centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1239

Procedimiento de Empleo Seguro
Microsoft Defender for Cloud Apps

Octubre 2025

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-26-126-5

Fecha de Edición: Octubre de 2025

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:03:02 +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 Apps es un servicio en la nube de Microsoft y un componente crítico del stack de seguridad de Microsoft. Este servicio está licenciado bajo la oferta de "Enterprise Mobility and Security" y requiere la suscripción E5 para casi todos sus servicios.
2. Ofrece una solución integral para ofrecer a las organizaciones una mejor visibilidad de las actividades en la nube, descubre el Shadow IT, evalúa riesgos, impone políticas, investiga actividades sospechosas e interviene contra amenazas.
3. Al hacer esto, Microsoft Defender for Cloud Apps proporciona a las organizaciones el nivel de confianza necesario para trasladarse a la nube, manteniendo al mismo tiempo el control sobre los datos críticos.
4. Microsoft Defender for Cloud Apps proporciona una protección completa para aplicaciones SaaS, ayudando a monitorear y proteger los datos de las aplicaciones en la nube en las siguientes áreas:
    - Funcionalidad básica del Broker de Seguridad de Acceso en la Nube (CASB): como el descubrimiento de Shadow IT, visibilidad en el uso de aplicaciones en la nube, protección contra amenazas basadas en aplicaciones desde cualquier lugar en la nube, y evaluaciones de protección de información y cumplimiento.
    - Características de Gestión del Postura de Seguridad para SaaS (SSPM): que permiten a los equipos de seguridad mejorar la postura de seguridad de la organización.
    - Protección avanzada contra amenazas: como parte de la solución de detección y respuesta extendidas (XDR) de Microsoft, que permite una correlación de señales y visibilidad a lo largo de toda la cadena de ataque de amenazas avanzadas.
    - Protección entre aplicaciones: que extiende los escenarios de amenazas principales a aplicaciones habilitadas para OAuth que tienen permisos y privilegios sobre datos y recursos críticos.

2 OBJETO Y ALCANCE

5. El objetivo del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Defender for Cloud Apps.
6. Esta solución se sitúa dentro de la categoría “Protección de Equipos y Servicios” del catálogo CPSTIC para categoría 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

7. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Defender Portal** [REF1] y se enviarán de forma segura los accesos pertinentes a la plataforma.
8. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
9. 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

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

4.3 REGISTRO Y LICENCIAS

13. Los servicios prestados son mediante contratación y no es necesario una instalación.
14. La licencia, una vez activado el usuario, se basa en una licencia de coste por uso.

4.4 CONSIDERACIONES PREVIAS

15. 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.
16. Los prerrequisitos para poder usar el producto son los siguientes:
    - Se necesita tener una suscripción a Microsoft 365.
    - Se debe haber habilitado Microsoft Defender for Cloud Apps en la suscripción de Microsoft 365.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

17. El producto consta de los siguientes componentes principales:
    - Servicio en la nube: Espacio del usuario en la nube accesible mediante el uso de Microsoft Security portal.
    - API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
18. Microsoft Defender for Cloud Apps utiliza conectores de aplicaciones, que son APIs de proveedores de aplicaciones en la nube de terceros, para realizar una integración profunda, protección contra amenazas, acciones gubernamentales y aplicación de políticas. Cuando esto ocurre, la seguridad de aplicaciones en la nube puede consultar la API de aplicaciones en la nube para los registros de actividad, y comenzar a scanear datos, cuentas y contenido en la nube.

19. Los siguientes servicios de Microsoft 365 serán considerados como parte del entorno de operación:

    - Microsoft Defender XDR.
    - Microsoft Defender for Cloud.
    - Microsoft Sentinel.
    - Microsoft Defender for Endpoint.
    - Microsoft Security Exposure Management (Preview).
    - Microsoft Purview.
    - Microsoft Entra ID Protection.

5 FASE DE INSTALACIÓN

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

    - Alta del servicio en Microsoft 365.
    - Activación de Microsoft Defender for Cloud Apps.

5.1 ALTA DEL SERVICIO EN LA NUBE

21. Al tratarse de un servicio en la nube, se requiere el alta en el portal de Microsoft 365 adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del producto.

22. 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 APPS

23. Obtener una licencia de Defender for Cloud Apps para cada usuario que desee proteger mediante Defender for Cloud Apps. Para obtener más información, consulte la **Hoja de datos de licencias de Microsoft 365** [REF2].

24. Defender for Cloud Apps está disponible como parte de una evaluación de Microsoft 365 E5 y puede comprar licencias en Centro de administración de Microsoft 365 > Marketplace. Para obtener más información, consulte **Probar o comprar Microsoft 365** [REF3].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

25. 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** [REF4]**.**
26. 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 Entra ID antes de cualquier interacción con el producto.
27. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de 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

28. El producto usa 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.
29. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC). Un rol concede los permisos para realizar un conjunto de tareas y un grupo de roles es un conjunto de roles que permite a los usuarios realizar las tareas en el producto. Un usuario puede ser miembro de un rol. El producto puede usar varios roles.
30. 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.
31. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF5].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

32. Al ser un producto en la nube que forma parte de la infraestructura de Microsoft 365, 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.
33. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft 365, la administración del producto se realiza de forma remota.
35. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Entra ID. Sólo los usuarios con el rol de

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

36. El producto utiliza 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.

37. 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.

38. El producto forma parte de la infraestructura de Azure y usa Entra ID para administrar las cuentas de usuario. Las sesiones expiran después de un período establecido por el administrador en Entra ID. Los valores predeterminados son:

    - Duración máxima de la sesión: 1440 minutos.
    - Duración mínima de la sesión: 5 minutos.

39. 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.

40. 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].

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

42. 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

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

6.5 GESTIÓN DE CERTIFICADOS

44. 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.
45. 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]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

46. 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

47. 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

48. 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.
49. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

50. 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

51. 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

52. El TOE genera registros de auditoría clasificados por actividades que son auditadas en la infraestructura Azure, para más información se puede consultar la guía **Filtrar y consultar actividades de Defender for Cloud Apps** [REF8]. Puede buscar estos eventos buscando en el registro de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:

    - Inicio y fin de funciones de auditoría. Estas funciones no se aplican ya que se trata de un servicio en la nube y la funcionalidad está siempre activada, y no se puede inicio ni el fin se pueden gestionar.
    - Operaciones de gestión de roles como crear/ver/borrar asignaciones de roles y crear/ver/borrar definiciones de roles personalizados.
    - Cambios en la configuración del sistema. Cuando se produce un cambio o modificación en la configuración, se guarda el evento.
    - Proceso de login de personal autorizado (estos eventos provienen de la integración con Entra ID). Debido a la arquitectura y modo de funcionamiento de infraestructura Azure, la plataforma utiliza 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.
        - Fallo: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.

  - Interrumpido: La contraseña del usuario está caducada, y por lo tanto su login o sesión ha finalizado. Cuando se usuario se le pregunta si desea mantenerse con la sesión iniciada en el navegador, para hacer futuros inicios de sesión más sencillos.
- Investigación de las actividades utilizando los archivadores y consultas:
  - Objeto de la actividad
  - Tipo de acción
  - Tipo de actividad
  - Actividad administrativa

53. El Audit Log se muestra en la página de búsqueda de registros de auditoría.

54. Los resultados de una búsqueda en el Audit 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 Audit 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.

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.

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 365.

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 Apps 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 DETECCIÓN DE LA NUBE

62. La página Detección de nube proporciona un panel diseñado para proporcionarle más información sobre cómo se usan las aplicaciones en la nube en su organización.

63. El panel proporciona una vista general de los tipos de aplicaciones que se usan, las alertas abiertas y los niveles de riesgo de las aplicaciones de la organización.

64. También muestra quiénes son los principales usuarios de la aplicación y proporciona un mapa de ubicación de la sede central de la aplicación.

65. Para más información sobre el panel de detección de la nube se debe consultar la guía Visualización de aplicaciones detectadas con el panel de detección de nube [REF9][REF8].

7.2 POSICIÓN DE SEGURIDAD

66. Los entornos de la aplicación SaaS pueden configurarse en una posición de riesgo.

67. Microsoft Defender for Cloud Apps proporciona evaluaciones de configuración de seguridad de riesgos para las aplicaciones SaaS para ayudarle a evitar posibles riesgos.

68. Estas recomendaciones se muestran a través de la guía **Puntuación de seguridad de Microsoft** [REF10] [REF9] una vez que tiene un conector para una aplicación.

69. Para más información sobre cómo activar y administrar la posición de seguridad de la nube se debe consultar la guía **Activar y administrar la posición de seguridad de SaaS** [REF11]**.**

7.3 CONTROLAR LAS APLCIACIONES EN LA NUBE CON DIRECTIVAS

70. Las directivas permiten definir el modo en que quiere que se comporten sus usuarios en la nube. Permiten detectar comportamientos, infracciones o puntos de datos y actividades sospechosos en el entorno de la nube.

71. Para más información sobre controlar las aplicaciones en la nube con directivas se debe consultar la guía **Controlar las aplicaciones en la nube con directivas** [REF12][REF13][REF11]**.**

7.4 CONTROL DE APLICACIONES DE ACCESO CONDICIONAL EN MICROSOFT DEFENDER FOR CLOUD APPS

72. El control de aplicaciones de acceso condicional usa directivas de acceso y directivas de sesión para supervisar y controlar el acceso y las sesiones de aplicaciones de usuario en tiempo real en toda la organización.

73. Para más información sobre aplicaciones de acceso condicional se debe consultar la guía **Control de aplicaciones de acceso condicional en Microsoft Defender for Cloud Apps** [REF13].

7.5 INVESTIGACIÓN DE RIESGOS DE APLICACIONES EN LA NUBE Y ACTIVIDAD SOSPECHOSA

74. Con Microsoft Defender for Cloud Apps se obtiene un conocimiento más profundo de lo que sucede en el entorno de nube. En función de su entorno concreto y de cómo se usa, puede identificar los requisitos para proteger su organización frente a riesgos.

75. Un paso importante para comprender la nube es etiquetar las aplicaciones como autorizadas o no autorizadas, para poder identificar actividades sospechosas.

76. Para más información sobre riesgo de aplicaciones y actividad sospechosa se debe consultar la guía **Investigación de riesgos de aplicaciones en la nube y actividad sospechosa** [REF14]**.**

7.6 ADMINISTACIÓN DE APLCIACIONES CONECTADAS

77. La gobernanza le permite controlar lo que hacen los usuarios en todas las aplicaciones.

78. En el caso de las aplicaciones conectadas, puede aplicar acciones de gobernanza a archivos o actividades.

79. Las acciones de gobernanza son acciones integradas que puede ejecutar en archivos o actividades directamente desde Microsoft Defender for Cloud Apps. Las acciones de gobernanza controlan lo que hacen los usuarios en las aplicaciones conectadas.

80. Para más información sobre administración de aplicaciones conectadas se debe consultar la guía **Administración de aplicaciones conectadas** [REF15].

8 REFERENCIAS

[REF1] Microsoft Defender Portal
https://security.microsoft.com/

[REF2] Hoja de datos de licencias de Microsoft 365
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/modern-work-plan-comparison-enterprise.pdf

[REF3] Probar o comprar Microsoft 365
https://learn.microsoft.com/es-es/microsoft-365/commerce/try-or-buy-microsoft-365?view=o365-worldwide

[REF4] Documentación de Microsoft Defender for Cloud Apps
https://learn.microsoft.com/es-es/defender-cloud-apps/

[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] 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

[REF7] Roles Integrados de Microsoft EntraID
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

[REF8] Filtrar y consultar actividades de Defender for Cloud Apps
https://learn.microsoft.com/es-es/defender-cloud-apps/activity-filters-queries

[REF9] Visualización de aplicaciones detectadas con el panel de detección de nube
https://learn.microsoft.com/es-es/defender-cloud-apps/discovered-apps

[REF10] Puntuación de seguridad de Microsoft
https://learn.microsoft.com/es-es/defender-vulnerability-management/tvm-security-recommendation

[REF11] Activar y administrar la posición de seguridad de SaaS
https://learn.microsoft.com/es-es/defender-cloud-apps/security-saas

[REF12] Controlar las aplicaciones en la nube con directivas
https://learn.microsoft.com/es-es/defender-cloud-apps/control-cloud-apps-with-policies

[REF13] Control de aplicaciones de acceso condicional en Microsoft Defender for Cloud Apps
https://learn.microsoft.com/es-es/defender-cloud-apps/proxy-intro-aad

[REF14] Investigación de riesgos de aplicaciones en la nube y actividad sospechosa
https://learn.microsoft.com/es-es/defender-cloud-apps/investigate

[REF15] Administración de aplicaciones conectadas
https://learn.microsoft.com/es-es/defender-cloud-apps/governance-actions

9 ABREVIATURAS

API	Interfaz de Programación de Aplicaciones.
CASB	Cloud Access Security Broker.
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.
Entra ID	Microsoft Entra ID (anteriormente Azure Active Directory - Azure AD).
HTTPS	Secure Hyper Text Transfer Protocol.
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
SSPM	SaaS Security Posture Management.
TLS	Transport Layer Security.
XDR	Extended Detection and Response.

PUBLICACIONES DE DEFENSA

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