centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1228

Procedimiento de Empleo Seguro
Microsoft Defender for Endpoint

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

NIPO: 083-24-144-9.
Fecha de Edición: abril de 2024.

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 09:31:41 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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

ÍNDICE

1 INTRODUCCIÓN

1. Microsoft Defender for Endpoint forma parte de la suite de seguridad integrada Microsoft 365 Defender. Es una plataforma de seguridad de extremo de empresa diseñada para ayudar a las redes empresariales a prevenir, detectar, investigar y responder a amenazas avanzadas.

2. Microsoft Defender for Endpoint utiliza una combinación de tecnología integrada en Windows 10 y el servicio de la nube de Microsoft:

   - Sensores de comportamiento de extremo: integrados en Windows 10, estos sensores recopilan y procesan señales de comportamiento del sistema operativo y envían estos datos del sensor a la instancia privada de la nube de Microsoft Defender for Endpoint.
   - Inteligencia de amenazas: generada por los hunters de Microsoft (equipo de buscadores expertos en amenazas cibernéticas de Microsoft), equipos de seguridad y enriquecida por la inteligencia de amenazas proporcionada por otros partners, la inteligencia de amenazas permite a Defender for Endpoint identificar herramientas, técnicas y procedimientos de atacantes y generar alertas cuando se observan en datos de sensor recopilados.
   - Análisis de seguridad en la nube: Al aprovechar los macrodatos (big-data), el aprendizaje de dispositivos y la óptica exclusiva de Microsoft en todo el ecosistema de Windows, los servicios empresariales de la nube (como Office 365) y los activos en línea, las señales de comportamiento se traducen en conocimientos, detecciones y respuestas recomendadas a amenazas avanzadas.

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 for Endpoint. 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) dentro de la Familia de EDR (Endpoint Detection and Response) de la taxonomía definida por el Centro Criptológico Nacional en la guía CCN-STIC 140.

3 ORGANIZACIÓN DEL DOCUMENTO

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

5. 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.
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 podrá activar las licencias por cada usuario dentro de la plataforma (ver sección **4.3**).

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. Al ser un servicio en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.
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 servicio.

4.3 REGISTRO Y LICENCIAS

11. Para que el cliente pueda hacer uso de la plataforma al tratarse de un servicio en la nube, el cliente deberá adquirir una licencia de Microsoft Defender for Endopoint a través de la plataforma puede ver más información en **Requisitos previos de Microsoft Defender for Endpoint (REF2)**.

4.4 CONSIDERACIONES PREVIAS

12. Como corresponde a un servicio 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.
13. Los prerrequisitos necesarios para la implementación del servicio se pueden consultar en las secciones 1.4 y 1.5 de la guía CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint **(REF4)**.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. El servicio consta de los siguientes componentes principales:
    - **Servicio en la nube:** espacio del usuario en la nube accesible mediante el uso de Microsoft Defender Portal.
    - **API:** conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
    - **Endpoint:** componentes de seguridad en el *endpoint*.
15. **El servicio no requiere de otros componentes externos para cumplir con su funcionalidad de seguridad.**

16. El servicio consta de otros componentes dentro de la infraestructura del propio fabricante que trabajan juntos para proporcionar la completa protección de los endpoints. Estos componentes no son completamente transparentes a los usuarios finales:

    - **Descubrimiento de activos:** El servicio utiliza la detección de activos para encontrar los dispositivos de red y el punto final para evaluarlos y protegerlos. Utiliza puntos de conexión ya incorporados para recopilar, sondear o escanear la red para detectar dispositivos no administrados.
    - **Gestión de amenazas y vulnerabilidades:** Identificar, evaluar y corregir las debilidades de los puntos finales.
    - **Reducción de la superficie de ataque:** La reducción de la superficie expuesta a ataques ayuda a reducir la superficie expuesta a ataques y se considera un elemento de protección clave, especialmente para clientes desconectados (sin conectividad a Internet).
    - **Protección de última generación:** Heurística basada en el comportamiento y solución antivirus en tiempo real con tecnología de Microsoft Defender Antivirus.
    - **Detección y respuesta de *endpoints*:** Detecciones avanzadas de ataques y visibilidad del alcance total de una infracción.
    - **Investigación y corrección automáticas:** Corrección automática de los activos comprometidos.
    - **Expertos en amenazas de Microsoft:** Microsoft Threat Experts es el servicio administrado de búsqueda de amenazas y tiene dos componentes. En primer lugar, las acciones de ataques dirigidos proporcionan información y análisis especiales que ayudan a identificar y responder a las amenazas más críticas de forma rápida y precisa. Y el segundo es Experts on Demand. Puede ponerse en contacto con los expertos en amenazas de Microsoft, que le proporcionarán una consulta técnica sobre las detecciones y los adversarios relevantes.
    - **Configuración y administración centralizadas:** El servicio se puede utilizar como un lugar central para configurar la línea de base y los ajustes de seguridad individuales de los puntos de conexión. El servicio se puede integrar con otras soluciones mediante el uso de las API. Los clientes pueden integrar el servicio con sus infraestructuras de seguridad existentes mediante el uso de un amplio conjunto de API. Para ello, el portal de Microsoft Defender se usa para supervisar y ayudar a responder a alertas de posibles infracciones de datos o actividad de amenazas persistentes avanzadas.

5 FASE DE INSTALACIÓN

17. 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 Endpoint.

5.1 ALTA DEL SERVICIO EN LA NUBE

18. Al tratarse de un servicio alojado en la nube, el proveedor dará de alta los datos del cliente y le enviará sus datos de acceso de forma segura a los accesos pertinentes del servicio.

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 DESPLIEGUE DE MICROSOFT DEFENDER FOR ENDPOINT

20. Este apartado esta descrito en la sección 2 de la guía CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint **(REF4)**.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

21. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el servicio.

22. 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 cada interacción con el servicio.

23. 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.

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

25. El sensor que se instala en la infraestructura del cliente establece por defecto una conexión segura con el servicio en la nube mediante el uso de TLS1.2.

26. El servicio puede conectarse con el gestor de eventos de Microsoft Sentinel o a uno externo mediante API REST. Siempre usando TLS1.2 para las comunicaciones seguras. Se recomienda el uso de Microsoft Sentinel por su total integración. Para configurar la integración con Microsoft Sentinel, ver la sección 1.3.2 de la guía CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint **(REF4)**.

6.2 AUTENTICACIÓN

27. 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. En el caso del sensor, se utilizan las credenciales locales del sistema operativo y se autentica mediante la sesión de inicio de sesión.

28. 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.

29. 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.

30. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure **(REF5)**.

6.3 ADMINISTRACIÓN DEL SERVICIO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. Al tratarse de un servicio en la nube siendo 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.
32. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

33. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del servicio se realiza de forma remota.
34. 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.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

6.5 GESTIÓN DE CERTIFICADOS

36. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure y los certificados usan RSA con longitud de clave de 2048 bits.

6.6 SERVIDORES DE AUTENTICACIÓN

37. 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 (**REF5**).
38. En el caso del sensor, se utilizan las credenciales locales del sistema operativo y se autentica mediante la sesión de inicio de sesión.

6.7 SINCRONIZACIÓN

39. 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

40. 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

41. 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

42. 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 (*sing-ins*) se registran con los siguientes estados descritos:
        - Éxito: inicio de sesión exitoso.
        - Error: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.
        - Interrumpido: la contraseña del usuario ha caducado y, por lo tanto, su inicio de sesión o sesión ha finalizado. Donde se le pregunta 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 del servicio seleccionando la categoría adecuada:
        - Rol agregado/modificado/eliminado.
        - Cambios en la política de retención de datos.
        - Establecer funciones avanzadas (habilitar/deshabilitar la investigación automatizada, la respuesta en vivo, permitir o bloquear el archivo).
    - Eventos relacionados con la funcionalidad del servicio buscando la categoría adecuada en las actividades (actividades de respuesta):
        - Se ejecutó un análisis antivirus.
        - Dispositivo aislado.
        - Paquete de *onboarding* descargado.

43. 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.

44. 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

45. 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.

6.10.3 ALMACENAMIENTO REMOTO

46. El servicio puede conectarse con un gestor de eventos externo mediante API REST. Siempre usando TLS1.2 para las comunicaciones seguras.

47. Para ver los detalles de la configuración, se puede consultar la sección 4.1.3 de la guía CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint **(REF4)**.

6.11 BACKUP

48. Las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

6.12 FUNCIONES DE SEGURIDAD

49. Este apartado se debe consultar en la guía CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint **(REF4).**

7 FASE DE OPERACIÓN

50. 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.

51. 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.

8 REFERENCIAS

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

REF2 Requisitos previos de Microsoft Defender for Endpoint
https://learn.microsoft.com/es-es/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

REF3 MDE-DOC
Documentación Microsoft Defender for Endpoint (9/9/2022)
https://learn.microsoft.com/es-es/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide#licensing-requirements

REF4 CCN-STIC-885E – Guía de configuración segura para Microsoft Defender for Endpoint
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/6254-ccn-stic-885e-guia-de-configuracion-segura-para-microsoft-defender-for-endpoint/file.html

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

9 ABREVIATURAS

AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
EDR	Endpoint Detection and Response
HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
MFA	Multi-Factor Authentication
NTP	Network Time Protocol
RBAC	Role Based Access Control
STIC	Seguridad TIC
TLS	Transport Layer Security
URL	Uniform Resource Locator

PUBLICACIONES DE DEFENSA

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