centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1629

Procedimiento de empleo seguro
Microsoft Defender for Office 365

Abril 2024

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

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J,
ou=CENTRO CRIPTOLOGICO NACIONAL,
o=CENTRO CRIPTOLOGICO NACIONAL,
c=ES
2024.04.12 10:04:42 +02'00'

NIPO: 083-24-148-0.
Fecha de Edición: abril de 2024.

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

ÍNDICE 2
1. INTRODUCCIÓN 3
2. OBJETO Y ALCANCE 4
3. ORGANIZACIÓN DEL DOCUMENTO 5
4. FASE PREVIA A LA INSTALACIÓN 6
4.1 ENTREGA SEGURA DEL SERVICIO 6
4.2 ENTORNO DE INSTALACIÓN SEGURO 6
4.3 REGISTRO Y LICENCIAS 6
4.4 CONSIDERACIONES PREVIAS 6
4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
5. FASE DE INSTALACIÓN 8
5.1 ALTA DEL SERVICIO EN LA NUBE 8
5.2 DESPLIEGUE DE MICROSOFT DEFENDER FOR OFFICE 365 8
6. FASE DE CONFIGURACIÓN 9
6.1 MODO DE OPERACIÓN SEGURO 9
6.2 AUTENTICACIÓN 9
6.3 ADMINISTRACIÓN DEL SERVICIO 9
6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 9
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES 10
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 11
6.5 GESTIÓN DE CERTIFICADOS 11
6.6 SERVIDORES DE AUTENTICACIÓN 12
6.7 SINCRONIZACIÓN 12
6.8 ACTUALIZACIONES 12
6.9 ALTA DISPONIBILIDAD 12
6.10 AUDITORÍA 12
6.10.1 REGISTRO DE EVENTOS 12
6.10.2 ALMACENAMIENTO LOCAL 13
6.10.3 ALMACENAMIENTO REMOTO 14
6.11 BACKUP 14
6.12 FUNCIONES DE SEGURIDAD 14
7. FASE DE OPERACIÓN 15
8. REFERENCIAS 16
9. ABREVIATURAS 17

1. INTRODUCCIÓN

1. Microsoft Defender para Office 365 es un servicio de filtrado de correo electrónico basado en la nube que ayuda a proteger su organización frente a amenazas avanzadas a las herramientas de correo electrónico y colaboración, como suplantación de identidad (*phishing*), riesgo de correo electrónico empresarial y ataques de *malware*. Defender para Office 365 también proporciona funcionalidades de investigación, búsqueda y corrección para ayudar a los equipos de seguridad a identificar, priorizar, investigar y responder a amenazas de forma eficaz.

2. Microsoft Defender para Office 365 ofrece:

   - Directivas de protección contra amenazas: definir directivas de protección contra amenazas para establecer el nivel de protección adecuado para la organización.
   - Informes: vea informes en tiempo real para supervisar el rendimiento de Microsoft Defender para Office 365 en la organización.
   - Investigación y respuesta de amenazas: usar las herramientas más avanzadas para investigar, entender, simular y evitar las amenazas.
   - Investigación automatizada y funcionalidades de respuesta: ahorrar tiempo y esfuerzo al investigar y mitigar las amenazas.

2. OBJETO Y ALCANCE

3. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Defender para Office 365. Al ser una solución en la nube, este documento no afecta a una versión específica.

4. Este servicio ha sido cualificado, e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en la Familia de *Protección de correo electrónico* de la taxonomía definida por el Centro Criptológico Nacional en la guía CCN-STIC 140.

3. ORGANIZACIÓN DEL DOCUMENTO

5. Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del servicio.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del servicio.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del servicio, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del servicio.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL SERVICIO

6. Al tratarse de un servicio en la nube, se dará de alta los datos del cliente en la plataforma de **Microsoft Office 365 (REF1)** y se enviarán de forma segura los accesos pertinentes a la plataforma.
7. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
8. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma (ver sección **4.3**).

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. Como corresponde a un servicio en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.
10. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para garantizar la seguridad de las comunicaciones.
11. Sólo los usuarios autorizados y con la licencia activa podrá acceder al servicio.

4.3 REGISTRO Y LICENCIAS

12. Los servicios prestados son mediante contratación y no es necesario la instalación.
13. El administrador asigna las licencias por cada usuario dentro de la suscripción contratada. Ver Asignar o anular la asignación de licencias para los usuarios del Centro de administración de Microsoft 365 (**REF9**).

4.4 CONSIDERACIONES PREVIAS

14. Al ser 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 servicio.
15. Los prerrequisitos necesarios para la implementación del servicio están descritos en el enlace de **Revisión de los requisitos de arquitectura de Microsoft Defender para Office 365 y los conceptos clave (REF2).**

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. El servicio se encuentra formado por los siguientes componentes:
    - **EOP:** evita ataques amplios, basados en volumen y conocidos.
    - **MDOP1:** Agrega protección de correo electrónico y colaboración contra malware de día cero, *phishing* y compromiso de correo electrónico empresarial.
    - **MDOP2:** Agrega investigación, búsqueda y respuesta posteriores a la infracción, así como automatización y simulación (para entrenamiento).

17. El servicio no requiere de otros componentes para cumplir con su funcionalidad de seguridad.

5. FASE DE INSTALACIÓN

18. En este apartado se describe la implementación del servicio. Consta de los siguientes pasos:

    - Alta del servicio en la nube.
    - Despliegue de Microsoft Defender for Office 365.

5.1 ALTA DEL SERVICIO EN LA NUBE

19. Al tratarse de un servicio en la nube, lo único que se requiere para ser utilizado es que el proveedor del servicio asigne un usuario en el sistema.

20. Una vez dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 DESPLIEGUE DE MICROSOFT DEFENDER FOR OFFICE 365

21. Este apartado esta descrito en la sección 2 de la guía CCN-STIC 885G Guía de configuración segura para Microsoft Defender for Office 365 **(**REF6**).**

6. FASE DE 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 servicio.

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 servicio. Todos los usuarios deben ser autenticados por Azure AD antes de cualquier interacción con el servicio.

24. El servicio es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del servicio. Ver sección 3.1.1 de la guía **CCN-STIC 885G Guía de configuración segura para Microsoft Defender for Office 365 (REF6).**

25. Respecto al cliente no es necesario ninguna configuración segura ya que todo se realiza desde el portal de Microsoft 365 Defender.

6.2 AUTENTICACIÓN

26. El servicio usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el servicio 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). 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 servicio. Un usuario puede ser miembro de un rol. El servicio puede usar varios roles.

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 885G Guía de configuración segura para Microsoft Defender for Office 365 (**REF6**).

6.3 ADMINISTRACIÓN DEL SERVICIO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. Al ser un servicio en la nube, que forma parte de la infraestructura de Microsoft Azure, la administración del servicio se realiza de forma remota utilizando el protocolo seguro HTTPS con TLSv1.2 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. Como es un servicio en la nube, que forma parte de la infraestructura de Microsoft Azure, la administración del servicio se realiza de forma remota.

33. El servicio es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del servicio.

34. Algunos de estos roles y funciones pueden ser los siguientes:

    - Global administrator: Puede administrar todos los aspectos del identificador de Azure AD y los servicios de Microsoft que usan identidades de Azure AD.
    - Security administrator: Puede leer información e informes de seguridad, y administrar la configuración en Azure AD y Office 365.
    - Global reader: Puede leer todo lo que puede leer un administrador global, pero no actualizar nada.

35. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Roles integrados de Microsoft Entra (REF4).**

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

    - Duración máxima de la sesión: 1440 minutos.
    - Duración mínima de la sesión: 60 minutos.
    - Cuánto tiempo antes de que expire la sesión antes de que se muestre la advertencia de tiempo de espera: 20 minutos.

37. El servicio utiliza Azure AD 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.

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

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 8 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 guía CCN-STIC-884A - Guía de configuración segura para Azure (**REF8**).

40. En la sección 3.1.1 de la guía **CCN-STIC 885G Guía de configuración segura para Microsoft Defender for Office 365 (REF6)** está definido el control de acceso implementado por el servicio.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

6.5 GESTIÓN DE CERTIFICADOS

42. Forma parte de la infraestructura de Microsoft Azure y los certificados usan RSA con longitud de clave de 2048 bits.

6.6 SERVIDORES DE AUTENTICACIÓN

43. El servicio usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el servicio cuando el acceso se realiza a través de la interfaz web. Ver sección 2 y 3 de CCN-STIC-884A Guía de configuración segura para Azure (**REF8**).

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. El proveedor de servicios en la nube actualiza el software en sus servicios administrados, y se encarga de mantener sus sistemas actualizados sin la intervención del usuario.

6.9 ALTA DISPONIBILIDAD

46. 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.

6.10 AUDITORÍA

6.10.1 REGISTRO DE EVENTOS

47. El servicio genera registros de auditoría clasificados por actividades que se auditan en Microsoft 365. 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 Azure AD). 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 (*sign-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 a un 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 Azure AD)
    - Cambios en la configuración de servicio:
        - Agregar/Modificar/Borrar roles.
        - Añadir permisos de delegación en buzones.
        - Añadir permisos en carpeta.
    - Eventos relacionados con la funcionalidad del servicio:
        - Mensaje de cuarentena

- Crear/Acceder a un buzón.
- Evento de simulación de ataque.
- Mensajes eliminados.

48. El registro de auditoría se muestra en la página de búsqueda del registro de auditoría. Los resultados de una búsqueda en el registro de auditoría se muestran con la siguiente información:

    - Fecha: la fecha y hora en que ocurrió el evento
    - Dirección IP: la dirección IP del dispositivo que se utilizó cuando se registró la actividad. La dirección IP se muestra en formato de dirección 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 seleccionadas en la lista desplegable Actividades. En el caso de un evento del registro de auditoría de administración de Exchange, el valor de esta columna es un `cmdlet` de Exchange.
    - Elemento: El objeto que se creó o modificó como resultado de la actividad correspondiente. Por ejemplo, el archivo que se ha visto o modificado o la cuenta de usuario que se ha actualizado. No todas las actividades tienen un valor en esta columna.
    - Detalle: Información adicional sobre una actividad. Una vez más, no todas las actividades tienen un valor.

49. Puede ver más detalles sobre un evento haciendo clic en el registro del evento en la lista de resultados de búsqueda. Se muestra una página flotante que contiene las propiedades detalladas del registro de eventos. Las propiedades que se muestran dependen del servicio en el que se produce el evento.

6.10.2 ALMACENAMIENTO LOCAL

50. El almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. El almacenamiento en reposo de la información se lleva a cabo mediante el uso de la infraestructura de Azure empleando el cifrado con AES-256 bits.

51. El TOE forma parte de la infraestructura de Azure, por lo que no es un dispositivo. Sin embargo, hay un período de retención de registros que puede ser modificado por un usuario autorizado, la granularidad de esta política es por tipo de registro (los diferentes tipos de registro pueden tener diferentes períodos de retención). Los valores posibles son:

    - 90 días (predeterminado).
    - 6 meses.
    - 9 meses.
    - 1 año.
    - 10 años.

52. Una vez que se alcanza el período de retención, se eliminan los registros.

6.10.3 ALMACENAMIENTO REMOTO

53. Se puede utilizar la API de Actividad de administración de Office 365 para recuperar información sobre acciones y eventos de usuario, administrador, sistema y directivas de los registros de actividad de Office 365 y Azure AD.

54. La API de Actividad de administración de Office 365 es un servicio web REST que se puede usar para desarrollar soluciones mediante cualquier lenguaje y entorno de hospedaje que admita HTTPS y certificados X.509. La API se basa en Azure AD y el protocolo OAuth2 para la autorización y autenticación. Para acceder a la API desde la aplicación, primero deberá registrarla en Azure AD y configurarla con los permisos apropiados. Esto permitirá que la aplicación solicite los tokens de acceso OAuth2 que necesita para llamar a la API.

55. Para más información se puede consultar **Referencia de la API de Actividad de administración de Office 365 (REF7).**

6.11 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.

6.12 FUNCIONES DE SEGURIDAD

57. Este apartado se debe consultar en la guía **CCN-STIC 885G Guía de configuración segura para Microsoft Defender for Office 365 (REF6).**

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 servicio:

    - 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 servicio.
    - Los administradores mantendrán sus credenciales de acceso al servicio seguras y protegidas.
    - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.
    - Revisar directivas de seguridad en las que la configuración es menos segura que la configuración del perfil protección estándar.

8. REFERENCIAS

REF1 Microsoft Office 365
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

REF2 Revisión de los requisitos de arquitectura de Microsoft Defender para Office 365 y los conceptos clave
https://learn.microsoft.com/es-es/microsoft-365/security/defender/eval-defender-office-365-architecture?view=o365-worldwide

REF3 Introducción a Microsoft Defender para Office 365
https://learn.microsoft.com/es-es/microsoft-365/security/office-365-security/mdo-deployment-guide

REF4 Roles integrados de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/role-based-access-control/permissions-reference

REF5 Documentación de autenticación de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/authentication/

REF6 CCN-STIC 885G Guía de configuración segura para Microsoft Defender for Office 365
https://www.ccn-cert.cni.es/es/series-ccn-stic/guias/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/6350-ccn-stic-885g-gcs-para-microsoft-defender-for-office-365/file.html

REF7 Referencia de la API de Actividad de administración de Office 365
https://learn.microsoft.com/es-es/office/office-365-management-api/office-365-management-activity-api-reference

REF8 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

REF9 Asignar o anular la asignación de licencias para los usuarios del Centro de administración de Microsoft 365
https://learn.microsoft.com/es-es/microsoft-365/admin/manage/assign-licenses-to-users?view=o365-worldwide

9. ABREVIATURAS

AD	Directorio Activo
AES	Advanced Encryption Standard
API	Application Programming Interface
CCN	Centro Criptográfico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
ENS	Esquema Nacional de Seguridad.
EOP	Exchange Online Protection
HTTPS	Hyper Text Transfer Protocol Secure
MDOP1	Microsoft Defender for Office P1
MDOP1	Microsoft Defender for Office P2
MFA	Autenticación Multifactor
NTP	Network Time Protocol
OAuth2	Open Authorization 2.0
RBAC	Control de Acceso Basado en Roles
REST	REST Representational State Transfer
TLS	Transport Layer Security
TOE	Target Of Evaluation

PUBLICACIONES DE DEFENSA

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