Guía de Seguridad de las TIC
CCN-STIC 1237

Procedimiento de Empleo Seguro
Microsoft Defender for Cloud

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-124-4

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 09:49:39 +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

ÍNDICE

1 INTRODUCCIÓN

1. Microsoft Defender for Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP) que se compone de medidas y prácticas de seguridad diseñadas para proteger las aplicaciones basadas en la nube frente a diversas amenazas cibernéticas y vulnerabilidades.
2. Microsoft Defender for Cloud incluye las siguientes funcionalidades que cubren los tres grandes pilares de la seguridad cloud:

- Plataforma de Protección de Cargas de Trabajo en la Nube (CWPP)
  - Protección en tiempo real contra amenazas para máquinas virtuales y contenedores.
  - Respuesta más rápida a amenazas mediante integración con herramientas de respuesta a incidentes.
  - Visibilidad y control sobre cargas de trabajo en la nube en entornos multi-nube.
- Gestión de Postura de Seguridad en la Nube (CSPM)
  - Evaluación en tiempo real del estado de seguridad en la nube.
  - Detección de malas configuraciones y vulnerabilidades de seguridad.
  - Implementación de las mejores prácticas de seguridad en entornos multi-nube.
- Gestión de Seguridad para DevOps
  - Integración fluida con procesos y flujos de trabajo de DevOps.
  - Automatización de la seguridad en el pipeline de desarrollo.
  - Seguridad integrada en entornos multi-nube desde el inicio del proceso de desarrollo.

2 OBJETO Y ALCANCE

3. El objetivo del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Defender for Cloud.
4. Este servicio Microsoft Defender for Cloud ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Otras Herramientas”.

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

5. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Azure Portal** [REF1] y se enviarán de forma segura los accesos pertinentes a la plataforma.
6. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
7. Una vez dado el alta en la plataforma se podrán activar las licencias por cada usuario dentro de la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

4.3 REGISTRO Y LICENCIAS

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

4.4 CONSIDERACIONES PREVIAS

13. 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.
14. Los prerrequisitos para poder usar el producto son los siguientes:
    - Se necesita tener una suscripción a Microsoft Azure.
    - Se debe haber habilitado Microsoft Defender for Cloud en la suscripción de Microsoft Azure.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

15. 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.
16. 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 Key Vault Managed HSM: claves criptográficas y secretos.
- Servicios Azure: los recursos pueden ser protegidos por el producto.

5 FASE DE INSTALACIÓN

17. En este apartado se describe la implementación del producto. Consta de los siguientes pasos:

    - Alta del servicio en Microsoft Azure.
    - Activación de Microsoft Defender for Cloud.

5.1 ALTA DEL SERVICIO EN LA NUBE

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

19. 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 MICROSOFT DEFENDER FOR CLOUD

20. El proveedor proporciona documentación acerca de la Activación Microsoft Defender for Cloud [REF2].

6 FASE DE CONFIGURACIÓN

21. Una vez dado de alta en el sistema, un usuario de 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

22. 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 Defender for Cloud** [REF3]**.**
23. 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.
24. 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

25. 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.
26. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
27. 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.
28. 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

29. 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.
30. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

31. 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.

32. 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.

33. 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.

34. 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.

35. El producto utiliza 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.

36. 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** [REF6].

37. 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

38. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra ID** [REF5].

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** [REF4]**.**

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 producto 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-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

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 **Uso del registro de actividad de Azure Monitor y la información del registro de actividad** [REF7][REF6].
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** [REF8]**.** Se pueden buscar estos eventos buscando el Activity Log en el portal de seguridad y cumplimiento, seleccionando las siguientes categorías:

    - Inicio y fin de las funciones de auditoría: Estas funciones no aplican ya que es un servicio en la nube y la funcionalidad siempre está activada; ni el inicio ni el final pueden ser gestionados.
    - Operaciones de administración de roles: como crear/ver/eliminar asignaciones de roles y crear/ver/eliminar definiciones de roles personalizados.
    - Cambios en la configuración del sistema: Cuando hay un cambio o modificación en la configuración, se guarda el evento.
    - Proceso de inicio de sesión de personal autorizado: estos eventos provienen de la integración con Entra ID. Debido a la arquitectura y modo de operación de la

infraestructura de Azure, la plataforma utiliza la capacidad de sesiones y no hay eventos de cierre de sesión. Los accesos (inicios de sesión) se registran con los siguientes estados:
    - Éxito: inicio de sesión exitoso.
    - Fallido: Error al validar las credenciales debido a un nombre de usuario o contraseña inválidos.
    - Interrumpido: La contraseña del usuario ha expirado, por lo que su acceso o sesión se ha finalizado. Donde al usuario se le pregunta si desea quedarse conectado en este navegador para facilitar logins futuros.

50. Investigación de las actividades utilizando los filtros y consultas:

- Objeto de actividad
- Tipo de acción
- Tipo de actividad
- Actividad administrativa.

51. El Activity Log se muestra en la página de búsqueda de registros de auditoría.

52. Los resultados de una búsqueda en el Activity Log se muestran con la siguiente información:

- Fecha: La fecha y hora en que ocurrió el evento.
- Dirección IP: La dirección IP del dispositivo utilizado durante la actividad registrada. La dirección IP se muestra en formato IPv4 o IPv6.
- Usuario: El usuario (o cuenta de servicio) que realizó la acción que desencadenó el evento.
- Actividad: La actividad realizada por el usuario. Este valor corresponde a las actividades que seleccionaste en la lista desplegable de Actividades. Para un evento del Activity Log de Exchange admin, el valor en esta columna es un cmdlet de Exchange.
- Elemento: El objeto creado o modificado como resultado de la actividad correspondiente. No todas las actividades tienen un valor en esta columna.
- Detalle: Información adicional sobre una actividad. De nuevo, no todas las actividades tienen un valor.

53. El producto sobrescribe los registros siguiendo los criterios más antiguos. Cada tipo de datos se almacena durante un período diferente:

- “Métricas” tienen una retención de 93 días,
- “Logs” son configurables hasta 12 años a través de Azure Portal y API, y 7 años a través de PowerShell.

54. Defender for Cloud registra eventos de seguridad y auditoría en el Activity Log de la suscripción. Este registro proporciona información sobre cambios en los recursos, configuración de alertas y actividades relacionadas con el producto realizadas por un administrador.

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.

6.12 BACKUP

57. 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

58. 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.

59. 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.

60. Microsoft Defender for Cloud ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.

61. 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 para garantizar su uso de manera segura, eficiente y conforme a las directrices establecidas.

7.1 SEGURIDAD DEVOPS

62. La seguridad de DevOps en Defender for Cloud usa una consola central para permitir a los equipos de seguridad proteger las aplicaciones y los recursos desde el código a la nube en entornos de varias canalizaciones.

63. Para ello, el producto utiliza acceso interno basado en tokens de seguridad en el caso de Azure Repositorios de código (Azure Devops) y proceso de autorización.

64. Para más información sobre seguridad Devops se debe consultar la guía **Información general sobre la seguridad de DevOps** [REF9].

7.2 CONEXIONES DESDE UN CSP EXTERNO

65. Microsoft Defender for Cloud puede supervisar la posición de seguridad de las máquinas que no son de Azure, pero, para ello, debe conectarlas primero a Azure.

66. Para más información sobre las conexiones desde un CSP externo se debe consultar la guía de Conexión de máquinas que no son de **Azure a Microsoft Defender for Cloud [**REF10].

7.3 INFORMACIÓN DEL ESTADO DE SEGURIDAD DE LOS SISTEMAS

67. Microsoft Defender for Cloud ofrece asistencia a los usuarios para obtener información sobre el estado de seguridad de sus sistemas.

68. Para más información sobre el estado de seguridad de los sistemas se puede consultar la guía de **Revisión de la protección de cargas de trabajo** REF12**.**

7.4 SISTEMA DE ALERTAS DE SEGURIDAD

69. Microsoft Defender for Cloud permite configurar notificaciones por correo electrónico para alertas y rutas de acceso de ataques.

70. La configuración de notificaciones por correo electrónico permite la entrega de notificaciones oportunas a los destinatarios adecuados cuando se requiere una acción para mejorar el estado de seguridad de un recurso.

71. Para más información sobre el sistema de alertas se debe consultar la guía **Configuración de notificaciones de correo electrónico** [REF12].

8 REFERENCIAS

[REF1] Microsoft Azure Portal
https://portal.azure.com

[REF2] Activación Microsoft Defender for Cloud
https://learn.microsoft.com/es-es/azure/defender-for-cloud/connect-azure-subscription

[REF3] Documentación completa de Microsoft Defender for Cloud
https://learn.microsoft.com/es-es/azure/defender-for-cloud/

[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 EntraID
https://learn.microsoft.com/en-us/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] Información general sobre la seguridad de DevOps
https://learn.microsoft.com/es-es/azure/defender-for-cloud/defender-for-devops-introduction

[REF10] Conexión de máquinas que no son de Azure a Microsoft Defender for Cloud
https://learn.microsoft.com/es-es/azure/defender-for-cloud/quickstart-onboard-machines

[REF11] Revisión de la protección de cargas de trabajo
https://learn.microsoft.com/es-es/azure/defender-for-cloud/workload-protections-dashboard

[REF12] Configuración de notificaciones por correo electrónico para alertas y rutas de acceso de ataques
https://learn.microsoft.com/es-es/azure/defender-for-cloud/configure-email-notifications

9 ABREVIATURAS

API	Interfaz de Programación de Aplicaciones.
CCN	Centro Criptográfico Nacional.
CNAPP	Cloud-Native Application Protection Platform.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSP	Cloud Service Provider.
CSPM	Cloud Security Posture Management.
CWPP	Cloud Workload Protection Platform.
DevOps	Development and Operations.
ENS	Esquema Nacional de Seguridad.
HSM	Módulo de Seguridad Hardware.
HTTPS	Secure Hyper Text Transfer Protocol.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 6.
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
TLS	Transport Layer Security.
WAF	Firewall de Aplicación Web.

PUBLICACIONES DE DEFENSA

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