Guía de Seguridad de las TIC
CCN-STIC 1519

Procedimiento de Empleo Seguro
Azure Confidential Computing

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:28:16 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. El servicio se denomina Azure Confidential Computing. Confidential Computing es un término de la industria definido por el Confidential Computing Consortium (CCC), que es parte de la Linux Foundation y está dedicado a definir y acelerar la adopción de la computación confidencial.
2. El producto protege/cifra los datos en uso, mientras están en RAM y durante los cálculos, proporcionando una garantía verificable de la integridad y confidencialidad de los datos. Asegura que, cuando los datos están "en claro" (lo cual es necesario para un procesamiento eficiente), los datos estén protegidos dentro de un Entorno de Ejecución Confiable (TEE, también conocido como enclave).
3. El producto proporciona información de la Base de Computación Confiable (TCB) para aplicar una línea base mínima para las soluciones de atestiguamiento. La Base de Computación Confiable (TCB) se refiere a todos los componentes de hardware, firmware y software de un sistema que proporcionan un entorno seguro. Los componentes dentro del TCB se consideran "críticos".
4. Si un componente dentro del TCB se ve comprometido, la seguridad de todo el sistema puede estar en peligro. Un TCB más bajo significa mayor seguridad, ya que hay menos riesgo de exposición a diversas vulnerabilidades, malware, ataques y personas maliciosas.
5. Azure Confidential Computing tiene las siguientes funcionalidades principales:
    a) Prevención de acceso no autorizado a los datos en la nube: Previene el acceso no autorizado a los datos dentro de la infraestructura de la nube.
    b) Protección de información personal cumpliendo con la regulación: Asegura que la información personal esté protegida cumpliendo con las normativas de privacidad y seguridad aplicables.
    c) Protección de procesos de datos mediante capacidades aisladas: Garantiza que los datos se procesen de manera segura y aislada, evitando cualquier manipulación externa no autorizada.
6. Para más información sobre Azure Confidential Computing, consultar la guía **Computación confidencial de Azure** [REF1].

2 OBJETO Y ALCANCE

7. El objetivo del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Azure Confidential Computing.

8. El producto Azure Confidential Computing ha sido incluido en el catálogo de productos y servicios STIC (CPSTIC). Para conocer el listado, categoría o nivel y familia de éste, consulte: https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic.

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

9. 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.
10. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
11. 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

12. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
13. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.
14. Sólo los usuarios autorizados y con la licencia activa podrá acceder al producto.

4.3 REGISTRO Y LICENCIAS

15. Los servicios prestados son mediante contratación y no es necesario la instalación. Las licencias se activan por cada usuario dentro de la suscripción contratada.

4.4 CONSIDERACIONES PREVIAS

16. Al tratarse de un servicio alojado en la nube, la principal consideración previa es tener conexión a Internet y estar dado de alta en la plataforma para hacer uso del producto.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El producto consta de los siguientes componentes principales:
    a) Servicio Azure Confidential Computing: capacidad de Azure accesible y administrable mediante Azure Portal y la capa de gestión de Azure, sobre la que se despliegan y operan los recursos confidenciales asociados al servicio.
    b) API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
18. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    a) Azure Portal: acceso al portal de gestión.
    b) Entra ID: autenticación de usuarios, acceso condicional, políticas.
    c) Azure Gateway: equilibrador de carga de tráfico web.
    d) Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.

e) Azure Monitor Activity Log: registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción.

f) Azure Storage: solución de almacenamiento en la nube.

g) Azure Event Hub: servicio de transmisión de datos utilizado para recolectar, transformar y almacenar eventos.

h) Azure Key Vault Managed HSM: claves criptográficas y secretos.

5 FASE DE INSTALACIÓN

19. En este apartado se describe la implementación del producto.

5.1 ALTA DEL SERVICIO EN LA NUBE

20. Al tratarse de un servicio en la nube, se requiere el alta en el portal de Microsoft Azure Portal adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del servicio.
21. 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 CONFIDENTIAL COMPUTING

22. El proveedor proporciona documentación acerca de Creación de soluciones de computación confidencial [REF10].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. 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 guía **Azure Confidential Computing Overview** [REF3]**.**
24. 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 Microsoft Entra ID antes de cualquier interacción con el producto.
25. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft 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

26. El producto usa la infraestructura de Azure vinculado a 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.
27. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
28. 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.
29. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF4].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. 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.
31. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

32. 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.
33. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Sólo los usuarios con el rol

de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

34. El producto utiliza Azure RBAC (Control de Acceso Basado en Roles) para gestionar el acceso a los recursos de Azure . Para la configuración y administración del servicio, se deberán asignar los roles necesarios conforme al principio de mínimo privilegio. Entre los roles integrados relevantes se incluyen [REF4]:

    a) Propietario (Owner): Tiene acceso completo a todos los recursos, incluyendo el derecho para delegar el acceso a otros.

    b) Colaborador (Contributor): Puede crear y administrar todos los tipos de recursos de Azure, pero no puede conceder acceso a otros.

    c) Lector (Reader): Puede ver los recursos existentes de Azure.

    d) Administrador de Acceso de Usuario (User Access Administrator): Le permite gestionar el acceso de los usuarios a los recursos de Azure.

35. Estos roles permiten controlar quién puede realizar acciones sobre los recursos de Azure asociados al servicio.

36. El producto utiliza Microsoft Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad haciendo uso de 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:

    a) Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 10

    b) 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 [REF5]**.

38. El producto utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Microsoft Entra ID. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Microsoft Entra ID. Los siguientes requisitos de directiva de contraseñas de Microsoft Entra ID se aplican a todas las contraseñas que se crean, cambian o restablecen en Microsoft 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	Un mínimo de 12 caracteres y un máximo de 256.
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

39. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID** [REF6].

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

40. Todo acceso al producto se realiza de forma remota a través del plano de administración de Azure, mediante Microsoft Azure Portal [REF2] y los servicios de gestión de Azure, utilizando HTTPS con TLS 1.2 o superior.

6.5 GESTIÓN DE CERTIFICADOS

41. 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.

42. 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** [REF4].

6.6 SERVIDORES DE AUTENTICACIÓN

43. 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

44. 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

45. 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.
46. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

47. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-chequeos (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

48. 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

49. El producto es parte de la infraestructura de Azure y también forma parte de Azure Activity Monitor para auditar todos los eventos que se generan por parte del producto y otros servicios de Azure.
50. Para más información, se puede consultar la guía oficial de Uso del registro de actividad de Azure Monitor y la información del registro de actividad [REF7].
51. 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** [REF8]**.** Se pueden buscar estos eventos buscando el Activity Log en el portal de seguridad y cumplimiento, seleccionando las siguientes categorías:

    a) Proceso de inicio de sesión del personal autorizado (estos eventos proceden de la integración con Entra ID). Debido a la arquitectura y modo de operación de la infraestructura Azure, la plataforma utiliza sesiones y no se dispone de un evento específico de cierre de sesión. No obstante, las sesiones pueden finalizar por expiración, cierre manual o revocación, quedando registrados los eventos de inicio de sesión y auditoría asociados:

        i. Éxito: inicio de sesión exitoso.

ii. Fallo: Error al validar las credenciales debido a que el nombre de usuario o la contraseña no son válidos.
iii. Interrumpido: La contraseña del usuario ha caducado, por lo que su login o sesión ha sido finalizado. Cuando se pregunta al usuario si desea seguir conectado a este navegador para facilitar el inicio de sesión en el futuro.

b) Funcionalidad de Azure VM:

iv. Creación, modificación o eliminación.
v. Inicio y fin.

6.11.2 ALMACENAMIENTO LOCAL

52. 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

53. 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. Azure Event Hubs puede emplearse para integrar los registros con soluciones SIEM de la organización.

54. Para más información sobre la transmisión de datos de Azure Monitor a Event Hubs y herramientas SIEM, consultar la guía Transmisión de datos de supervisión de **Transmisión de datos de supervisión de Azure a un centro de eventos y asociado externo** [REF12].

55. 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** [REF9].

6.12 BACKUP

56. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

7 FASE DE OPERACIÓN

57. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta tanto por el proveedor del servicio como por la organización cliente.

58. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:

    a) Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.

    b) Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.

    c) Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.

    d) Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

59. Azure Confidential Computing ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.

60. En las siguientes subsecciones de la fase de operación, se analizarán dichas funcionalidades en detalle, haciendo referencia, cuando corresponda, a la documentación oficial proporcionada por el proveedor. En particular, para la operación de máquinas virtuales confidenciales se deberán aplicar los procedimientos de seguridad del proveedor, incluyendo la gestión de claves y secretos conforme a las guías **Secret and Key Management in Azure Confidential Computing** [REF13] y **Azure Key Vaul**t [REF14].

7.1 PROTECCIÓN DE LA MEMORIA DE LAS VM CON SEV-SNP

61. El producto utiliza la tecnología SEV-SNP (Secure Encrypted Virtualization-Secure Nested Paging) para proteger la memoria de las máquinas virtuales (VM), implementando protecciones de cifrado de memoria e integridad que impiden que el hipervisor o procesos externos accedan a los datos sensibles.

62. SEV-SNP emplea algoritmos criptográficos para garantizar la seguridad de la memoria y evitar la lectura no autorizada de los datos.

63. Esta tecnología de AMD SEV ofrece múltiples protecciones, como cifrado de memoria, claves únicas de CPU, cifrado para el estado de los registros del procesador, fuerte protección de integridad, prevención de retroceso de firmware, endurecimiento contra canales laterales y restricciones en el comportamiento de interrupciones y excepciones.

64. Las máquinas virtuales confidenciales combinan la tecnología SEV-SNP de AMD con tecnologías de Azure, como cifrado completo de disco y Azure Key Vault Managed HSM, proporcionando una solución integral para proteger los datos sensibles.

65. Para obtener más información sobre las máquinas virtuales confidenciales, consultar la guía **Información general sobre las máquinas virtuales confidenciales** [REF11].

7.2 ASIGNACIÓN DE CLAVE DE CIFRADO ÚNICA CON SEV-SNP

66. El producto utiliza SEV-SNP para asignar una clave de cifrado única a cada CPU, asegurando que los datos cifrados por una CPU no puedan ser descifrados por otra CPU ni por el hipervisor.
67. AMD SEV asigna una clave de cifrado única a cada CPU, lo que garantiza que los datos cifrados por una CPU permanezcan seguros y aislados, incluso del hipervisor.
68. Esta protección asegura que la información cifrada no pueda ser descifrada por ninguna otra CPU, manteniendo la seguridad e integridad de los datos en todo momento.

7.3 VALIDACIÓN DE LA VERSIÓN DEL FIRMWARE DURANTE EL ARRANQUE

69. El producto valida la versión del firmware durante cada proceso de arranque y solo permite que se ejecute la versión más reciente y autorizada.
70. Para ello, se emplean mecanismos de firma digital, asegurando que solo las versiones de firmware válidas y actualizadas sean cargadas.
71. SEV incluye protecciones contra ataques de retroceso de firmware mediante la validación de la versión del firmware durante cada proceso de arranque.
72. Los mecanismos de prevención de retroceso de firmware aseguran que solo se pueda ejecutar la versión más reciente y autorizada, evitando que un atacante explote vulnerabilidades en versiones anteriores y menos seguras del firmware.
73. Esta característica se implementa a través de técnicas criptográficas que validan la integridad del firmware y la información de la versión antes de que sea cargada.

8 REFERENCIAS

[REF1] Computación confidencial de Azure
https://learn.microsoft.com/es-es/azure/confidential-computing/

[REF2] Microsoft Azure Portal
https://portal.azure.com

[REF3] Azure Confidential Computing Overview
https://learn.microsoft.com/es-es/azure/confidential-computing/overview

[REF4] 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

[REF5] 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

[REF6] Roles Integrados de Microsoft Entra ID
https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/permissions-reference

[REF7] Uso del registro de actividad de Azure Monitor y la información del registro de actividad
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-insights

[REF8] Esquema de eventos del registro de actividad de Azure
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/activity-log-schema

[REF9] 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

[REF10] Creación de soluciones de computación confidencial
https://learn.microsoft.com/es-es/azure/confidential-computing/confidential-computing-solutions

[REF11] Información general sobre las máquinas virtuales confidenciales
https://learn.microsoft.com/es-es/azure/confidential-computing/confidential-vm-overview

[REF12] Transmisión de datos de supervisión de Azure a un centro de eventos y asociado externo
https://learn.microsoft.com/es-es/azure/azure-monitor/platform/stream-monitoring-data-event-hubs

[REF13] Secret and Key Management in Azure Confidential Computing
https://learn.microsoft.com/en-us/azure/confidential-computing/secret-key-management

[REF14] Azure Key Vault
https://learn.microsoft.com/es-es/azure/key-vault/general/overview

9 ABREVIATURAS

API	Interfaz de Programación de Aplicaciones
CCC	Confidential Computing Consortium
CCN	Centro Criptográfico Nacional.
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.
HSM	Hardware Security Module
HTTPS	Secure Hyper Text Transfer Protocol.
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado)
SEV-SNP	Secure Encrypted Virtualization – Secure Nested Paging
TCB	Trusted Computing Base
TEE	Trusted Execution Environment
TLS	Transport Layer Security.
VM	Virtual Machine