

Guía de Seguridad de las TIC

CCN-STIC 1516

Procedimiento de Empleo Seguro Microsoft Azure HSM



Octubre 2025



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

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2025
NIPO: 083-26-132-5



Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:43:28 +02'00'

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN	3
2 OBJETO Y ALCANCE	5
3 ORGANIZACIÓN DEL DOCUMENTO	6
4 FASE PREVIA A LA INSTALACIÓN	7
4.1 ENTREGA SEGURA DEL PRODUCTO	7
4.2 ENTORNO DE INSTALACIÓN SEGURO	7
4.3 REGISTRO Y LICENCIAS	7
4.4 CONSIDERACIONES PREVIAS	7
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN	7
5 FASE DE INSTALACIÓN	9
5.1 ALTA DEL SERVICIO EN LA NUBE	9
5.2 ACTIVACIÓN AZURE MANAGED HSM	9
6 FASE DE CONFIGURACIÓN	10
6.1 MODO DE OPERACIÓN SEGURO	10
6.2 AUTENTICACIÓN	10
6.3 ADMINISTRACIÓN DEL PRODUCTO	10
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA	10
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES	11
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS	13
6.5 GESTIÓN DE CERTIFICADOS	13
6.6 SERVIDORES DE AUTENTICACIÓN	14
6.7 SINCRONIZACIÓN	14
6.8 ACTUALIZACIONES	14
6.9 AUTO-CHEQUEOS	14
6.10 ALTA DISPONIBILIDAD	14
6.11 AUDITORÍA	14
6.11.1 REGISTRO DE EVENTOS	14
6.11.2 ALMACENAMIENTO LOCAL	16
6.11.3 ALMACENAMIENTO REMOTO	16
6.12 BACKUP	16
7 FASE DE OPERACIÓN	17
8 REFERENCIAS	18
9 ABREVIATURAS	20

1 INTRODUCCIÓN

1. Azure Managed HSM (módulo de seguridad de hardware administrado de Azure), en adelante HSM, es un servicio en la nube totalmente administrado, de alta disponibilidad y un solo inquilino (organización o entidad que utiliza y administra un HSM dedicado en la nube de Azure) y compatible con los estándares que le permite proteger las claves criptográficas de las aplicaciones en la nube mediante HSM validados FIPS (Estándar Federal de Protección de la Información) 140-2 de nivel 3. Proporciona las siguientes funcionalidades:
 - Totalmente administrado: El servicio controla las operaciones de aprovisionamiento, configuración, revisión y mantenimiento.
 - Alta disponibilidad: Cada clúster de HSM consta de varias particiones HSM. Si se produce un error de hardware, las particiones de miembro del clúster de HSM se migran automáticamente a los nodos correctos.
 - Inquilino único: Cada instancia de HSM administrada está dedicada a un solo cliente y consta de un clúster de varias participaciones de HSM. Cada clúster de HSM usa un dominio de seguridad específico del cliente que aísla de forma criptográfica el clúster HSM de cada cliente.
 - Administración de claves centralizada: Se administran claves críticas y de alto valor para una organización en un solo lugar. Con permisos pormenorizados por clave, se controla el acceso a todas las claves en base al principio de “acceso con menos privilegios”.
 - Control de acceso aislado: El modelo de control de acceso "RBAC local" de HSM administrado permite a los administradores de clústeres de HSM designados tener un control completo sobre los HSM que ni siquiera los administradores de grupos de administración, suscripciones o grupos de recursos pueden invalidar.
 - Puntos de conexión privados: Se usan puntos de conexión privados para conectarse de forma segura y privada a HSM administrado desde la aplicación que se ejecuta en una red virtual.
 - HSM validados por FIPS 140-2 Nivel 3: Se protegen sus datos y se cumplen con los requisitos de cumplimiento con los HSM validados por FIPS 140-2 Nivel 3. Los HSM administrados utilizan adaptadores HSM Marvell LiquidSecurity.
 - Supervisión y auditoría: Completamente integrado con Azure Monitor. Se pueden obtener registros completos de toda la actividad a través de Azure Monitor. Se puede usar Azure Log Analytics para los análisis y las alertas.
 - Residencia de datos: HSM administrado no almacena ni procesa datos del cliente fuera de la región en la que el cliente implementa la instancia de HSM.
 - Se pueden generar (o importar mediante BYOK) claves y usarlas para cifrar los datos en reposo en servicios de Azure como Azure Storage, Azure SQL, Azure Information Protection y Customer Key para Microsoft 365. Para obtener una lista más completa de los servicios de Azure que funcionan con HSM administrado, se debe consultar la guía de **Modelos de Cifrado de Datos** [REF1].
 - Se pueden migrar fácilmente las aplicaciones existentes que usan un almacén (multi-inquilino) para usar HSM administrados.
 - Se puede utilizar los mismos patrones de implementación y desarrollo de aplicaciones para todas las aplicaciones, con independencia de la solución de administración de claves en uso: almacenes multi-inquilino o HSM administrados con un solo inquilino.

- Se pueden generar claves protegidas con HSM en el HSM local e importarlas de forma segura en los HSM administrados.

2 OBJETO Y ALCANCE

2. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Azure Managed HSM.
3. Este servicio se sitúa dentro de la Familia de Módulo de Seguridad Hardware de la tipología definida por el CCN (CPSTIC) para la categoría ENS ALTA.

3 ORGANIZACIÓN DEL DOCUMENTO

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.
- d) Apartado 7. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

4. Al tratarse de un servicio en la nube, se dará de alta los datos del cliente en la plataforma de **Microsoft Azure Portal** [REF2] y se enviarán de forma segura los accesos pertinentes a la plataforma.
5. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
6. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

7. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.

4.3 REGISTRO Y LICENCIAS

8. Los servicios prestados son mediante contratación y no es necesario una instalación.
9. La licencia, una vez activado el usuario, se basa en una licencia de coste por uso. Sólo los usuarios autorizados y con la licencia activa podrán acceder al producto.

4.4 CONSIDERACIONES PREVIAS

10. Al ser un servicio alojado en la nube, la consideración principal es, tener conexión a internet y darse de alta en la plataforma para hacer uso del producto.
11. Los prerequisites necesarios para la implementación del producto se encuentran descritos en la sección de “Requisitos previos” de la siguiente guía proporcionada por el proveedor **Activación Azure Managed HSM** [REF3].

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

12. El producto consta de los siguientes componentes principales:
 - Servicio en la nube: Espacio del usuario en la nube accesible mediante el uso de Microsoft Azure portal.
 - API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
13. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
 - Azure Portal: acceso al portal de gestión.
 - Entra ID: autenticación de usuarios, acceso condicional, políticas.
 - Azure Gateway: equilibrador de carga de tráfico web.
 - Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.

- Azure Monitor Activity Log: registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción.
- Azure Storage: solución de almacenamiento en la nube.
- Azure Events Hub: flujo de datos nativo en la nube

5 FASE DE INSTALACIÓN

14. En este apartado se describe la implementación del producto. Consta de los siguientes pasos:
 - a) Alta del servicio en Azure
 - b) Activación de Azure Managed HSM.

5.1 ALTA DEL SERVICIO EN LA NUBE

15. Al tratarse de un servicio en la nube, se requiere el alta en el portal de Azure adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del producto.
16. Una vez que se encuentre dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 ACTIVACIÓN AZURE MANAGED HSM

17. El proveedor proporciona documentación acerca de **Activación Azure Managed HSM mediante CLI** [REF3].

6 FASE DE CONFIGURACIÓN

18. Una vez dado de alta en el sistema, un usuario con rol administrador o similar debe configurar y/o comprobar que todos los artículos de seguridad estén debidamente configurados. Los próximos apartados describirán esta configuración.

6.1 MODO DE OPERACIÓN SEGURO

19. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. Para más información sobre el producto se debe consultar la **Documentación completa de Microsoft HSM administrado de Azure Key Vault** [REF4].
20. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por Azure Entra ID antes de cualquier interacción con el producto.
21. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

22. El producto usa la infraestructura de Azure vinculado a Microsoft Entra ID, para que los usuarios se autenticuen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.
23. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
24. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.
25. Más información en la guía **CCN-STIC-884A Guía de configuración segura para Azure**[REF5][REF6].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

26. Al ser un producto en la nube que forma parte de la infraestructura de Microsoft Azure, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLS 1.2 o superior para el establecimiento de las comunicaciones seguras.
27. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

28. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del producto se realiza de forma remota.
29. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.
30. El producto utiliza Azure RBAC (Control de Acceso Basado en Roles) para acceder a los recursos. A continuación, se enumeran cuatro roles fundamentales integrados. Los primeros tres se aplican a todos los tipos de recursos:
 - Propietario (Owner): Tiene acceso completo a todos los recursos, incluyendo el derecho para delegar el acceso a otros.
 - Colaborador (Contributor): Puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.
 - Lector (Reader): Puede ver los recursos existentes de Azure.
 - Administrador de Acceso de Usuario (User Access Administrator): Le permite gestionar el acceso de los usuarios a los recursos de Azure.
31. Estos roles son esenciales para controlar quién tiene permiso para realizar acciones específicas en los recursos de Azure, asegurando una gestión segura y eficiente del acceso.
32. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID** [REF6][REF7].
33. Una vez autenticados los usuarios a través de Microsoft Entra ID, el acceso a un HSM administrado se controla mediante dos interfaces:
 - Plano de administración: El plano de gestión utiliza Azure role-based access control (Azure RBAC), un sistema de autorización basado en Azure Resource Manager. Los siguientes roles se utilizarán en el plano de gestión:
 - Global administrator: Puede administrar todos los aspectos del identificador de Entra ID y los servicios de Microsoft que usan identidades de Azure Entra ID.
 - Security administrator: Puede leer información e informes de seguridad, y administrar la configuración en Azure Entra ID y Office 365.
 - Global reader: Puede leer todo lo que puede leer un administrador global, pero no actualizar nada.
 - Plano de datos: El plano de datos utiliza un RBAC a nivel de HSM gestionado (Managed HSM local RBAC), un sistema de autorización que se implementa y aplica en el nivel del HSM gestionado. Los siguientes roles se utilizarán en el plano de datos:
 - Managed HSM Administrator: Concede permisos para realizar todas las operaciones relacionadas con el dominio de seguridad, la copia de seguridad completa y la restauración, y la administración de roles. No se permite realizar ninguna operación de administración de claves.
 - Managed HSM Crypto Officer: Concede permisos para realizar todas las tareas de administración de roles, purga o recuperación de claves eliminadas, y exportación de claves. No se permite realizar otras operaciones de administración de claves.

- Managed HSM Crypto User: Concede permisos para realizar todas las operaciones de administración de claves, excepto la purga o recuperación de claves eliminadas y la exportación de claves.
 - Managed HSM Policy Administrator: Concede permisos para crear y eliminar asignación de roles.
 - Managed HSM Crypto Auditor: Concede permisos de lectura para leer (pero no usar) los atributos clave.
 - Usuario de cifrado del servicio de criptografía de HSM administrado: Concede permisos para usar una clave para el cifrado del servicio.
 - Usuario de la versión del servicio criptográfico de HSM administrado: Concede permisos para liberar una clave en un entorno de ejecución de confianza.
 - Managed HSM Backup: Concede permisos para realizar una copia de seguridad de HSM completa o de clave única.
 - Restauración de HSM administrada: Concede permisos para realizar la restauración de una sola clave o de HSM completa.
34. Cuando se crea un HSM administrado, el solicitante proporciona una lista de administradores de planos de datos (se admiten todas las entidades de seguridad). Solo estos administradores pueden tener acceso al plano de datos de HSM administrado para realizar operaciones clave y administrar asignaciones de roles del plano de datos (RBAC local de HSM administrado).
35. Para más información sobre estos roles locales de HSM administrado y las operaciones propias de cada rol, se puede consultar la guía de **Roles integrados de RBAC local para HSM administrado** [REF7][REF8].
36. El producto utiliza Azure Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad como la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:
- Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 10
 - Duración del bloqueo: 60 segundos.
37. Para más información sobre los diferentes mecanismos de seguridad de la tecnología Smart Lockout y cómo modificar los valores establecidos, se puede consultar la siguiente guía, **Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra** [REF8][REF9][REF5].
38. El producto utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Azure Entra ID. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Azure Entra ID. Los siguientes requisitos de directiva de contraseñas de Azure Entra ID se aplican a todas las contraseñas que se crean, cambian o restablecen en Azure Entra ID:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # \$ % ^ & * - _ ! + = [] { } \ : ' , . ? / ` ~ " () ; < > Espacio en blanco
Caracteres no permitidos	Caracteres unicode
Longitud de la contraseña	Aunque el producto establezca un mínimo de 8 caracteres y un máximo de 256, se deben establecer contraseñas de 12 a 256 caracteres.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos
Contraseña no utilizada recientemente	Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser la misma que las contraseñas actuales o usadas recientemente.

Tabla 1: Política de contraseñas

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

39. Todo acceso al producto se realiza mediante el uso de HTTPS con TLS1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

40. Al tratarse de un servicio en la nube, siendo parte de la infraestructura de Microsoft Azure, los certificados usan RSA con longitud de clave de 2048 bits. Este cifrado es suficientemente robusto y, aunque se considera seguro para las comunicaciones en el momento de creación de este documento, se recomienda la utilización de RSA con longitud de clave de 3072 bits.
41. Para la gestión y configuración de la longitud de clave ver la subsección “Creación de claves” de la sección “3.1.2.2 Protección de claves criptográficas” de la guía **CCN-STIC-884A Guía de configuración segura para Azure** [REF5][REF6].

6.6 SERVIDORES DE AUTENTICACIÓN

42. El producto usa Microsoft Entra ID para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.

6.7 SINCRONIZACIÓN

43. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

44. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el servicio es parte de la infraestructura de Azure.
45. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

46. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-cheques (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas del producto de manera automatizada.

6.10 ALTA DISPONIBILIDAD

47. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

48. Debido a que el producto es parte de la infraestructura de Azure, hace uso de Azure Activity Monitor Log para auditar todos los eventos que se generan por parte del producto y otros servicios de Azure, que el producto utiliza para funcionar correctamente. Para más información se puede consultar la guía oficial de **Azure Activity Monitor Log** [REF9][REF10][REF9].
49. El servicio genera registros de auditoría clasificados por actividades que se auditan en la infraestructura de Azure, para más información se puede consultar la guía **Esquema de eventos del registro de actividad de Azure**[REF10][REF11]. Puede buscar estos eventos buscando en el registro de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:
 - Proceso de inicio de sesión del personal autorizado (estos eventos son de la integración con Entra ID). Debido a la arquitectura y el modo de funcionamiento de la infraestructura de Azure, la plataforma usa la funcionalidad de sesiones y no hay

eventos de cierre de sesión. Los inicios de sesión (sing-ins) se registran con los siguientes estados descritos:

- Éxito: inicio de sesión exitoso.
 - Error: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.
 - Interrumpido: la contraseña del usuario ha caducado y, por lo tanto, su inicio de sesión o sesión ha finalizado. Donde se le pregunta al usuario si desea permanecer conectado a este navegador para facilitar los inicios de sesión posteriores.
 - Cambio en las credenciales de usuario (estos eventos son de la integración con Entra ID).
 - Cambios en la configuración del producto seleccionando la categoría apropiada:
 - Operaciones de administración de roles, como puede ser: la creación/visualización/borrado de la asignación de roles y la creación/visualización/borrado de las definiciones personalizadas de los roles.
 - Operaciones relacionadas con el Security Domain, como pueden ser: la inicialización & download, la inicialización de la recuperación y la subida.
 - Backup completo del HSM, recuperación y operaciones de recuperación selectivas.
 - Eventos relacionados con la funcionalidad del producto, buscando la categoría apropiada para la actividad (generación, destrucción, importación, exportación y modificación de las claves criptográficas):
 - Creación, modificación y borrado de las claves.
 - Firmar, verificar, encriptar, desencriptar, envolver y desenvolver las claves, y listar las claves.
 - Backup, restauración y purga de las claves.
 - Liberar las claves.
 - Detección de una intrusión o ataque físico:
 - Se deben registrar todas las peticiones API REST autenticadas, incluyendo las peticiones fallidas que pueden ocurrir por las siguientes causas: permisos de accesos, errores de sistemas o peticiones erróneas. También se deben incluir las peticiones no autenticadas que tienen como resultado una respuesta 401. Ejemplos de esto pueden ser: peticiones que no tienen un token portador, peticiones malformadas o expiradas, y peticiones con un token inválido.
50. Los registros del HSM administrado son almacenados en el contenedor “insights-logs-auditevent” dentro de la cuenta de almacenamiento (Azure Storage) que se ha especificado. Para visualizar estos logs, se deben descargar los blobs. Se puede utilizar Azure Monitor Logs para visualizar y revisar los registros de los eventos de una auditoría del HSM administrado.
51. Los resultados de un registro de una auditoría muestran la siguiente información:
- Los campos “date” y “time” corresponden a la fecha y hora en el que el evento ha ocurrido.
 - Los campos “callerIpAddress”, “identity” y “clientInfo” corresponden al usuario/cliente que ha realizado la acción que ha activado el evento.
 - El campo “operationName” corresponde a la actividad realizada por el usuario.
 - Los campos “resourceId”, “category” y “resultType” corresponden al resultado de la actividad correspondiente que creó el evento.

52. El producto usa Azure Monitor Logs y los registros de una auditoria no pueden ser eliminados por cualquier usuario. Solo se pueden eliminar registros cuando el periodo de retención ha concluido.
53. No existe una política de retención establecida por defecto para los registros del HSM administrado. Pero se puede establecer una política de retención para que los registros más antiguos sean eliminados de manera automática. Por ejemplo, se puede establecer la política de retención estableciendo los parámetros: “-RetentionEnabled” a “\$true” y “-RetentionInDays” a “90”, de esta manera los registros con una antigüedad superior a 90 días serán eliminados de manera automática.
54. En lo que refiere a los Azure Montior Logs, existe una política por defecto de retención de 30 días. Pero este periodo de retención se puede modificar y establecer en: 31, 60, 90, 120, 180, 270, 365, 550 y 730, teniendo en cuenta que la modificación de este periodo supone un coste económico adicional. Se puede también activar el periodo de archivo a una retención total de 4.383 (12 años) usando el Azure Storage.

6.11.2 ALMACENAMIENTO LOCAL

55. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada.

6.11.3 ALMACENAMIENTO REMOTO

56. La opción de enviar eventos de registros a un servidor no está disponible. Únicamente se pueden enviar los registros a los siguientes recursos de Azure: Azure Storage, Azure Event Hubs y Azure Log Analytics workspace.
57. Para más información sobre cómo realizar el envío de registros a los recursos de Azure mencionados, se puede consultar la siguiente guía, **Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage**[REF11][REF12].[REF9]

6.12 BACKUP

58. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.
59. El usuario puede realizar una copia de seguridad del contenido del HSM, incluidas todas las claves, versiones, atributos, etiquetas y asignaciones de roles. La copia de seguridad se cifra con claves criptográficas asociadas al dominio de seguridad de HSM. Para realizar estas copias de seguridad se debe seguir el proceso descrito en la siguiente guía, **Copia de seguridad y restauración completas y restauración selectiva de claves**[REF12][REF13][REF12].

7 FASE DE OPERACIÓN

60. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.
61. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:
 - Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
 - Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.
 - Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
 - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.
62. Azure Managed HSM ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.
63. Para poder hacer uso del producto de una manera segura, eficiente y conforme a las directrices establecidas, se deben seguir los procedimientos descritos en la guía **Procedimientos recomendados para proteger HSM administrado**[REF13]Error! No se encuentra el origen de la referencia.[REF12].

8 REFERENCIAS

- [REF1] Modelos de Cifrado de Datos
<https://learn.microsoft.com/es-es/azure/security/fundamentals/encryption-models#supporting-services>
- [REF2] Microsoft Azure Portal
<https://portal.azure.com>
- [REF3] Activación Azure Managed HSM mediante CLI
<https://learn.microsoft.com/es-es/azure/key-vault/managed-hsm/quick-create-cli>
- [REF4] Documentación de HSM administrado de Azure Key Vault
<https://learn.microsoft.com/es-es/azure/key-vault/managed-hsm/>
- [REF5] CCN-STIC-884A Guía de configuración segura para Azure
<https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/4253-ccn-stic-884a-guia-de-configuracion-segura-para-azure/file.html>
- [REF6] Roles Integrados de Microsoft EntraID
<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>
- [REF7] Roles Integrados de RBAC local para HSM administrado
<https://learn.microsoft.com/es-es/azure/key-vault/managed-hsm/built-in-roles>
- [REF8] Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra
<https://learn.microsoft.com/es-es/entra/identity/authentication/howto-password-smart-lockout>
- [REF9] Azure Activity Monitor Log
<https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-insights>
- [REF10] Esquema de eventos del registro de actividad de Azure
<https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-schema>
- [REF11] Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage
<https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/resource-logs>
- [REF12] Copia de seguridad y restauración completas y restauración selectiva de claves
<https://learn.microsoft.com/es-es/azure/key-vault/managed-hsm/backup-restore>

- [REF13] Procedimientos recomendados para proteger HSM administrado
<https://learn.microsoft.com/es-es/azure/key-vault/managed-hsm/best-practices>

9 ABREVIATURAS

AES	Advanced Encryption Standard
API	Application Programming Interfaces
BYOK	Bring Your Own Key
CCN	Centro Criptográfico Nacional
CLI	Interfaz de Línea de Comandos
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
CSP	Cloud Service Provider
ENS	Esquema Nacional de Seguridad.
FIPS	Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ID	Identity
MFA	Multi-Factor Authentication
NTP	Network Time Protocol
RBAC	Control de Acceso Basado en Roles
RSA	Rivest, Shamir y Adleman (Sistema Criptográfico de clave pública)
TLS	Transport Layer Security
WAF	Web Application Firewall

