centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1607

Procedimiento de empleo seguro Rubrik CDM

Julio 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.07.15 14:04:21 +02'00'

NIPO: 083-19-212-2

Fecha de Edición: julio de 2019
Rubrik ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO Y ALCANCE 5
3 ORGANIZACIÓN DEL DOCUMENTO 5
4 FASE DE DESPLIEGUE E INSTALACIÓN FÍSICA 6
4.1 INSTALACIÓN SEGURA 6
5 FASE DE CONFIGURACIÓN 6
5.1 HABILITAR CIFRADO EN REPOSO 6
5.2 INSTALAR CERTIFICADO TLS RECONOCIDO 8
5.3 HABILITAR LA INTEGRACIÓN CON GESTOR DE CLAVES EXTERNO (KMIP) 11
5.4 INTEGRACIÓN DE GESTIÓN DE USUARIOS CON DIRECTORIO ACTIVO 16
5.5 CAMBIO DE CONTRASEÑA DE ACCESO A IPMI 21
5.5.1 RECOMENDACIONES PARA EL ESTABLECIMIENTO DE CONTRASEÑAS 22
5.6 CONFIGURACIÓN DE SERVIDOR DE "SYSLOG" 23
5.7 INSTALACIÓN DEL SERVICIO DE BACKUP RUBRIK EN SERVIDORES 25
5.8 DESPLIEGUE DE INSTANCIAS SOFTWARE DE RUBRIK CDM 25
6 FASE DE OPERACIÓN Y MANTENIMIENTO 26
6.1 GESTIÓN DEL SISTEMA 26
6.2 LA NUBE PÚBLICA COMO SERVICIO DE ALMACENAMIENTO 26
7 REFERENCIAS 28
8 ABREVIATURAS 29

1 INTRODUCCIÓN

1. Rubrik es una plataforma de gestión de datos convergente que unifica componentes de hardware y software tradicionalmente ubicados en silos. Para ello, combina software de copia de seguridad y almacenamiento en una única estructura de escalado horizontal que puede empaquetarse con hardware estándar del sector, permitiendo independencia del fabricante.

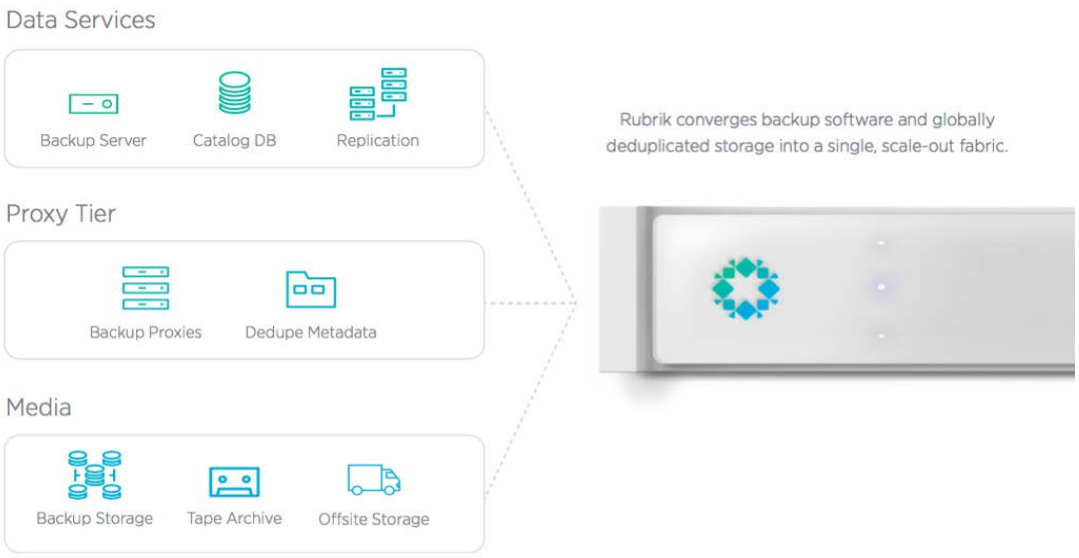


Figura 1 Arquitectura sistema Rubrik

2. La plataforma de datos convergente de Rubrik incorpora los siguientes principios de diseño:

   a) Convergencia de software: Condensa en un mismo software los diferentes componentes físicos presentes en la arquitectura de copia de seguridad y recuperación de varios niveles.

   b) Simplicidad: proporcionamos facilidad de uso a través de la simplicidad. Por ejemplo, la interfaz de usuario está diseñada para mostrar solo la información que requiere la atención del usuario, y reducir así la sobrecarga cognitiva.

   c) Escala web: Adopta tecnologías de escalabilidad web, lo que permite que los usuarios del sistema manejen volúmenes de información de crecimiento rápido con facilidad, gracias a la adición de más dispositivos en el clúster. Los usuarios evitan las laboriosas actualizaciones de gran impacto y pueden seguir gestionando RuBrik fácilmente como un solo sistema, en lugar de tener que utilizar varias islas de recursos.

   d) Eficiencia: implementa inteligencia software que permite ayudar a los usuarios a gestionar de forma eficiente los datos sin incurrir en costes innecesarios (por ejemplo, la clonación de cero bytes para ahorrar en la

capacidad de almacenamiento, enviando sólo datos deduplicados a la nube pública o al almacenamiento de objetos para reducir la transferencia de datos y el almacenamiento). Reduce la carga general de gestión (por ejemplo, búsqueda de archivos en un índice global que abarca nubes privadas y públicas).

e) Compatibilidad con el ecosistema: la plataforma de datos está diseñada para ser independiente de cualquier proveedor y funcionar con las aplicaciones y tecnologías de los centros de datos modernos.

2 OBJETO Y ALCANCE

3. En la presente guía se recoge el procedimiento de empleo seguro para los sistemas Rubrik Cloud Data Management (en adelante Rubrik CDM, o simplemente Rubrik) en su función de herramienta de copia de seguridad, tanto para entornos del Esquema Nacional de Seguridad (ENS) Categoría Alta como para entornos Clasificados.
4. Los requisitos recogidos podrán ser de configuración, uso y mantenimiento del producto y referenciarán los diferentes manuales que se encuentran publicados en la web del fabricante (https://support.rubrik.com/Downloads).
5. Aunque todas las plataformas presentan diferentes opciones de configuración, los algoritmos criptológicos utilizados en esta guía:

   a) Para el ámbito del ENS: cumplen con los requisitos estipulados en la CCN-STIC-807 Criptología de empleo en el ENS para la Categoría Alta.

   b) Para el ámbito de la información clasificada: no ha sido evaluada la capacidad de la cifra implementada por el producto para la protección de información clasificada. Por ello, en el caso en que se desee cifrar la información *on line* o *at rest*, deberá utilizarse en combinación con productos de cifra aprobados para el manejo de información clasificada hasta el nivel de clasificación requerido.

3 ORGANIZACIÓN DEL DOCUMENTO

6. El presente documento se divide en tres partes fundamentales, de acuerdo a distintas fases que componen el ciclo de vida del producto:

   a. Apartado 5. En este apartado se recogen los requisitos o recomendaciones asociadas a la fase de **despliegue e instalación** física del producto.

   b. Apartado 6. En este apartado se recogen requisitos o recomendaciones asociadas a la fase de **configuración segura** del producto.

   c. Apartado 2. En este apartado se recogen requisitos o recomendaciones relativas a las tareas de mantenimiento durante la fase de **operación y mantenimiento** del producto.

4 FASE DE DESPLIEGUE E INSTALACIÓN FÍSICA

4.1 Instalación segura

7. Los dispositivos deberán instalarse dentro de un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.
8. Para ello, la sala en la que se ubica el CPD estará dotada de un sistema de control que asegure que únicamente dichas personas pueden acceder al dispositivo (incluido fuera del horario laboral).

5 FASE DE CONFIGURACIÓN

5.1 Habilitar cifrado en reposo

9. En el momento de la instalación (*bootstrap*), se deberá habilitar el cifrado en reposo (*Encryption at Rest*) de los datos dentro del sistema. De esta forma, todos los datos se almacenan utilizando un algoritmo AES-256. Una vez habilitada, esta parametrización no puede ser deshecha, salvo que se resetee y reconfigure todo el sistema desde cero, lo que implicará un borrado de todos los datos almacenados.
10. La instalación y activación del cifrado *at rest* podrá realizarse por línea de comandos/consola o mediante el interfaz gráfico. Las siguientes figuras muestran la secuencia de comandos cuando se elige la primera opción:

```
RVM1[redacted] >> bootstrap

User configuration
==================
E-mail: [redacted]
Password:
Re-enter Password:
Re-entered password does not match
Password:
Re-enter Password:

Cluster configuration
=====================
Cluster name: [redacted]
DNS Nameservers [8.8.8.8]: [redacted]
DNS Search Domains (optional):
NTP Servers [pool.ntp.org]: [redacted]

Management Gateway: [redacted]
Management Subnet Mask: 255.255.255.0

IPMI Gateway [redacted]
IPMI Subnet Mask [255.255.255.0]: 255.255.255.0

Data Gateway (optional):
Enable Software Encryption (y/n)(optional) [n]: y
```

Figura 2 Instalación y activación del cifrado *at rest* por consola (I)

```
Proceed? (y/n) [y]: y

Bootstrap Progress
==================
Starting bootstrap . . . . . .
Setting up IP Services . . . . . .
Setting up Disks . . . . . .
Setting up Encryption at Rest . . . . . .
. . . . . .
Setting up Metadata Services . . . . . .
Setting up Data Services . . . . . .
```

Figura 3 Instalación y activación del cifrado at rest por consola (II)

11. La siguiente figura muestra el interfaz gráfico para la instalación y activación del cifrado:

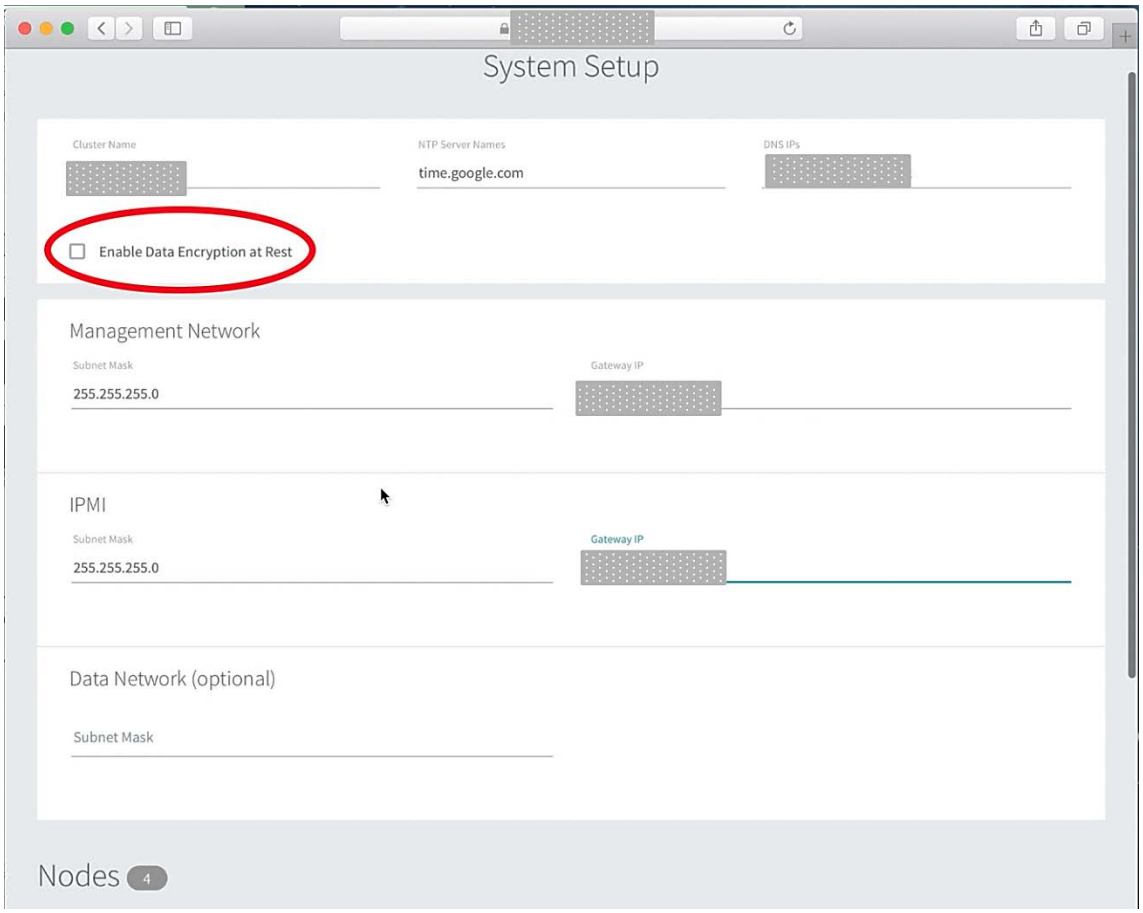


Figura 4 Instalación y activación del cifrado *at rest* por interfaz gráfico

5.2 Instalar certificado TLS reconocido

12. Los sistemas Rubrik usan TLS (*Transport Layer Security*) para la autenticación y transmisión segura de datos por red. Por defecto, Rubrik usa un certificado auto-firmado para autenticación y cifrado, que deberá sustituirse por un certificado firmado por una autoridad certificadora reconocida (CA).

13. De acuerdo a lo indicado en la CCN-STIC-807, los certificados utilizados deberán utilizar:

    a) claves de cifrado con una fortaleza criptográfica de 128 bits o superior, es decir, claves RSA de 3.072 bits o superior o claves de al menos 256 bits si se emplean curvas elípticas

    b) funciones resumen SHA-2 o SHA-3 superiores o iguales a 256 bits.

14. Para generar una petición de firma de certificado (*Certificate Signing Request* – CSR) desde la pantalla principal de administración web, deberán llevarse a cabo los siguientes pasos:

    a) Acceder al menú de configuración pinchando sobre el icono de rueda dentada:

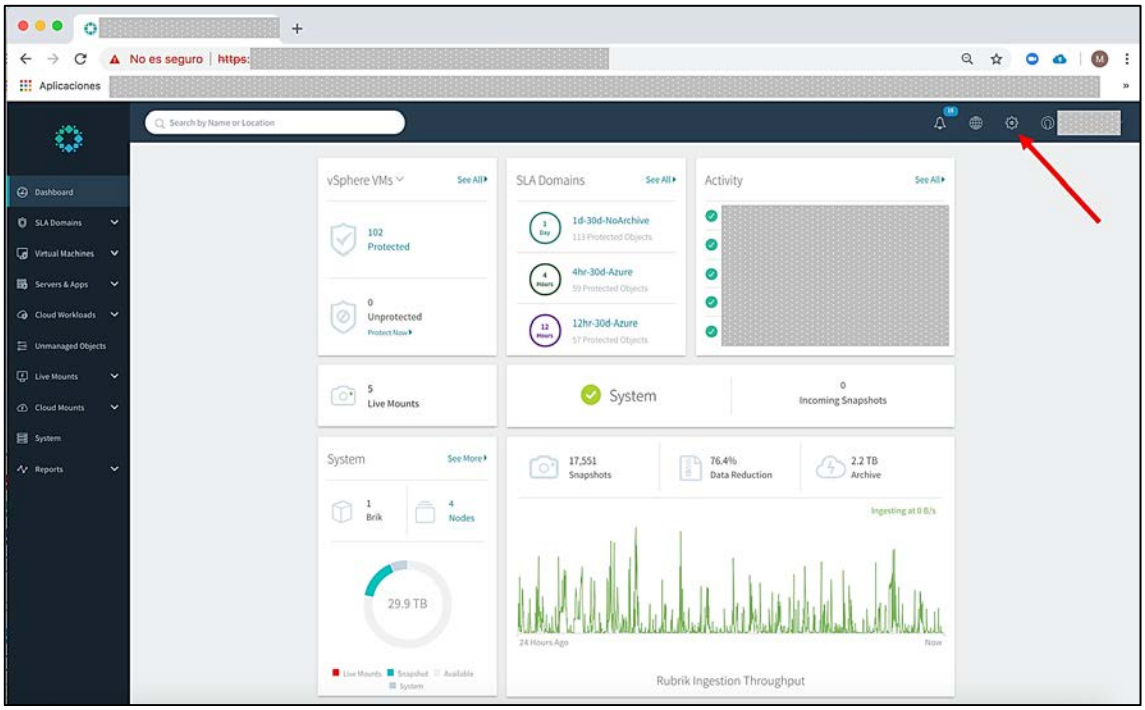
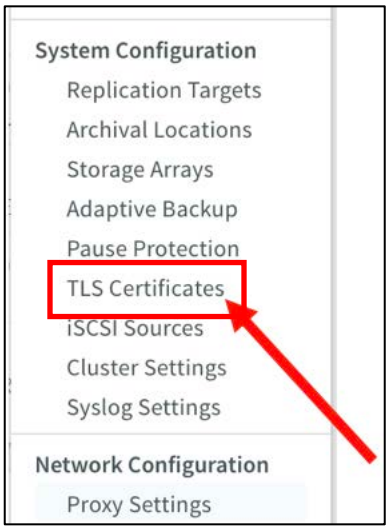


Figura 5 Menú de configuración

b) En el desplegable, seleccionar “System Configuration / TLS Certificates”:



c) Seleccionar “Generate CSR” pinchando el botón superior derecho:

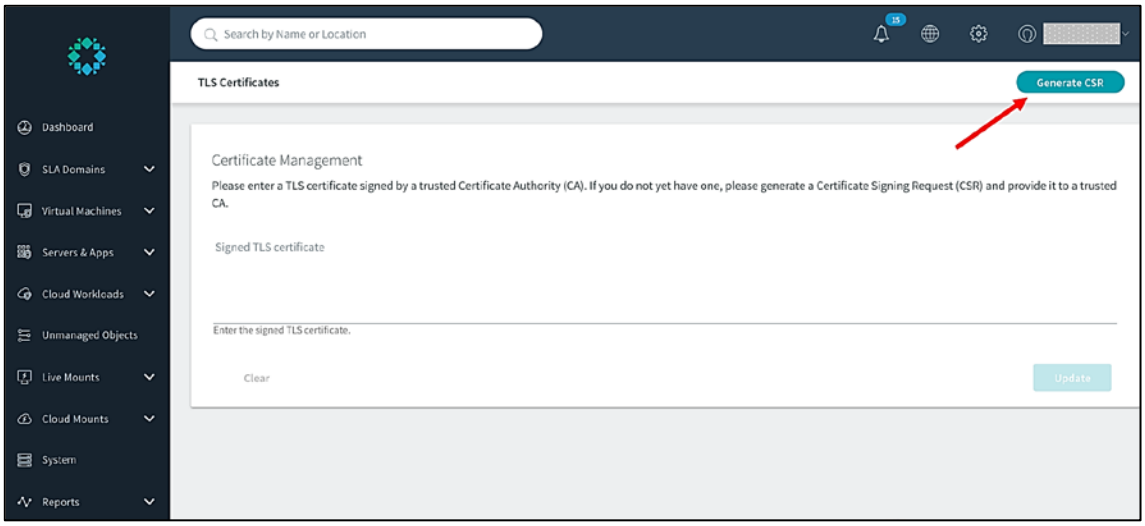


Figura 6 Generación de CSR I

d) Rellenar los campos y seleccionar "Generate":

Figura 7 Generación de CSR II

e) Descargar el CSR generado como fichero de texto. Dicho fichero de texto debe ser proporcionado como parte de la petición de generación de certificado TLS (X.509v3) a la autoridad certificadora. Una vez obtenido el certificado, repetir los pasos a y b, y a continuación, introducir el certificado firmado por la CA en el cuadro de texto (incluyendo las líneas "-----BEGIN CERTIFICATE-----" y "-----END CERTIFICATE-----"). Terminar pulsando el botón "Update":

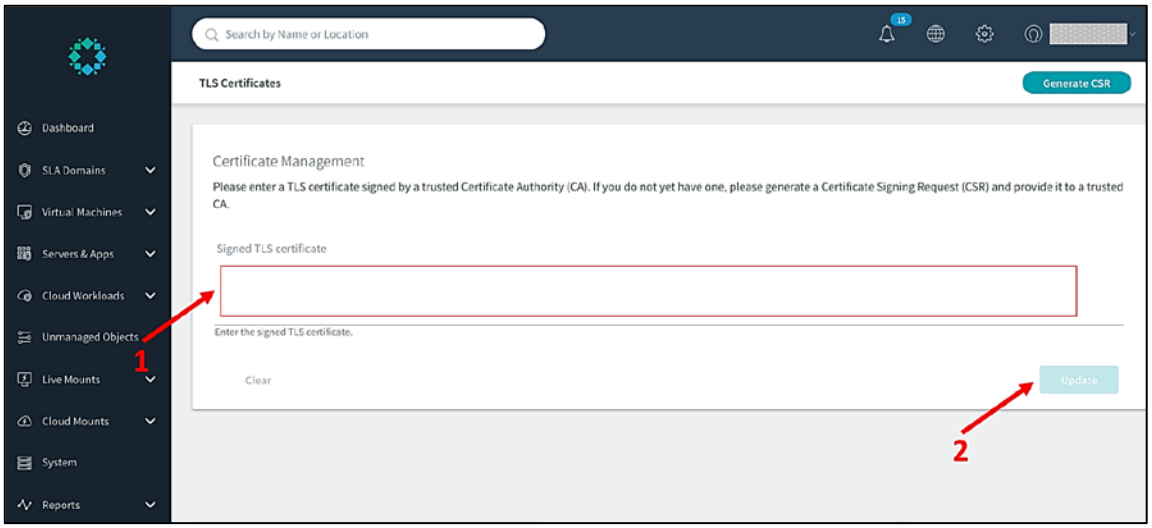


Figura 8 Obtención de certificado

5.3 Habilitar la integración con gestor de claves externo (KMIP)

15. Aunque el rotado de claves se puede realizar desde la propia herramienta de gestión del sistema Rubrik, o a través de API, se recomienda la integración con un gestor de claves externo (KMIP). Para ello deberán seguirse los siguientes pasos:

    a) Acceder al menú de configuración pinchando sobre el icono de rueda dentada (Ver Figura 5).

    b) Seleccionar “Manage Encryption”.

c) Seleccionar la pestaña de "KMIP Settings".

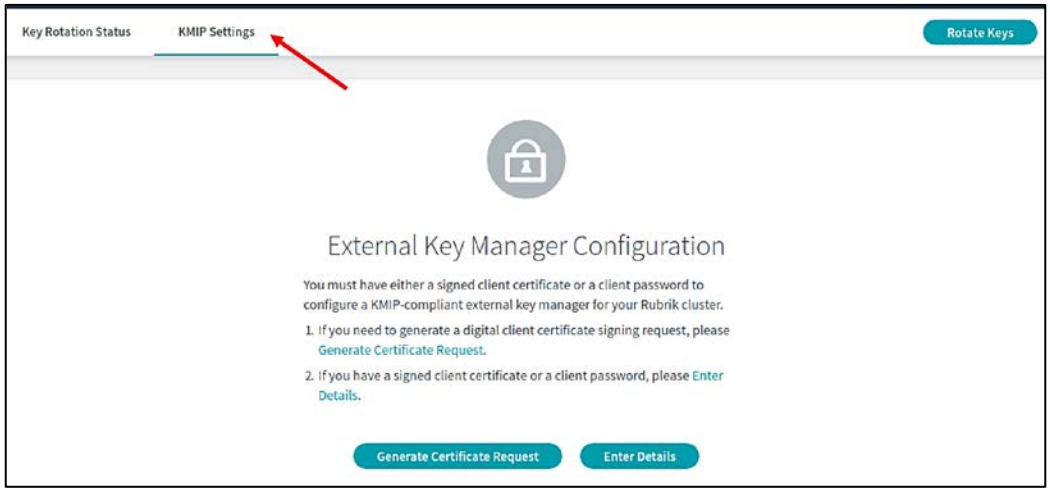


Figura 9 Pestaña KMIP Settings

i. Si el acceso al KMIP es por certificado, generar una petición de certificado.

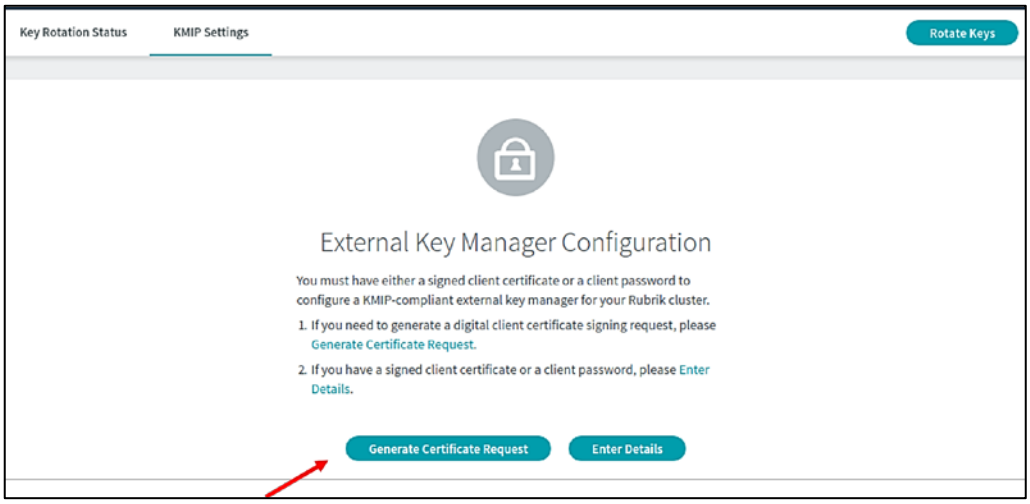


Figura 10 Generación de petición de certificado

ii. Usar el nombre del usuario para generar el certificado y descargarlo para que sea firmado por una autoridad certificado.

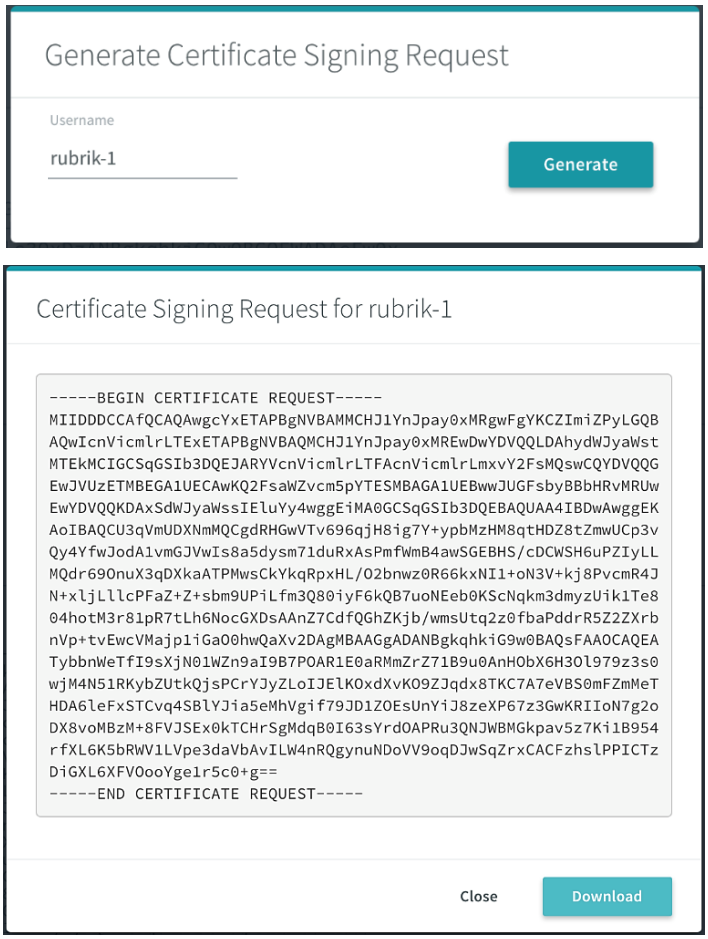


Figura 11 Generación y descarga de certificado

d) Acceder a los detalles de configuración del servidor KMIP.

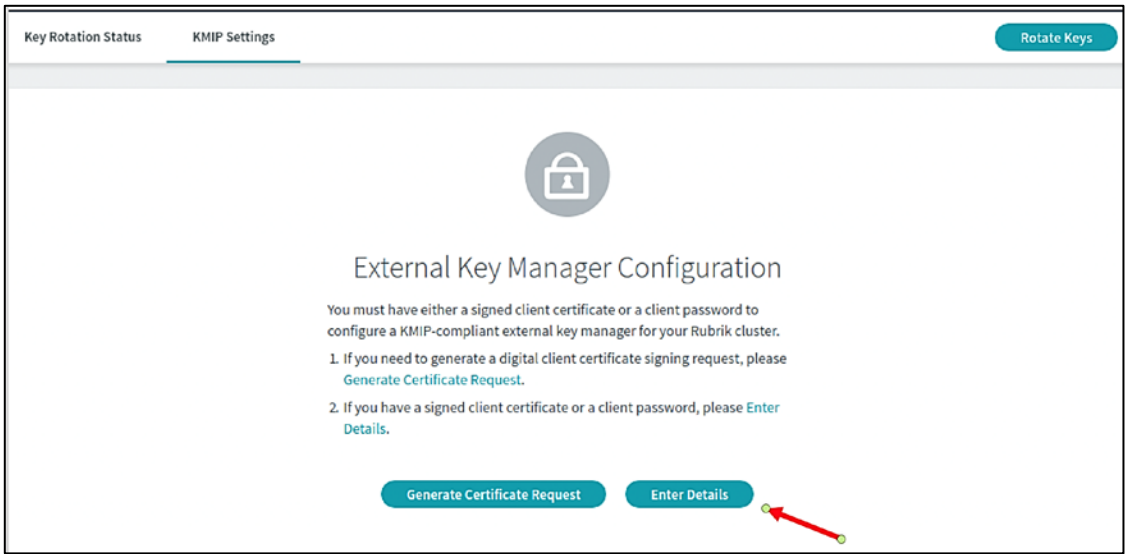
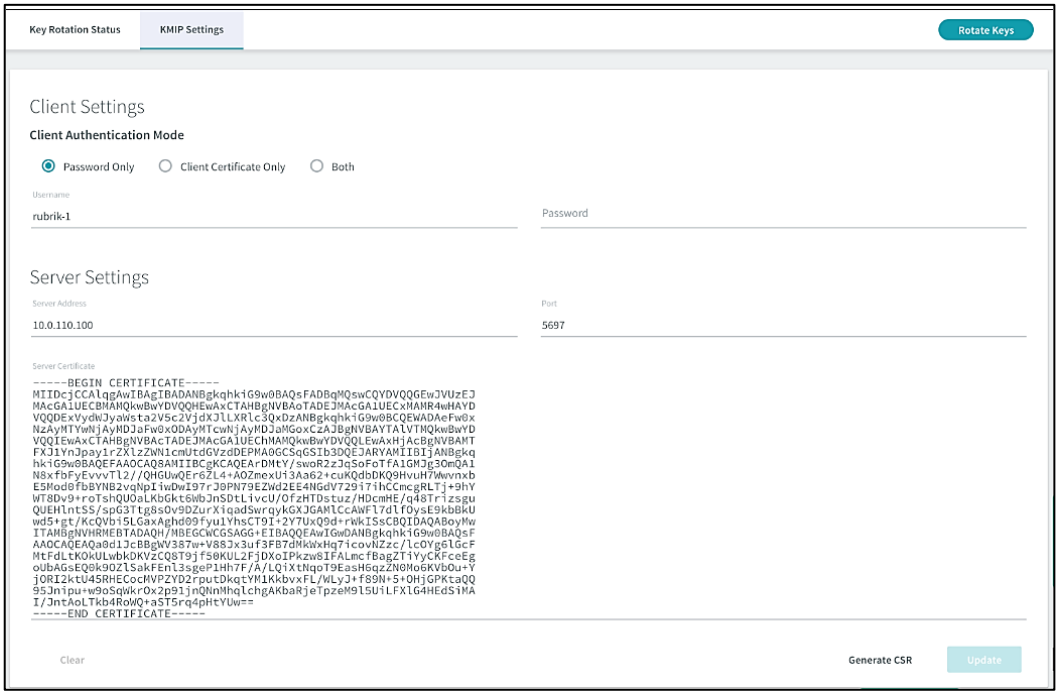
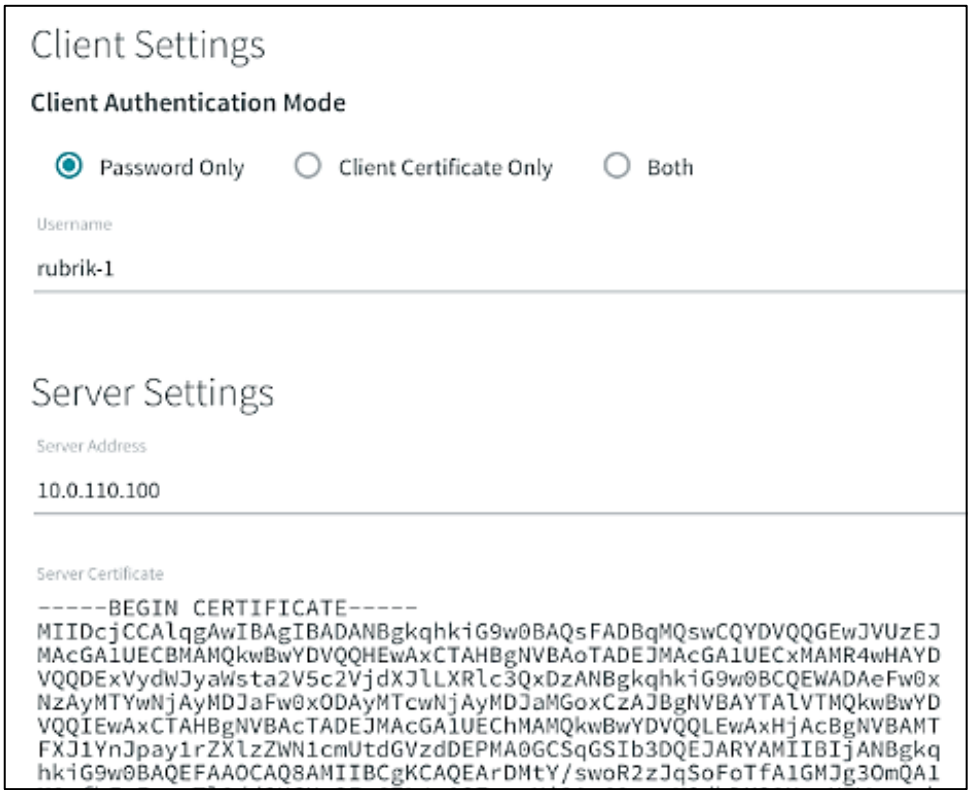


Figura 12 Detalles configuración servidor KMIP

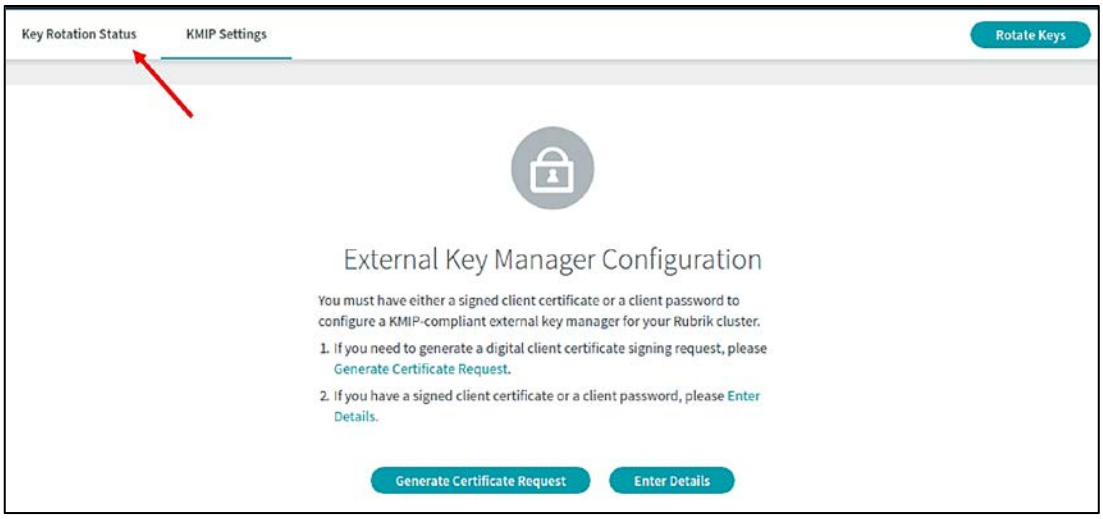
e) Configurar el acceso al servidor de gestión de claves (KMIP) según los requisitos de éste:

- Acceso por usuario y contraseña: introducir usuario y contraseña.
- Acceso por certificado: Introducir certificado firmado por autoridad obtenido en los pasos c)i y c)ii.
- Ambos tipos de acceso: Introducir usuario y contraseña, y además el certificado firmado por autoridad obtenido en los pasos c)i y c)ii.





f) Activar el rotado de claves a través del servidor de gestión (KMIP)



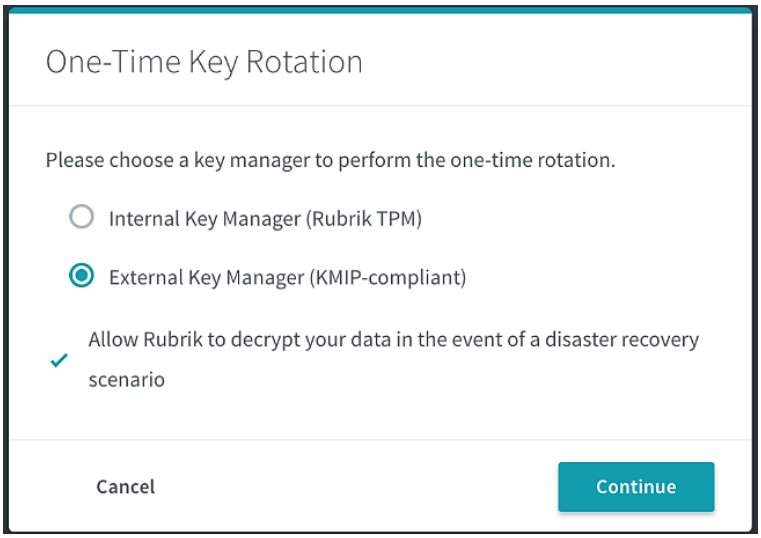
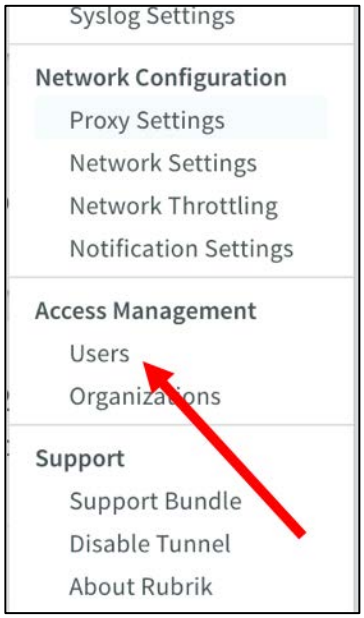


Figura 13 Activación del rotado de claves

5.4 Integración de gestión de usuarios con Directorio Activo

16. Como norma general, en la configuración del sistema deberán seguirse los principios de mínima funcionalidad y mínimo privilegio, es decir, se tratará que los usuarios administradores sean los mínimos posibles y que el conjunto de usuarios no disponga de más privilegios que los que necesita.
17. En la instalación del sistema, se creará por defecto un usuario denominado "admin", con una contraseña segura según el algoritmo "zxcvbn" (https://github.com/dropbox/zxcvbn). Este usuario tendrá acceso a todas las funciones del sistema, y deberá ser usado solo para ciertas tareas de administración (superusuario).
18. Para la administración diaria del sistema se recomienda la integración con un sistema de gestión de usuarios como el Directorio Activo de Microsoft. De esta manera, se podrá crear un usuario para las tareas diarias que se atenga a las reglas de seguridad establecidas dentro del Dominio Activo (rotación de contraseñas, validez de credenciales, etc.), dejando el acceso de superusuario solo para los casos necesarios.
19. Para ello, deberán llevarse a cabo los siguientes pasos:
    - **a)** Acceder al menú de configuración pinchando sobre el icono de rueda dentada (Ver Figura 5).
    - **b)** Seleccionar "Access Management / Users":



c) Acceder a la configuración de Directorio Activo:

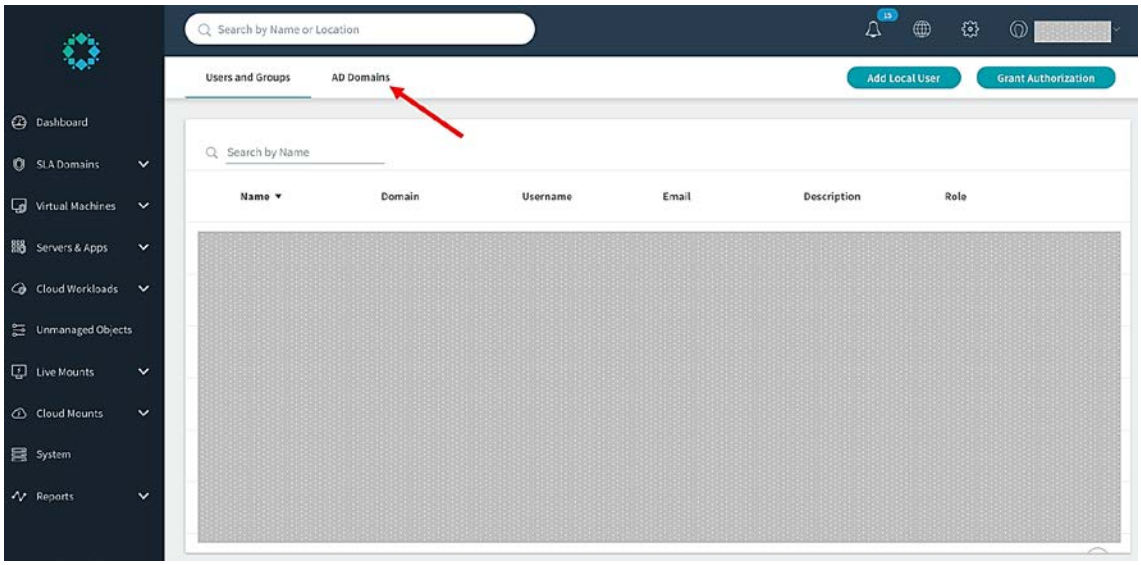


Figura 14 Configuración de directorio activo

d) Seleccionar “Connect AD Domain”:

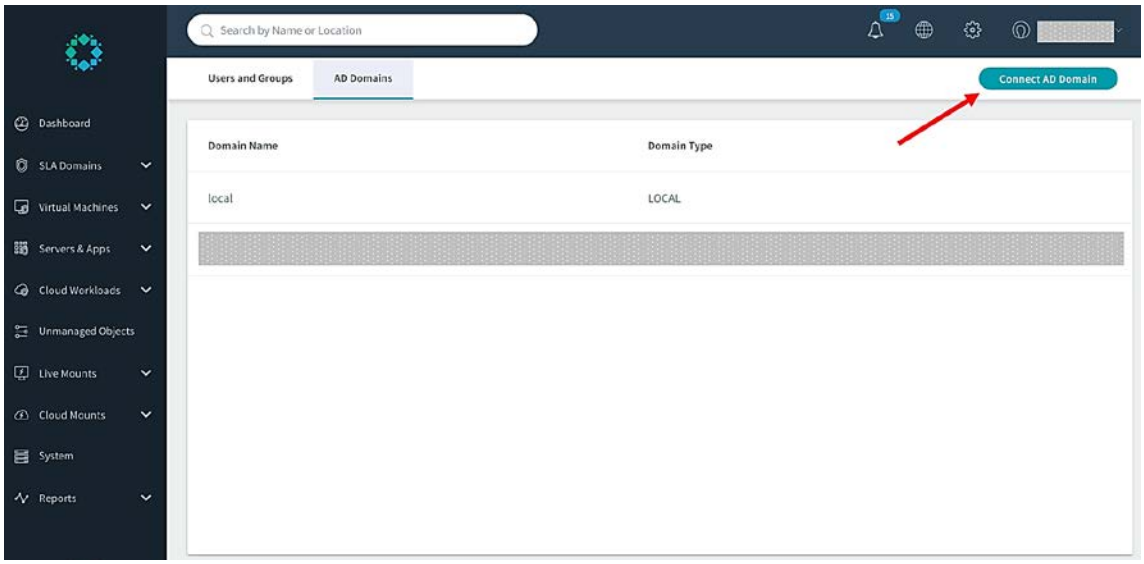


Figura 15 Conexión AD Domain I

e) Rellenar los campos y seleccionar conectar. El usuario deberá tener los permisos adecuados para registrar un nuevo "*computer name*" (CN) para dar de alta el sistema Rubrik en el Directorio Activo.

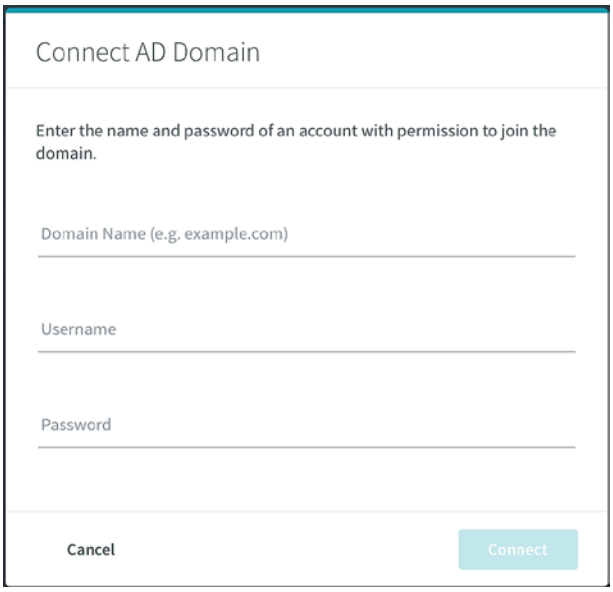


Figura 16 Conexión AD Domain II

f) A continuación, volvemos a la pantalla de configuración de usuarios:

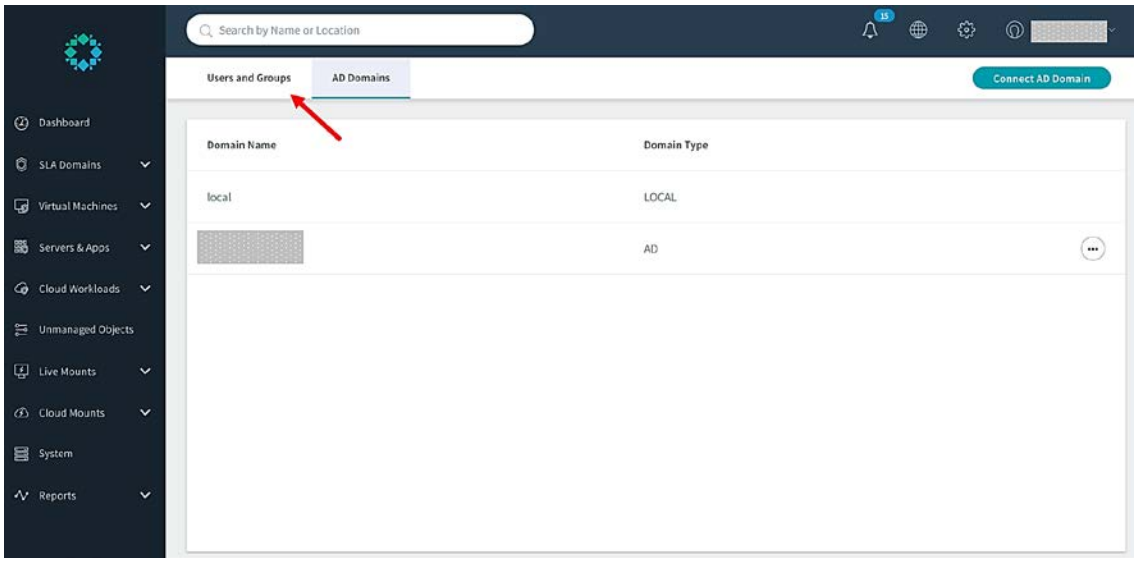


Figura 17 Pantalla configuración de usuarios

g) Seleccionar "Grant Authorization":

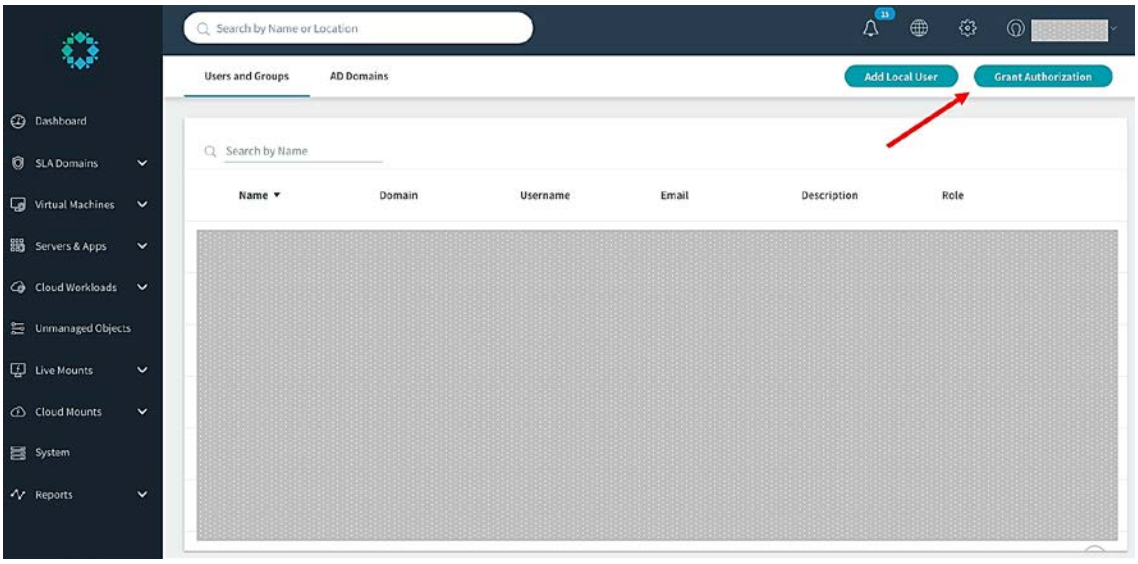


Figura 18 Selección de Grant Authorization

h) Seleccionar el Directorio Activo en el menú desplegable (1), buscamos el usuario designado para administrar el sistema (2) (en el ejemplo se ha usado el operador de backup) y lo seleccionamos (3):

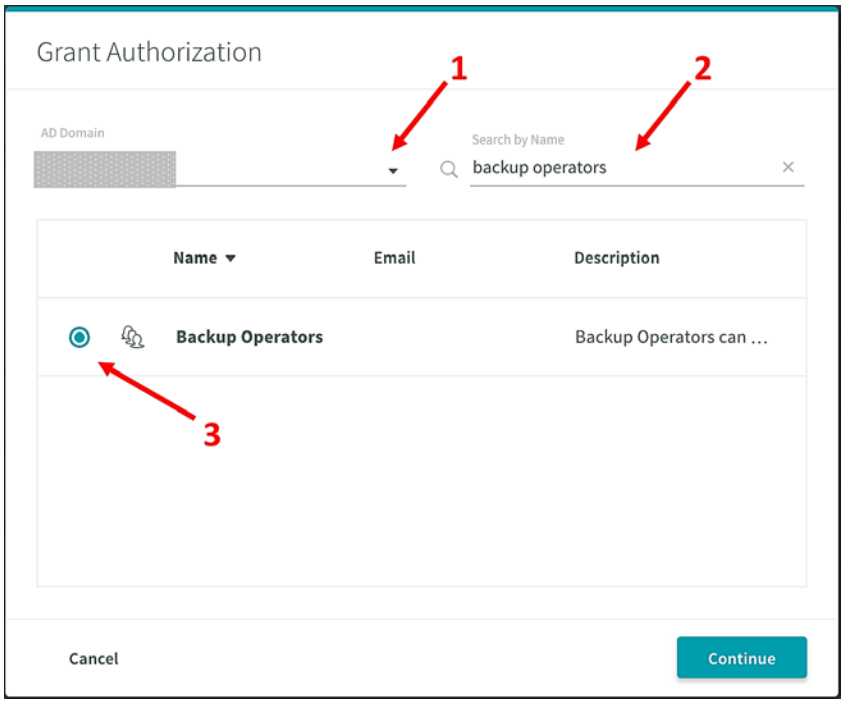


Figura 19 Grant Authorization

i) Continuar hacia la siguiente pantalla, donde asignaremos el rol de administrador al usuario del Dominio Activo asignado:

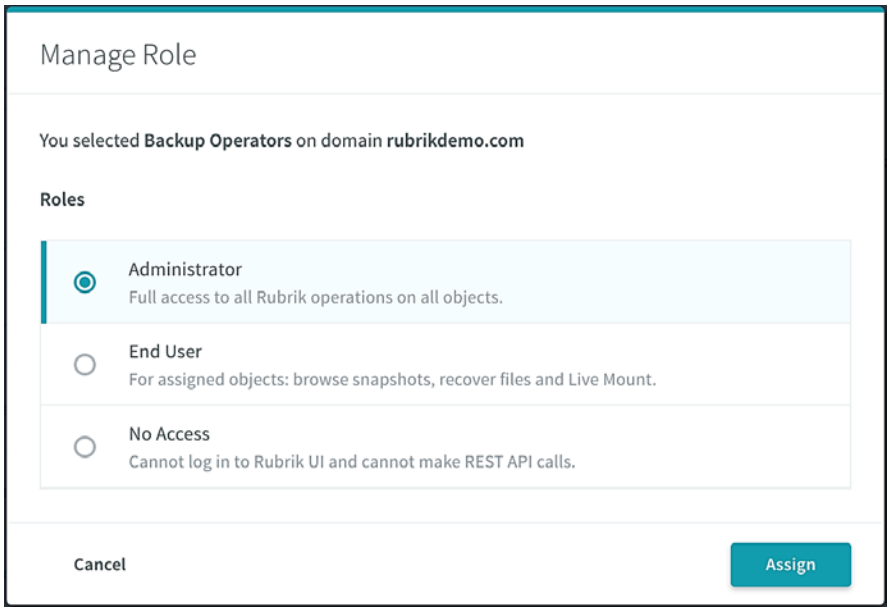


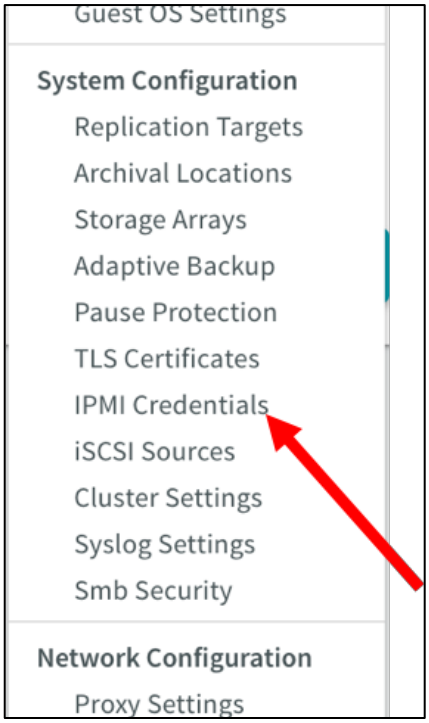
Figura 20 Asignación de rol de administrador

5.5 Cambio de contraseña de acceso a IPMI

20. Los nodos de cómputo de los sistemas Rubrik, vienen con un interfaz IPMI (*Intelligent Management Platform Interface*) que permite la gestión de ciertos parámetros hardware del sistema.
21. La administración del sistema podrá realizarse de manera local o remota, aunque la primera opción siempre será preferible a la segunda.
22. Inicialmente, deberá realizarse un cambio de la contraseña, que por defecto será la del usuario "admin" del sistema. Para ello, se deberán seguir los siguientes pasos:

    a) Acceder al menú de configuración pinchando sobre el icono de rueda dentada (Ver Figura 5).

    b) Seleccionar "System Configuration / IPMI Credentials"



    c) Habilitar los métodos de acceso siguientes (HTTPS/TLS, y SSH):

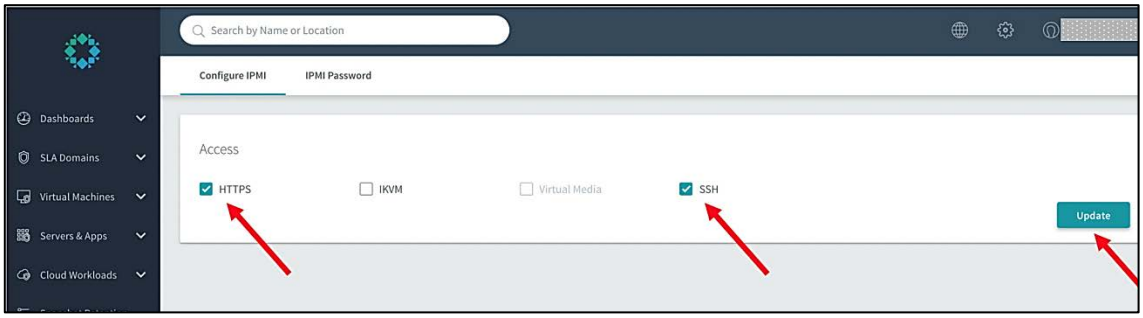


Figura 21 Métodos de acceso IPMI

d) Cambiar contraseña en la siguiente pestaña:

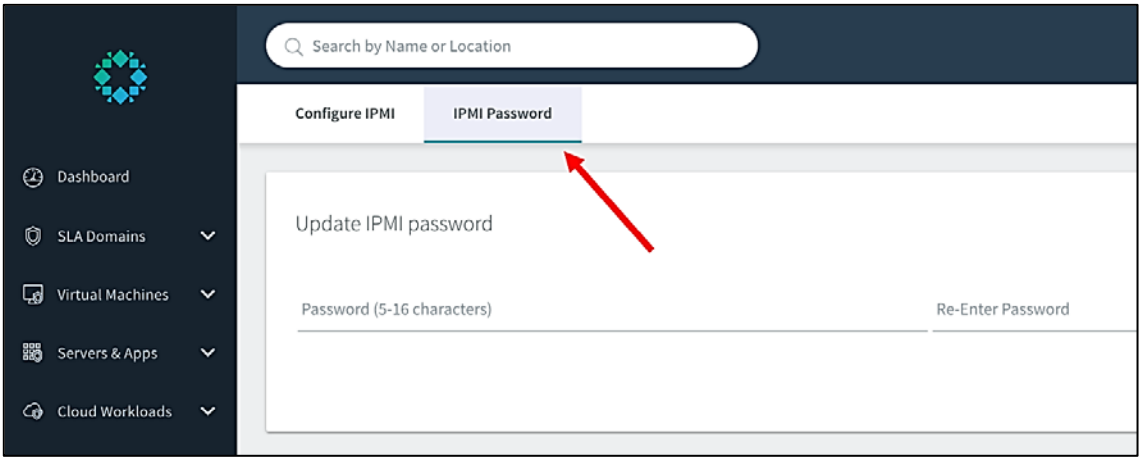


Figura 22 Pestaña de cambio de contraseña

23. El acceso por SSH se realizará con la herramienta IPMItool (http://openipmi.sourceforge.net/)

5.5.1 Recomendaciones para el establecimiento de contraseñas

24. A la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, deberán seguirse las siguientes directrices y opciones de configuración:

    a) Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.

    b) Deberán ser privadas y no compartirse con nadie.

    c) Deberán cambiarse periódicamente, con un período no superior a 180 días.

    d) No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas.

    e) No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.

    f) Deberán ser de 9 caracteres como mínimo.

    g) Deberán incluir caracteres alfanuméricos y caracteres especiales como “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“ y “)”, al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.

    h) Deberán contener un número mínimo de juegos de caracteres o de cambios en el juego de caracteres.

i) El uso de caracteres de control en las contraseñas no está recomendado.

j) Son contraseñas poco seguras:

i. Las palabras que puedan estar en o que existan como forma permutada en un archivo de sistema, como /etc/passwd.

ii. El nombre de host del sistema (siempre lo primero que se intenta).

iii. Cualquier palabra que aparezca en un diccionario, incluidos también diccionarios de otros idiomas distintos al inglés o al castellano, palabras que puedan aparecer en obras de autores famosos, palabras y frases habituales del mundo de los deportes, dichos, películas y series televisivas, etc.

iv. Permutaciones de todo lo anterior. Por ejemplo, una palabra del diccionario cuyas vocales se hayan sustituido por números (por ejemplo f00t) o a la que se añadan números al final.

v. Palabras generadas por máquinas. Los algoritmos reducen el espacio de búsqueda de los programas de adivinación de contraseñas, por lo que no conviene usarlos.

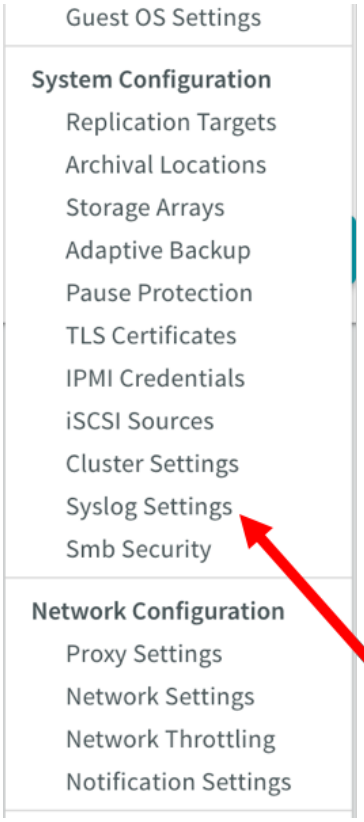
vi. Una contraseña fuerte y reutilizable puede basarse en letras de una frase o una palabra favorita que vaya después concatenada con otras palabras no relacionadas junto con números y signos de puntuación adicionales.

5.6 Configuración de servidor de "syslog"

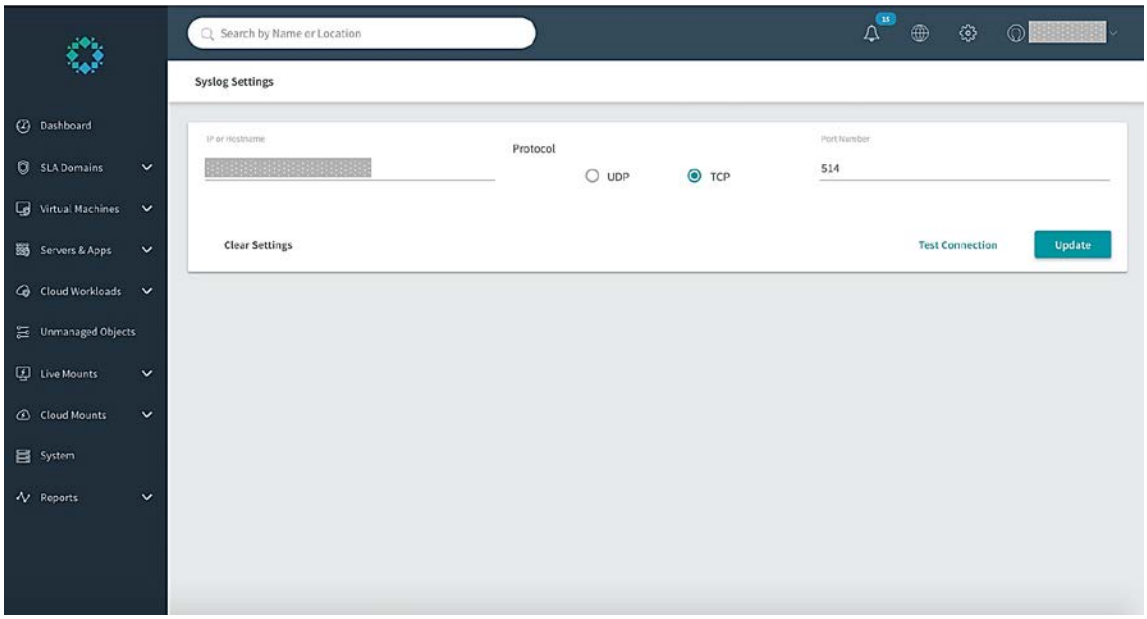
25. Aunque el sistema registra toda la actividad que se realiza en el sistema, es importante la exportación de los logs hacia un servidor desde donde se pueda revisar, especialmente, la actividad de los diferentes usuarios, como puede ser acceso (o intentos de acceso) al sistema, fallos de autenticación, *time out* de sesiones, etc. Para ello:

a) Acceder al menú de configuración pinchando sobre el icono de rueda dentada (Ver Figura 5).

b) Seleccionar "Syslog Settings".



c) Rellenar los datos de conexión y parametrización del servidor de recogida de logs de acuerdo a su configuración



5.7 Instalación del Servicio de Backup Rubrik en servidores

26. Aunque los servicios de backup de Rubrik se basan principalmente en interactuar con las APIs de los sistemas, en algunos casos, dichos sistemas no tienen un API accesible o definida, por lo que es necesario instalar el Servicio de Backup de Rubrik (RBS). Este servicio actúa de pasarela entre el sistema Rubrik, y los objetos de backup sin API definida. Entre ellos podemos encontrar sistemas de ficheros Windows/Unix/Linux/etc., bases de datos SQL, sistemas de correo Exchange, etc.
27. RBS interactúa a nivel de fichero con estos sistemas, para obtener un backup consistente a dicho nivel o incluso a nivel de aplicación, como puede ser Microsoft® SQL o Exchange, con la integración del VSS provider.
28. Además, **RBS lleva un certificado asociado**, de tal manera que la comunicación con el sistema de backup, se hace sin necesidad de introducir usuarios y contraseñas en el proceso de backup o restore.
29. Dicha instalación puede ser realizada desde el propio sistema Rubrik, proporcionando un usuario y contraseña privilegiado, pero se recomienda su instalación desde el propio servidor, o desde un gestor seguro de infraestructura/configuraciones, como por ejemplo Chef. La obtención de RBS puede ser realizada desde el propio servidor/cliente, accediendo al UI de Rubrik, o accediendo a la web de descarga del RBS en el propio sistema Rubrik. Proceder el según el manual de usuario según el método elegido.

5.8 Despliegue de instancias software de Rubrik CDM

30. Dado que el cifrado en reposo de los datos y el cifrado de las claves de cifrado se apoyan en un hardware específico de los sistemas, en los despliegues virtuales se hace necesario que estas funciones se realicen de otra forma. De esta manera se recomienda que, tanto en despliegues de Rubrik Edge/Air en entornos virtualizados, como en despliegues de Rubrik CloudCluster en nube pública, se usen las herramientas nativas de las soluciones que alberguen Rubrik CDM para efectuar el cifrado en reposo de los datos y la gestión del cifrado de claves

6 FASE DE OPERACIÓN Y MANTENIMIENTO

6.1 Gestión del sistema

31. Durante la fase de operación de los dispositivos, los administradores de seguridad deberán llevar a cabo las siguientes tareas de mantenimiento:

    a) Comprobaciones periódicas del hardware y software para asegurar que no se ha introducido hardware o software no autorizado. El código fuente del código activo y su integridad deberá verificarse periódicamente y estará libre de software malicioso.

    b) Aplicación regular de aquellas actualizaciones del firmware del sistema que impacten en las funcionalidades de seguridad, de cara a mantener su configuración segura. La existencia de nuevas actualizaciones, se notifican a los responsables del sistema (administradores). Estas notificaciones podrán realizarse de forma proactiva, ante algún fallo del propio sistema o por recomendación debido a un posible fallo futuro (o de configuración), a través de casos de soporte de forma reactiva, o a través de *newsletters* de proveedor.

    c) Mantenimiento de registros de auditoria incluyendo los eventos del sistema. Estos registros estarán protegidos de borrado y modificación no autorizada y solamente el personal de seguridad autorizado podrá acceder a ella. La información de auditoría se guardará en las condiciones establecidas en la normativa de seguridad.

    d) Auditoría de al menos los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

    e) Comprobación de que los ficheros de auditoria están protegidos del borrado y modificación no autorizada, incluso accidentales.

    f) Control de acceso a la información de auditoria de forma que únicamente el personal de seguridad designado pueda acceder a ella.

    g) Almacenamiento de la información de auditoria en las condiciones establecidas en la normativa de seguridad y por el período establecido.

6.2 La nube pública como servicio de almacenamiento

32. En aquellos casos en los que el sistema:

    a) Gestione información cuya confidencialidad e integridad demanden un nivel alto de seguridad

    y

    b) Se utilice un servicio de almacenamiento en nube pública.

Deberá complementarse la utilización de esta herramienta con la de algún producto de cifrado *off-line* Cualificado (en el caso del ENS) o Aprobado para el

nivel de clasificación de la información (en el caso de información clasificada), de tal forma que todo lo que se suba a la nube haya sido debidamente protegido mediante cifrado desde el sistema origen.

7 REFERENCIAS

STIC.1 CCN-STIC-807 Criptografía de empleo en el ENS.

STIC.2 Rubrik CDM User Guide. Version 4.1

STIC.3 Rubric CLI Reference. Version 4.1

8 ABREVIATURAS

AD	*Active Directory*
AES	*Advanced Encription Standard*
CA	*Certification Authority*
CCN	Centro Criptológico Nacional
CN	*Computer Name*
CPD	Centro de Procesamiento de Datos
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSR	*Certificate Signing Request*
ENS	Esquema Nacional de Seguridad
HTTPS	*Hypertext Transfer Protocol Secure*
IPMI	*Intelligent Management Platform Interface*
KMIP	*Key Management Interoperability Protocol*
RBS	*Rubrick Backup System*
SSH	*Secure Shell*
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*