centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1517

Procedimiento de Empleo Seguro
Microsoft Purview Communication Compliance

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: 083-26-134-6

Fecha de Edición: Octubre de 2025

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.05.05 10:46:30 +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. Communication compliance de Microsoft Purview es una solución de riesgo interno que le ayuda a detectar, capturar y actuar sobre mensajes inadecuados que pueden dar lugar a posibles incidentes de seguridad de datos o cumplimiento dentro de su organización. El cumplimiento de comunicaciones evalúa los mensajes basados en imágenes y texto en Aplicaciones de Microsoft y de terceros (Teams, Microsoft Copilot para Microsoft 365, Viva Engage, Outlook, WhatsApp, etc.) en busca de posibles infracciones de directivas empresariales, incluido el uso inadecuado de compartir información confidencial, lenguaje amenazante o hostigador, así como posibles infracciones normativas (como manipulaciones de acciones y capital).
2. El producto usa modelos de Machine Learning y patrones de teclado para identificar mensajes que contengan potenciales violaciones de conductas de empresa y directivas de administración, que posteriormente serán revisadas por un investigador. El producto utiliza un acceso de control basado en roles que cultiva la privacidad del usuario mediante la pseudo-anonimación y el uso responsable del producto.
3. El producto ayuda a las organizaciones permitiendo detectar, clasificar y remediar las comunicaciones que supongan una posible violación de la conducta de la empresa o de la regulación de conformidad.
4. Ofrece las siguientes plantillas de directivas que usan clasificadores de Machine Learning para los usuarios:
   - Business conduct: Discriminación, Insultos, Amenazas y Clasificadores de acoso selectivo.
   - Regulatory compliance: Sabotaje corporativo, Quejas de clientes, Regalos y Entretenimiento, Lavado de dinero, Colisión normativa, Manipulación de acciones y Clasificadores de divulgación no autorizados.
5. El producto puede ayudar a revisar los mensajes en la organización en varias áreas importantes de cumplimiento:
   - Políticas corporativas: Los usuarios deben cumplir con el uso aceptable, las normas éticas y otras políticas corporativas en todas sus comunicaciones relacionadas con la empresa.
   - Gestión de riesgos: Las organizaciones son responsables de todas las comunicaciones distribuidas por su infraestructura y sistemas de red corporativos. El uso de políticas de cumplimiento de las comunicaciones para ayudar a identificar y gestionar la posible exposición legal y el riesgo puede ayudar a minimizar los riesgos antes de que puedan dañar las operaciones corporativas.
   - Cumplimiento normativo: La mayoría de las organizaciones deben cumplir algún tipo de norma de cumplimiento normativo como parte de sus procedimientos operativos normales.
6. Las políticas de cumplimiento de las comunicaciones comprueban, detectan y capturan mensajes en varios canales de comunicación para ayudarle a revisar y corregir rápidamente los problemas de cumplimiento:
   - Microsoft Teams
   - Exchange Online
   - Microsoft Copilot para Microsoft 365

- Viva Engage

7. Cumplimiento de las comunicaciones:
   - El cumplimiento de las comunicaciones ayuda a abordar los puntos débiles comunes asociados con el cumplimiento de las políticas internas y los requisitos de cumplimiento normativo. Con plantillas de políticas centradas y un flujo de trabajo flexible, puede utilizar información procesable para resolver rápidamente los problemas de cumplimiento detectados.
   - Identificar y resolver problemas de cumplimiento con la comunicación usa el siguiente esquema de trabajo:
     - Configurar: Es el paso de trabajo siguiente en la cadena de procesos de cumplimiento de la comunicación. En este paso, se identifica la configuración de cumplimiento requerida y se configuran las políticas de cumplimiento de la comunicación aplicables.
     - Investigar: En este paso, se puede profundizar más en los problemas detectados, como coincidencias con las políticas de cumplimiento de la comunicación.
     - Remediar: El siguiente paso es remediar los problemas de cumplimiento de la comunicación que hayan sido investigados.
8. Para obtener más información puede consultar **Cumplimiento de comunicaciones** [REF1]**.**
9. Microsoft Purview dispone de funcionalidades compatibles con sitios de inteligencia artificial de terceros, como ChatGPT, Google Gmini y DeepSeek. Los admitidos se pueden consultar en **la lista de sitios de IA admitidos** [REF14] y el listado de dichas funcionalidades se puede consultar en **Uso de Microsoft Purview para administrar la seguridad de datos & cumplimiento de otras aplicaciones de inteligencia artificial** [REF15]**.**

2 OBJETO Y ALCANCE

10. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Purview Communication Compliance.
11. Este servicio se sitúa dentro de la Familia de “Otras herramientas” de la tipología definida por el CCN (CPSTIC) para categoría ENS 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

12. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Purview Portal** [REF2] y se enviarán de forma segura los accesos pertinentes a la plataforma.
13. El envío de los datos se relacionará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
14. 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

15. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras.

4.3 REGISTRO Y LICENCIAS

16. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
17. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para las comunicaciones seguras. Sólo los usuarios autorizados y con la licencia activa podrán acceder al producto.
18. Se requiere la obtención de una licencia de Microsoft 365 E5. Más información en Microsoft 365 Licenses [REF3].

4.4 CONSIDERACIONES PREVIAS

19. 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

20. El producto forma parte de la solución Data Security del servicio Microsft Purview, que se suma a las soluciones de Data Governance y Complience Solutions.
21. El producto está compuesto de los siguientes tres componentes principales:
    - Cloud: Un cliente inquilino en la nube que es accesible a través del portal de Microsfot Purview.
    - API: Una señal compartida con otras soluciones de seguridad de Microsoft y otros sistemas externos (conectores de Información).
    - Scope: Dónde las políticas van a ser aplicadas.
22. Los siguientes servicios de Microsoft Azure serán considerados como parte del entorno de operación:
    - Azure Portal: acceso al portal de gestión.

- Entra ID: autenticación de usuarios, acceso condicional, políticas.
- Azure Gateway: equilibrador de carga de tráfico web.
- Azure WAF: protección de aplicaciones web contra ataques de bots y vulnerabilidades web comunes.
- Azure Monitor Activity Log: registro de la plataforma que proporciona información sobre los eventos a nivel de suscripción.
- Azure Events Hub: servicio de flujo de datos utilizado para recopilar, transformar y almacenar eventos.
- Azure Key Vault Managed HSM: claves criptográficas y secretos.
- Servicios MS365: Teams, Exchange Online, Copilot, Viva.

5 FASE DE INSTALACIÓN

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

    - Alta del servicio en Microsoft 365 E5.
    - Activación de Microsoft Purview Communication Compliance.

5.1 ALTA DEL SERVICIO EN LA NUBE

24. 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.

25. 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 PURVIEW COMMUNICATION COMPLIANCE

26. El proveedor proporciona documentación acerca de la activación y uso de licencia para poder hacer uso de la funcionalidad del producto. Consultar la sección “Suscripciones y licencias” de la guía **Introducción al cumplimiento de las comunicaciones** [REF4]**.**

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

27. 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 completa de Microsoft Purview** [REF5]**.**
28. 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.
29. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC, puede utilizar varios roles (Azure integrado y Purview). Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

6.2 AUTENTICACIÓN

30. 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.
31. 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
32. 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.
33. Más información en la guía CCN-STIC-884A Guía de configuración segura para Azure [REF6].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

34. 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.
35. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

36. 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.
37. El producto utiliza Microsoft Entra ID para que los usuarios se autentiquen antes de cualquier interacción del TOE accediendo a través de la interfaz web y cloud shell.
38. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Microsoft Entra ID. Un rol concede los permisos

para hacer una serie de tareas y un grupo de roles es un conjunto de roles que permite a los usuarios hacer sus labores dentro del producto. Un usuario puede formar parte de varios roles (roles predeterminados de Azure o de Purview).

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

- Global administrator (predeterminado de Azure): Puede acceder a todas las funcionalidades administrativas en todos los servicios de Microsoft 365. Solo los Global administrators pueden asignar roles administrativos.
- Security administrator (predeterminado de Azure): Controla la seguridad general de la organización mediante la administración de las políticas de seguridad, revisando análisis de seguridad y reportes de los productos de Microsoft 365, y manteniéndose actualizado con las amenazas más recientes.
- Global reader (predeterminado de Azure): Es la versión de solo lectura del Global Administrator. Puede visualizar todos los ajustes e información administrativa de Micrososft 365.
- Compliance Administrator (Purview): Los miembros pueden administrar los ajustes del dispositivo para: gestiones, prevención de pérdida de datos, reportes y preservación.
- Compliance Manager Readers (Purview): Puede visualizar el contexto general del Compliance Manager excepto por las funciones administrativas.

40. El producto tiene capacidad para asignar 5 perfiles diferentes para los roles:

- Communication Compliance: gestionar todo.
- Communication Compliance Admins: Para configurar las políticas, gestionar los ajustes de privacidad y ver y exportar actualizaciones de políticas.
- Communication Compliance Analysts: Para acceder a las alertas e investigarlas.
- Communication Compliance Investigators: Acceder a las alertas e investigarlas, ver pestañas de Conversación y Traducción para un mensaje específico, tomar medidas de corrección avanzadas, como escalar para investigar/eliminar mensaje en Teams, descargar elementos y ejecutar flujos de Power Automate y crear informes de detalles de mensajes.
- Communication Compliance Viewers: Para acceder a informes y ver y exportar actualizaciones de políticas.

41. Para ampliar la información sobre los roles, se puede consultar la información proporcionada por el fabricante en la guía **Roles and role groups in Microsoft Defender for Office 365 and Microsoft Purview** [REF7]**.**

42. Para ampliar la información sobre los roles y permisos que se utilizan para gestionar las funcionalidades del producto, se puede consultar la información proporcionada por el fabricante en la guía **Permissions in the Microsoft Purview compliance portal** [REF8]**.**

43. El producto forma parte de la infraestructura Microsoft Azure. Las sesiones expiran después de un período establecido por el administrador en Microsoft Entra ID. Los valores pueden ser predeterminados o personalizados. Para más información se puede consultar la guía **Tiempo de espera de sesión inactiva para Microsoft 365** [REF9].[REF8]

44. El producto utiliza Entra ID para las cuentas, y se aplican diferentes mecanismos de seguridad como Smart Lockout. Smart Lockout protege las cuentas de usuario de ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar:

- 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.

45. 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** [REF10][REF9].

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

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

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

6.5 GESTIÓN DE CERTIFICADOS

48. 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.
49. 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** [REF6]**.**

6.6 SERVIDORES DE AUTENTICACIÓN

50. 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

51. 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

52. 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.
53. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

54. 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

55. 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

56. El producto usa Microsoft Entra ID para autenticar a cualquier usuario antes de cualquier interacción con el producto. Entra ID envía la información del inicio de sesión al Activity Log y debido a que el producto es parte de la infraestructura de Azure, usa el Audit Log de Microsoft 365 para auditar todos los eventos de generados por el producto.
57. Por lo tanto, todas las actividades son registradas en el Audit Log de Microsoft 365.
58. El registro de auditoría se muestra en la página de búsqueda de Audit Log. El producto genera registros de auditoría clasificados por actividades que se auditan en la infraestructura Azure. Los resultados de una búsqueda de registro de auditoría se muestran con la siguiente información:

    - Date(UTC): La fecha y hora cuando el evento ha ocurrido.
    - IP address: La dirección IP del dispositivo que se utilizó para realizar la actividad.
    - User: La cuenta de usuario que realizó la actividad.
    - Record Type: El tipo de registro asociado a la actividad.
    - Activity: El nombre amigable de la actividad que se realizó.
    - Item: El nombre del archivo, carpeta o sitio en el que se realizó la actividad.
    - Admin Units: La unidad de administración a la que pertenece la cuenta de usuario que realizó la actividad.
    - Detail: Detalles adicionales sobre la actividad.

59. Se pueden visualizar más detalles de un evento haciendo click en el registro de eventos en la lista de resultados de búsqueda. Se muestra una página emergente que contiene las propiedades detalladas del registro del evento. Las propiedades que se muestran dependen del servicio que ocasiona que ocurra el evento.
60. El producto genera registros de auditoría clasificados por actividades que se auditan en la infraestructura de Azure. Puedes buscar estos eventos buscando los registros de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:

    - Funciones de inicio y fin 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 gestionar ni el inicio ni el final.
    - Operaciones de gestión de roles como crear/ver/borrar asignación de roles y crear/ver/borrar definiciones de roles personalizados.
    - Cambios en la configuración del sistema:
        - Cambio en las credenciales de usuario (estos eventos provienen de la integración con Microsoft Entra ID).
        - Aplicar etiqueta a mensaje(s)
    - Proceso de inicio de sesión de personal autorizado (estos eventos provienen de la integración con Microsoft Entra ID). Debido a la arquitectura y modo de funcionamiento de la infraestructura Azure, la plataforma utiliza la capacidad 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.
        - Fallo: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.

  - Interrumpido: La contraseña del usuario ha caducado, por lo que su inicio de sesión o sesión ha sido finalizado. Cuando se le pregunta al usuario si desea seguir conectado a este navegador para facilitar inicios de sesión posteriores.
- Los siguientes cambios de política generaran eventos:
  - Actualización de política: Un administrador de cumplimiento de comunicación ha realizado una actualización de política.
  - Coincidencia de política: Un usuario ha enviado un mensaje que coincide con la condición de una política.
- Eliminación de eventos:
  - Los eventos no se pueden borrar. Los eventos se sobrescriben cuando la política de retención de datos es aplicada (180 días).
- Acciones correctivas:
  - **Resolver**: Después de revisar un problema, se puede remediar resolviendo la alerta.
  - **Etiquetar un mensaje**: Como parte de la resolución de un problema, se puede etiquetar una coincidencia de política como: Conforme, No conforme o Cuestionable en relación con las políticas y normas de su organización. También puede crear una etiqueta personalizada.
  - **Notificar al usuario**: A menudo, los usuarios infringen accidental o inadvertidamente una política de cumplimiento de la comunicación. Se puede utilizar la función de notificar para proporcionar un aviso de advertencia al usuario y resolver el problema.
  - **Pasar a otro revisor**: A veces, el revisor inicial de una incidencia necesita la opinión de otros revisores para ayudar a resolver el incidente. Se puede escalar fácilmente a revisores de otras áreas de una organización como parte del proceso de resolución.
  - **Informe mal clasificado**: Los mensajes detectados incorrectamente como coincidentes con las políticas de cumplimiento se cuelan ocasionalmente en el proceso de revisión. Se puede marcar este tipo de alertas como mal clasificadas, enviar comentarios a Microsoft sobre la clasificación errónea para ayudar a mejorar los clasificadores globales y resolver automáticamente el problema.
  - **Eliminar mensaje en Teams**: Los mensajes potencialmente inapropiados pueden eliminarse en los canales de Microsoft Teams o en los mensajes de chat personales y de grupo.
  - **Escalar para investigación**: En las situaciones más graves, es posible que se necesite compartir información sobre el cumplimiento de las comunicaciones con otros revisores de su organización. El cumplimiento de las comunicaciones está estrechamente integrado con otras funciones de Microsoft Purview para ayudarle en la resolución de riesgos de principio a fin. Escalar un caso para su investigación permite transferir los datos y la gestión del caso a Microsoft Purview eDiscovery (Premium).

61. Para más información sobre el registro de actividad de en Communication Compliance se debe consultar la guía **Actividades del cumplimiento de comunicaciones** [REF11][REF9]**.**

6.11.2 ALMACENAMIENTO LOCAL

62. Al tratare de un servidor en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada.

6.11.3 ALMACENAMIENTO REMOTO

63. La opción de enviar eventos de registros a un servidor no está disponible. Únicamente se pueden enviar los registros a una cuenta de Azure Storage o a Azure Event Hubs.

6.12 BACKUP

64. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Purview.

7 FASE DE OPERACIÓN

65. 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.

66. 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.

67. Communication Compliance de Microsoft Purview ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.

68. 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 ACCIONES RECOMENDADAS PARA COMMUNICATION COMPLIANCE

69. El proveedor proporciona una guía con acciones recomendadas que el cliente debe seguir para trabajar correctamente el cumplimiento de las comunicaciones.

70. Se deben seguir las acciones recomendadas de la guía de **Acciones recomendadas** [REF12].

7.2 CREACIÓN Y ADMINISTARCIÓN DE DIRECTIVAS DE COMMUNICATION COMPLIANCE

71. Las directivas de cumplimiento de comunicaciones para organizaciones de Microsoft 365 se crean desde el portal de cumplimiento de Microsoft Purview.

72. Las directivas de cumplimiento de comunicaciones definen qué comunicaciones y usuarios están sujetos a revisión en su organización, definen qué condiciones personalizadas deben cumplir las comunicaciones y especifican quién debe realizar revisiones.

73. Para más información de cómo crear y administrar estas directivas se debe consultar la guía **Crear y administrar directivas de cumplimiento de comunicaciones** [REF13]**.**

8 REFERENCIAS

[REF1] Cumplimiento de comunicaciones.
https://learn.microsoft.com/es-es/purview/communication-compliance-solution-overview

[REF2] Microsoft Purview Portal
https://purview.microsoft.com/

[REF3] Microsoft 365 licenses
https://www.microsoft.com/en-in/licensing?rtc=1

[REF4] Introducción al cumplimiento de las comunicaciones
https://learn.microsoft.com/es-es/purview/communication-compliance-configure?tabs=purview-portal#subscriptions-and-licensing

[REF5] Guía completa de Microsoft Purview
https://learn.microsoft.com/es-es/purview/

[REF6] 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

[REF7] Roles and role groups in Microsoft Defender for Office 365 and Microsoft Purview
https://learn.microsoft.com/en-us/defender-office-365/scc-permissions?view=o365-worldwide&toc=%2Fpurview%2Ftoc.json&bc=%2Fpurview%2Fbreadcrumb%2Ftoc.json

[REF8] Permissions in the Microsoft Purview compliance portal
https://learn.microsoft.com/en-us/purview/purview-compliance-portal-permissions

[REF9] Tiempo de espera de sesión inactiva para Microsoft 365
https://learn.microsoft.com/es-es/microsoft-365/admin/manage/idle-session-timeout-web-apps?view=o365-worldwide&WT.mc_id=365AdminCSH_inproduct

[REF10] 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

[REF11] Actividades del cumplimiento de comunicaciones
https://learn.microsoft.com/es-es/purview/audit-log-activities#communication-compliance-activities

[REF12] Acciones recomendadas
https://learn.microsoft.com/es-es/purview/communication-compliance-configure?tabs=purview-portal#recommended-actions

[REF13] Crear y administrar directivas de cumplimiento de comunicaciones
https://learn.microsoft.com/es-es/purview/communication-compliance-policies?tabs=purview-portal

[REF14] Lista de sitios de inteligencia artificial admitidos por Administración de postura de seguridad de datos de Microsoft Purview para IA
https://learn.microsoft.com/es-es/purview/ai-microsoft-purview-supported-sites

[REF15] Uso de Microsoft Purview para administrar la seguridad de datos & cumplimiento de otras aplicaciones de inteligencia artificial
https://learn.microsoft.com/es-es/purview/ai-other-apps

9 ABREVIATURAS

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.
CSP	Cloud Service Provider.
ENS	Esquema Nacional de Seguridad.
HTTP	Hyper Text Transfer Protocol.
HTTPS	HyperText Transfer Protocol Secure
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman.
TLS	Transport Layer Security.
TOE	Target of Evaluation.
WAF	Firewall de Aplicación Web.

PUBLICACIONES DE DEFENSA

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