirmados, el sistema se apoya en el uso del comando *openssl* para la creación de una cadena de certificación, iniciada con la generación de un certificado digital de CA utilizado para la generación del resto de certificados utilizados en la plataforma. Es importante señalar que el uso de estos certificados se constriñe exclusivamente a garantizar la seguridad de las conexiones a la plataforma, y la interconexión de los diferentes servicios que la conforman. No se contempla la necesidad de generar nuevos certificados basados en esta cadena una vez instalada la plataforma.

El almacenamiento de credenciales de acceso a la base de datos interna de MariaDB ha sido reforzado con autenticación por certificado para que no se use únicamente la función no conforme SHA-1, de manera que su uso no supone una reducción en el nivel de seguridad ya que es necesario usar ambos factores (a efectos prácticos el conocimiento de la password es indiferente).

La contraseña maestra de la CA se genera de forma aleatoria, no se almacena en la plataforma en ningún momento y es documentada en el informe de entrega para su custodia por el responsable de seguridad del usuario final.

Los certificados almacenados son únicamente accesibles por usuarios administradores, considerados confiables según (H. Protección Física) y no son accesibles mediante acceso físico (H. Administración Confiable).

Todo el contenido del disco, incluidos estos certificados deberán ser destruidos al final de la vida útil del producto

Este apartado da cumplimiento a los requisitos ***CIF.1*** y ***CIF.2*** de la taxonomía.

5.1.8. FS. Hiperconvergencia

Esta función de seguridad mitiga la amenaza (A. DISP).

Se garantiza que la caída de alguno de los componentes que conforman el TOE no tiene impacto en la seguridad, ya que en caso de caída del servicio SSHD para el acceso CLI, o la imposibilidad de acceder al servicio de gestión de credenciales *KeyStone* impedirán el acceso al sistema (***HCI.1***).

El TOE suministra dentro de su arquitectura elementos para validar el estado de los diferentes componentes (hipervisor, almacenamiento, red). Esta funcionalidad es accesible desde la CLI o desde el dashboard. Esta acción sólo la podrá realizar un usuario debidamente autorizado y asociado al rol correspondiente. (***HCI.2***).

El sistema genera diferentes alertas en caso de fallo de integridad de la información: por un lado, el hardware se apoya el uso de sistemas RAID que alertan mediante indicadores luminosos en caso de fallo de un disco. Por otro lado, el sistema de almacenamiento para la gestión de volúmenes físicos y lógicos está sometido a monitorización permanente, quedando registrada cualquier incidencia en los logs del sistema. Por otro lado, el dashboard dispone de la capacidad de generación de ventanas popup en caso de detectar un problema, o una operación del sistema incorrecta. ***(HCI.3)***.

El TOE permite la generación de instantáneas de las instancias (máquinas virtuales) que se están ejecutando en todo momento y vuelta a ese instante temporal en caso necesario. No existe número límite de instantáneas por instancia y siempre se almacenan en el propio TOE. La generación de instantáneas se realiza de forma manual a través del dashboard o el CLI. Existe la posibilidad de programar mediante *Shellscripts*, en caso necesario, la generación de instantáneas de forma automática. (***HCI.4***).

El TOE permite a través del dashboard o el CLI generar instancias a partir de instantáneas con el contenido exacto con el que fueron generadas sin pérdida de información independientemente de que sus volúmenes (*datastores*) originales estén o no disponibles. ***(HCI.5)***

Es posible realizar el borrado seguro de los dispositivos de almacenamientos utilizados antes de desecharlos. Para ello hace uso de herramientas del sistema operativo del TOE y en concreto de herramientas que se apoyan en el mecanismo de sobreescritura. Los dispositivos de almacenamiento se sobrescriben utilizando el comando *shred*. La invocación de este comando con la opción *-v /dev/<Id de dispositivo>* realiza la sobreescritura de la información del mismo. Por defecto la plataforma realiza una triple sobreescritura, pero es posible incrementar el número de pasadas en caso necesario con el uso de parámetros adicionales. Los datos utilizados para la sobreescritura se generan por el propio sistema indicado como fuente de los mismos el generador */dev/urandom* del TOE. Esta operación es privilegiada y se realiza a través de línea de comandos. (***HCI.6***)

6. EVALUACIONES DE MÓDULOS OPCIONALES

6.1. (MEC) LISTADO DE MECANISMOS CRIPTOGRÁFICOS

En este apartado se listan los mecanismos criptográficos del TOE dentro del alcance de la evaluación criptográfica.

CIPHERSUITES:

Mecanismo Criptográfico	Área	Descripción
TLS 1.2	Comunicaciones DashBoard	*TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384* • Primitivas de intercambio de claves: ECDHE (Curvas: secp256k1, secp384r1, secp521r1, secp256r1) • Primitivas de autenticación: RSA (4096 bits) • Primitivas de encriptación: AES-256-CBC • Autenticación de mensajes: HMAC-SHA384 *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA* • Primitivas de intercambio de claves: ECDHE (Curvas: secp256k1, secp384r1, secp521r1, secp256r1) • Primitivas de autenticación: RSA (4096 bits) • Primitivas de encriptación: AES-256-CBC • Autenticación de mensajes: HMAC-SHA1
SSH	Comunicaciones CLI	*AES256-CBC* • Primitivas de intercambio de claves: Curva: secp256r1 • Primitivas de autenticación: Curva: secp256r1 • Primitivas de encriptación: AES-CBC-256 • Autenticación de mensajes: HMAC-SHA256 y HMAC-SHA512 *AES256-CTR* • Primitivas de intercambio de claves: Curva: secp256r1 • Primitivas de autenticación: Curva: secp256r1 • Primitivas de encriptación: AES-CTR-256

		• Autenticación de mensajes: HMAC-SHA256 y HMAC-SHA512

PRIMITIVAS CRIPTOGRÁFICAS:

Mecanismo Criptográfico	Descripción
TLS 1.2 **SSH**	*Función de HASH:* • SHA1 • SHA2 • SHA256 • SHA384 *Firma y verificación de mensajes:* • RSA (4096 bits) • Secp256r1 *Autenticación de mensajes:* • HMAC-SHA256 • HMAC-SHA1 • HMAC-SHA384 • HMAC-SHA512 *Encriptado/Desencriptado:* • AES-256-CBC • AES-256-CTR *Generación de claves:* • Secp256k1 • Secp384r1 • Secp521r1 • Secp256r1 • RSA (4096 bits)

7. REFERENCIAS

[CCN-STIC-2001]	Definición de la Certificación Nacional Esencial de Seguridad (LINCE)
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE)
[CCN-STIC-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE)
[CCN-STIC-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)
[CCN-STIC-140]	Taxonomía de referencia para productos de Seguridad TIC
[CCN-STIC-140-F10M]	Taxonomía de productos STIC- Anexo F.10M: Hiperconvergencia – abril 2020
[CCN-STIC-619]	Implementación de Seguridad sobre CentOS 7 (cliente independiente) – abril 2019

8. ACRÓNIMOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
KVM	Kernel-based Virtual Machine - Máquina virtual basada en el núcleo
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo de Revisión de Código Fuente
MEC	Módulo de Evaluación Criptográfica
QEMU	Quick EMUlator – Emulador de virtualización hardware
SELinux	Security-Enhanced Linux – Módulo de seguridad del kernel de Linux
ST	Security Target – Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	Target Of Evaluation – Objeto a Evaluar
VM	Virtual Machine – Máquina virtual