Guía de Seguridad de las TIC
CCN-STIC 1307

Procedimiento de Empleo Seguro
Azure Monitor Log Analytics

Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:26:10 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1. Azure Monitor es una solución integral para la recolección, análisis y respuesta a los datos de monitorización de entornos en la nube y locales. Azure Monitor incluye distintas capacidades, entre ellas métricas, registros, trazas, cambios, alertas y visualizaciones. Azure Monitor Logs y Log Analytics corresponden a las capacidades orientadas al almacenamiento, consulta y análisis de registros.
2. Azure Monitor recoge y agrega los datos de cada capa y componente del sistema a través de múltiples suscripciones e inquilinos de Azure y no Azure. Los almacena en una plataforma de datos común para su consumo por un conjunto de herramientas que pueden correlacionar, analizar, visualizar y/o responder a los datos. También puede integrarse con otras herramientas de Microsoft u otras herramientas.
3. Azure Monitor puede monitorear los siguientes tipos de recursos en Azure, otras nubes o entornos locales:
    a) Aplicaciones
    b) Máquinas virtuales
    c) Sistemas operativos invitados
    d) Contenedores, incluyendo métricas de Prometheus
    e) Bases de datos
    f) Eventos de seguridad en combinación con Azure Sentinel
    g) Eventos de red y estado en combinación con Network Watcher
    h) Fuentes personalizadas que usan las APIs para obtener datos en Azure Monitor
4. También es posible exportar los datos de monitoreo desde Azure Monitor a otros sistemas para:
    a) Integrarse con otras herramientas de monitoreo y visualización de terceros y de código abierto.
    b) Integrarse con sistemas de tickets y otros sistemas de ITSM (gestión de servicios de TI).
5. Para más información sobre el producto, consultar la guía **Documentación sobre Azure Monitor** [REF1].

2 OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía para realizar el alta, configuración y uso seguro del servicio Azure Monitor Log Analytics.

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

3 ORGANIZACIÓN DEL DOCUMENTO

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

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

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

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

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Al tratarse de un servicio en la nube, se dará de alta los datos del cliente en la plataforma de **Microsoft Azure Portal** [REF2] y se enviarán de forma segura los accesos pertinentes a la plataforma.
9. El envío de los datos se realizará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
10. Una vez dado el alta en la plataforma se podrán activar las licencias para cada usuario dentro de la plataforma.

4.2 ENTORNO DE INSTALACIÓN SEGURO

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

4.3 REGISTRO Y LICENCIAS

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

4.4 CONSIDERACIONES PREVIAS

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

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

16. El producto consta de los siguientes componentes principales:
    a) Azure Monitor / Log Analytics: servicio de Azure accesible y administrable mediante Azure Portal y la capa de gestión de Azure, que permite recopilar, almacenar, consultar, analizar y exportar registros y datos de monitorización.
    b) API: Conexión con otras soluciones de seguridad de Microsoft o sistemas de terceros.
17. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    a) Azure Portal: acceso al portal de gestión.
    b) Entra ID: autenticación de usuarios, acceso condicional, políticas.
    c) Tipo de fuente de datos (alcance): Azure Platform
    d) Azure Storage: Solución de almacenamiento en la nube.
    e) Azure Gateway: equilibrador de carga de tráfico web.

f) Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.

18. Los componentes anteriores se interrelacionan a través del plano de administración de Azure. El acceso de los administradores se realiza mediante Azure Portal, previa autenticación con Microsoft Entra ID. Azure Monitor / Log Analytics recoge y procesa la información procedente de las fuentes de datos configuradas y puede almacenar o exportar los registros hacia Azure Storage, Azure Event Hubs o áreas de trabajo de Log Analytics, según la configuración establecida.

5 FASE DE INSTALACIÓN

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

5.1 ALTA DEL SERVICIO EN LA NUBE

20. Al tratarse de un servicio en la nube, se requiere el alta en el portal de Microsoft Azure Portal adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del servicio.
21. Una vez que se encuentre dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 ACTIVACIÓN AZURE MONITOR LOG

22. El proveedor proporciona documentación acerca de Azure Monitor Logs y Log Analytics en las guías **Introducción a los registros de Azure Monitor** [REF10] y **Creación de áreas de trabajo de Log Analytics** [REF16].

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

23. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. Para más información sobre el producto se debe consultar la guía **Azure Monitor Overview** [REF3]**.**
24. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por Microsoft Entra ID antes de cualquier interacción con el producto.
25. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

26. El producto usa la infraestructura de Azure vinculado a Microsoft Entra ID, para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.
27. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC).
28. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, y al mismo tiempo mantiene la simplicidad para los usuarios. Proporciona más seguridad, ya que requiere una segunda forma de autenticación y ofrece autenticación segura a través de una variedad de métodos de autenticación.
29. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF4].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

30. Al ser un producto en la nube que forma parte de la infraestructura de Microsoft Azure, la administración se realiza de forma remota utilizando el protocolo seguro HTTPS con TLS 1.2 o superior para el establecimiento de las comunicaciones seguras.
31. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

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

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

34. El producto utiliza Azure RBAC (Control de Acceso Basado en Roles) para gestionar el acceso a los recursos de Azure asociados al servicio, incluyendo el área de trabajo de Log Analytics, las reglas de recopilación de datos, las configuraciones de diagnóstico y los recursos de destino de exportación. Para la configuración y administración del servicio, se deberán asignar los roles necesarios conforme al principio de mínimo privilegio. Entre los roles integrados relevantes se incluyen:

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

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

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

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

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

36. El producto utiliza Microsoft Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad haciendo uso de la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:

    a) Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 3 intentos fallidos.

    b) Duración del bloqueo: 5 minutos.

37. Para más información sobre los diferentes mecanismos de seguridad de la tecnología Smart Lockout y cómo modificar los valores establecidos, se puede consultar la siguiente guía, **Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra [REF5]**.

38. El producto utiliza Microsoft Entra ID para la gestión de cuentas y directivas de contraseñas. Estas directivas se aplican a las cuentas de usuario y administrador creadas y administradas directamente en Microsoft Entra ID. Los siguientes requisitos se aplican a las contraseñas que se crean, cambian o restablecen en Microsoft Entra ID:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > Espacio en blanco

Caracteres no permitidos	Caracteres unicode
Longitud de la contraseña	Un mínimo de 12 caracteres y un máximo de 256.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos
Contraseña no utilizada recientemente	Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser la misma que la contraseña actual ni coincidir con las 10 contraseñas anteriores.

Tabla 1. Política de contraseñas

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

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

6.5 GESTIÓN DE CERTIFICADOS

41. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure los certificados usan RSA con longitud de clave de 2048 bits. Este cifrado es suficientemente robusto y, aunque se considera seguro para las comunicaciones en el momento de creación de este documento, se recomienda la utilización de RSA con longitud de clave de 3072 bits.

42. Para la gestión y configuración de la longitud de clave ver la subsección “Creación de claves” de la sección “3.1.2.2 Protección de claves criptográficas” de la guía **CCN-STIC-884A** [REF4]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

43. El acceso al producto se realiza a través de la interfaz web, requiriendo la autenticación previa de los usuarios mediante Microsoft Entra ID antes de cualquier interacción con el producto.

6.7 SINCRONIZACIÓN

44. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.8 ACTUALIZACIONES

45. Las actualizaciones se realizan automáticamente cuando están disponibles. Este proceso está completamente controlado por el CSP (Proveedor de Servicios en la Nube) porque el servicio es parte de la infraestructura de Azure.

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

6.9 AUTO-CHEQUEOS

47. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube realiza los auto-chequeos (self-test) de integridad del software y de la operación de los algoritmos y funciones criptográficas del producto de manera automatizada.

6.10 ALTA DISPONIBILIDAD

48. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

49. El producto Azure Monitor Log se encarga de auditar todos los eventos que se generan por el propio producto y otros servicios de Azure. 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]**.**

50. El servicio genera registros de auditoría clasificados por actividades que se auditan en la infraestructura de Azure, para más información se puede consultar la guía **Esquema de eventos del registro de actividad de Azure** [REF8**].** Se pueden buscar estos eventos buscando el Activity Log en el portal de seguridad y cumplimiento, seleccionando las siguientes categorías:

    a) Operaciones de gestión de roles como crear/ver/eliminar asignaciones de roles y crear/ver/eliminar definiciones de roles personalizados.

    b) Cambios en la configuración del sistema. Cuando hay un cambio o modificación en la configuración, se guarda el evento.

    c) Proceso de inicio de sesión del personal autorizado (estos eventos proceden de la integración con Entra ID). Debido a la arquitectura y modo de operación de la infraestructura Azure, la plataforma utiliza la capacidad de sesiones y no hay eventos de cierre de sesión. Los inicios de sesión (sign-ins) se registran con los siguientes estados descritos:

        i. Éxito: inicio de sesión exitoso.
        ii. Fallo: Error al validar las credenciales debido a que el nombre de usuario o la contraseña no son válidos.

iii. Interrumpido: La contraseña del usuario ha caducado, por lo que su login o sesión ha sido finalizado. Cuando se pregunta al usuario si desea seguir conectado a este navegador para facilitar el inicio de sesión en el futuro.

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

    a) "Métricas" tienen una retención de 93 días,

    b) "Logs" son configurables hasta 12 años a través de Azure Portal y API, y 7 años a través de PowerShell.

52. Los registros de auditoría de Azure Monitor Log no pueden ser eliminados por cualquier usuario. Solo se pueden eliminar registros cuando el periodo de retención ha concluido. Este periodo por defecto es de 30 días, pero la retención se puede modificar y establecer en: 31, 60, 90, 120, 180, 270, 365, 550 y 730 días, teniendo en cuenta que la modificación de este periodo supone un coste económico adicional. Se puede también activar el periodo de archivo a una retención total de 4.383 (12 años) usando el Azure Storage.

6.11.2 ALMACENAMIENTO LOCAL

53. 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

54. 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.

55. Para más información sobre cómo realizar el envío de registros a los recursos de Azure mencionados, se puede consultar la siguiente guía, **Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage** [REF9].

6.12 BACKUP

56. Al tratarse de un servicio en la nube, las copias de seguridad y la disponibilidad de la plataforma son gestionadas por el proveedor en su plataforma de Microsoft Azure. Para los datos almacenados en Log Analytics, la organización cliente deberá configurar los períodos de retención y archivo de acuerdo con sus necesidades, teniendo en cuenta los planes de tabla y la retención de datos disponibles en Azure Monitor Logs.

57. Para más información sobre los planes de tabla y la retención de datos, consultar las guías **Selección de un plan de tabla basado en el uso de datos** [REF17] y **Administración de la retención de datos en un área de trabajo de Log Analytics** [REF18].

7 FASE DE OPERACIÓN

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

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

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

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

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

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

60. Azure Monitor Log 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 MONITORIZACIÓN DE APLICACIONES EN LA NUBE

62. La página de Monitorización de Aplicaciones en la Nube con Azure Monitor ofrece un panel diseñado para mostrar información detallada sobre el uso y rendimiento de las aplicaciones de la organización.

63. Este panel proporciona una visión general de las métricas y registros asociados a las aplicaciones, permitiendo identificar tendencias, detectar anomalías y garantizar un rendimiento óptimo.

64. Además, facilita la configuración de alertas personalizadas para notificar sobre eventos críticos o comportamientos inusuales en las aplicaciones.

65. Para obtener más información sobre cómo utilizar Azure Monitor para supervisar sus aplicaciones en la nube, consultar la guía **Información general sobre las métricas en Microsoft Azure** [REF11].

7.2 ANÁLISIS DE DATOS DE TRÁFICO DE RED

66. El producto analiza diferentes tipos de datos provenientes del tráfico de red haciendo uso de la herramienta **Azure Network Watcher** [REF12], permitiendo así obtener información clave para evaluar el rendimiento y la seguridad de la red.

67. Entre los datos más importantes que se analizan se incluyen los provenientes de los servicios de **Microsoft.Network**, **Microsoft.NetworkAnalytics**, **Microsoft.NetworkCloud** y **Microsoft.NetworkFunction**, cubriendo al menos los siguientes parámetros:
    a) Dirección IP de origen
    b) Dirección IP de destino
    c) Puerto de origen
    d) Puerto de destino
    e) Protocolo
68. Estos datos permiten obtener una visión completa de los flujos de tráfico en la red, asegurando que los sistemas de la organización puedan ser supervisados de manera eficiente y efectiva.

7.3 CAPTURA DE PAQUETES DE RED

69. El producto, mediante la captura de paquetes de **Azure Network Watcher**, crea sesiones de captura para rastrear el tráfico hacia y desde una máquina virtual o un conjunto de escalado.
70. Esta funcionalidad permite analizar en detalle los flujos de red, lo que facilita la identificación de problemas y el monitoreo de la comunicación entre los componentes de la infraestructura.
71. Además, se puede aplicar filtrado para capturar solo el tráfico definido por el usuario, utilizando parámetros como:
    a) Protocolo
    b) Dirección IP local
    c) Dirección IP remota
    d) Puerto local
    e) Puerto remoto
72. Para obtener más información sobre cómo configurar y utilizar la captura de paquetes con Azure Network Watcher, consultar la guía **Introducción a la captura de paquetes** [REF13].

7.4 EXPORTACIÓN DE LOGS

73. El producto permite exportar registros según el tipo de recurso que el administrador esté utilizando, ofreciendo flexibilidad en el formato de salida.
74. Los resultados de las consultas se pueden exportar a varios formatos, incluyendo:
    a) CSV
    b) Excel
    c) Power BI
75. Esta capacidad de exportación facilita el análisis y la visualización de los datos en diferentes herramientas, permitiendo un uso eficiente de la información generada.

76. Para obtener más información sobre cómo exportar registros en diferentes formatos, consultar la guía **Exportación de datos del área de trabajo de Log Analytics en Azure Monitor** [REF14].

7.5 REGISTRO DE ACTIVIDAD Y CAMBIOS

77. El producto dispone de registros que incluyen la tabla **Azure Activity**, la cual contiene toda la actividad monitoreada por **Azure Monitor** para un recurso específico. Además, se incluyen métricas que indican cómo ha cambiado el uso del recurso a lo largo del tiempo, proporcionando una visión detallada de la evolución de su rendimiento y utilización.

78. Adicionalmente, cuenta con un **Change Data Store**, que contiene una serie de eventos relacionados con aplicaciones y recursos. Estos eventos son rastreados y almacenados cuando se utiliza el servicio **Change Analysis**, que se apoya en **Azure Resource Graph** como su repositorio de datos.

79. Para obtener más información sobre los registros de actividad y el análisis de cambios, consultar la guía **Documentación de Azure Resource Graph** [REF15].

8 REFERENCIAS

[REF1] Documentación sobre Azure Monitor
https://learn.microsoft.com/es-es/azure/azure-monitor/

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

[REF3] Azure Monitor Overview
https://learn.microsoft.com/es-es/azure/azure-monitor/fundamentals/overview

[REF4] CCN-STIC-884A Guía de configuración segura para Azure
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/4253-ccn-stic-884a-guia-de-configuracion-segura-para-azure/file.html

[REF5] Protección de las cuentas de usuario frente a ataques con el bloqueo inteligente de Microsoft Entra
https://learn.microsoft.com/es-es/entra/identity/authentication/howto-password-smart-lockout

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

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

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

[REF9] Envío de registros de recursos de Azure a áreas de trabajo de Log Analytics, Event Hubs o Azure Storage
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/resource-logs

[REF10] Introducción a los registros de Azure Monitor
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/data-platform-logs

[REF11] Información general sobre las métricas en Microsoft Azure
https://learn.microsoft.com/es-es/azure/azure-monitor/essentials/data-platform-metrics

[REF12] Documentación de Network Watcher
https://learn.microsoft.com/es-es/azure/network-watcher/

[REF13] Introducción a la captura de paquetes
https://learn.microsoft.com/es-es/azure/network-watcher/packet-capture-overview

[REF14] Exportación de datos del área de trabajo de Log Analytics en Azure Monitor
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/logs-data-export

[REF15] Documentación de Azure Resource Graph
https://learn.microsoft.com/es-es/azure/governance/resource-graph/

[REF16] Creación de áreas de trabajo de Log Analytics
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/quick-create-workspace

[REF17] Selección de un plan de tabla basado en el uso de datos
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/logs-table-plans

[REF18] Administración de la retención de datos en un área de trabajo de Log Analytics
https://learn.microsoft.com/es-es/azure/azure-monitor/logs/data-retention-configure

9 ABREVIATURAS

API	Interfaz de Programación de Aplicaciones
CCN	Centro Criptográfico Nacional.
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSP	Cloud Service Provider
ENS	Esquema Nacional de Seguridad.
HTTPS	Secure Hyper Text Transfer Protocol.
ITSM	IT Service Management
MFA	Autenticación Multifactor.
NTP	Network Time Protocol
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman
TLS	Transport Layer Security.