centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1518

Procedimiento de Empleo Seguro
Microsoft Purview Information Protection

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 10:50:21
+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. El cliente de Microsoft Purview Information Protection ayuda a clasificar y etiquetar los datos de su organización en el momento de la creación, así como a aplicar la protección, en función de los derechos de cifrado y uso de los datos confidenciales.
2. Las etiquetas y la protección son persistentes, viajan con los datos a lo largo de su ciclo de vida, de modo que sea detectable y controlado en todo momento, independientemente de dónde se almacene o con quién se comparta, interna o externamente.
3. Estas funcionalidades de protección de la información proporcionan las herramientas necesarias para:

   - Conocer los datos de la organización: Comprender el entorno de datos e identificar los datos importantes en un entorno híbrido.
   - Prevenir la pérdida de datos: Detectar comportamientos de riesgo y evitar la divulgación accidental de información confidencial.
   - Proteger los datos: Aplicar medidas de protección flexibles, como cifrado, restricciones de acceso y señalización visual.
   - Controlar los datos: Conservar, suprimir y almacenar automáticamente datos y registros de forma conforme a la normativa.

   Para más información sobre las funcionalidades que ofrece Microsoft Purview Information Protection, se debe consultar la guía **Proteja sus datos confidenciales con Microsoft Purview** [REF1].

2 OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Purview Information Protection.

5. El servicio Microsoft Purview Information Protection ha sido cualificado en el catálogo CPSTIC para categoría ENS ALTA en la familia “Otras herramientas”.

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

6. Al tratarse de un servicio en la nube, se dará 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.
7. El envío de los datos se relacionará 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.

4.2 ENTORNO DE INSTALACIÓN SEGURO

9. 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

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

4.4 CONSIDERACIONES PREVIAS

13. 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

14. El producto está compuesto de los siguientes dos 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).

5 FASE DE INSTALACIÓN

15. 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 Information Protection.

5.1 ALTA DEL SERVICIO EN LA NUBE

16. Al tratarse de un servicio en la nube, se requiere el alta en el portal de **Microsoft 365** [REF4] adquiriendo una suscripción y dar el alta para que el usuario pueda hacer uso del producto.
17. 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 INFORMATION PROTECTION

18. El proveedor proporciona documentación acerca de la activación y uso de licencia para poder hacer uso de la funcionalidad del producto, consultar la última sección “Requisitos de licencias” de la guía **Proteja sus datos confidenciales con Microsoft Purview** [REF1]**.**

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

19. 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** [REF4]**.**
20. 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.
21. 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

22. 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.
23. 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.
24. 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.
25. Más información en la guía **CCN-STIC-884A Guía de configuración segura para Azure** [REF5].

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

26. 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.
27. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

28. 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.
29. El producto utiliza Microsoft Entra ID para que los usuarios se autentiquen antes de cualquier interacción del producto accediendo a través de la interfaz web y cloud shell.

30. 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 predetermiandos de Azure o de Purview).

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

    - Global administrator (predeterminado de Azure): Puede acceder a todas las funcionalidades adminsitrativas 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 solo de 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.

32. El producto gestiona perfiles a través del portal Microsoft Defender, Microsoft Purview y los portales clásicos de cumplimiento y gobierno Microsoft. El producto define 5 perfiles diferentes:

    - Protección de la información: Control total sobre todas las funciones de protección de la información, incluidas etiquetas de sensibilidad y sus políticas, DLP, todos los tipos de clasificadores, exploradores de actividad y contenido, y todos los informes relacionados.
    - Administradores de protección de la información: Crear, editar y eliminar políticas de DLP, etiquetas de sensibilidad y sus políticas, y todos los tipos de clasificadores. Administrar la configuración de la DLP de endpoints y el modo de simulación para las políticas de etiquetado automático.
    - Analistas de protección de la información: Acceder y gestionar las alertas de DLP y el explorador de actividades. Acceso de solo visualización a las políticas de DLP, las etiquetas de sensibilidad y sus políticas, y todos los tipos de clasificadores.
    - Investigadores de protección: Acceso y administración de alertas de DLP, explorador de actividades y explorador de contenido. Acceso de solo visualización a las políticas de DLP, las etiquetas de sensibilidad y sus políticas, y todos los tipos de clasificadores.
    - Lectores de protección de la información: Acceso de solo visualización a informes para políticas de DLP y etiquetas de sensibilidad y sus políticas.

33. 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]**.**

34. 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]**.**

35. 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]**.**

36. 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.

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** [REF10].

38. 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

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

6.5 GESTIÓN DE CERTIFICADOS

40. 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.
41. 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

42. 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

43. 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

44. 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.
45. Todas las actualizaciones están firmadas digitalmente y aplicadas automáticamente por el CSP.

6.9 AUTO-CHEQUEOS

46. 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

47. 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

48. El producto usa Microsoft Entra ID para autenticar a cualquier usuario antes de cualquier interacción con el producto. 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.

49. Por lo tanto, todas las actividades son registradas en el Audit Log de Microsoft 365.

50. 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: La fecha y hora cuando el evento ha ocurrido.
    - IP address: La dirección IP del dispositivo que se ha usado cuando se generó la actividad. La dirección IP aparecerá en formato IPv4 o IPv6.
    - User: El usuario (o cuenta del servicio) que realizó la actividad que desencadenó el evento.
    - Activity: La actividad realizada por el usuario. El valor corresponde con la actividad que se ha seleccionado en el menú desplegable de Activities. Para un evento del registro auditable de un administrador Exchange, el valor de la columna es una “Exchange cmdlet”.
    - Item: El objeto que ha sido creado o modificado como resultado de la actividad correspondiente. Por ejemplo, el archivo que ha sido visualizado o modificado, o la cuenta que ha sido actualizada. No todas las actividades tienen un valor en esta columna.
    - Detail: Información adicional sobre una actividad. De nuevo, no todas las actividades tienen un valor.

51. 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.

52. 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 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.

53. 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.

54. Eliminación de eventos:

- Los eventos no se pueden borrar. Los eventos se sobrescriben cuando la política de retención de datos es aplicada (180 días).

55. Acciones correctoras (utilizando la funcionalidad DLP). Se pueden crear reglas donde las acciones de remediación son definidas para cuando una condición se cumple:

- Extensión de archivo: cuando se detecta cierta extensión de archivo (.doc, .pdf).
- Tipo de archivo es: cuando se detecta cierto tipo de archivo (Excel, PowerPoint, Zip).
- Patrones de coincidencia de nombre de documento: documentos cuyo nombre de archivo coincide con se detectan patrones específicos.

56. Para más información sobre el registro de actividad de en Purview Information Protection se deben consultar las guías **MicrosoftPurviewInformationProtection** [REF11][REF10][REF9] y **Referencia del registro de auditoría de Azure Information Protection** [REF12][REF10]**.**

6.11.2 ALMACENAMIENTO LOCAL

57. 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

58. La opción de enviar eventos de registros a un servidor no está disponible.

6.12 BACKUP

59. 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

60. 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.

61. 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.

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

63. 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 ETIQUETAS DE CONFIDENCIALIDAD

64. Las etiquetas de confidencialidad de Microsoft Purview Information Protection permiten clasificar y proteger los datos de una organización, a la vez que se asegura de que la productividad de los usuarios y su capacidad de colaboración no se vean obstaculizadas.

65. Para más información sobre las etiquetas de confidencialidad, se debe consultar la guía **Información sobre las etiquetas de confidencialidad** [REF13][REF11][REF10]**.**

66. Para más información sobre cómo usar las etiquetas de confidencialidad y los entornos en los que usarlas, se debe consultar la guía **Empiece a usar las etiquetas de confidencialidad** [REF14][REF12][REF11]**.**

7.2 ACTIVIDADES DE ETIQUETADO EN EL EXPLORADOR DE ACTIVIDADES

67. El explorador de actividades permite supervisar lo que se está haciendo con el contenido etiquetado.

68. El explorador de actividades le permite supervisar lo que se hace con el contenido etiquetado. El Explorador de actividades proporciona una vista histórica de las actividades en el contenido etiquetado. La información de actividad se recopila de los registros de auditoría unificados de Microsoft 365, se transforma y, a continuación, se hace disponible en la interfaz de usuario del explorador de actividad.

69. Para más información sobre las actividades de etiquetado dentro del explorador de actividades, se debe consultar al guía **Actividades de etiquetado que están disponibles en el Explorador de actividades** [REF15][REF13][REF12]**.**

7.3 NOTIFICACIÓN DE INCIDENTES

70. Microsoft Purview Information Protection forma parte de la suite Microsoft Purview y utiliza la funcionalidad DLP para notificar los incidentes.

71. Para más información sobre la funcionalidad de DLP para notificar incidentes se debe consultar la guía **Introducción a las alertas de prevención de pérdida de datos** [REF16][REF13].

8 REFERENCIAS

[REF1] Proteja sus datos confidenciales con Microsoft Purview
https://learn.microsoft.com/es-es/purview/information-protection

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

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

[REF4] Microsoft 365
https://www.office.com/

[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] MicrosoftPurviewInformationProtection
https://learn.microsoft.com/en-us/azure/azure-monitor/reference/tables/microsoftpurviewinformationprotection

[REF12] Referencia del registro de auditoría de Azure Information Protection (versión preliminar pública)
https://learn.microsoft.com/es-es/azure/information-protection/audit-logs

[REF13] Información sobre las etiquetas de confidencialidad
https://learn.microsoft.com/es-es/purview/sensitivity-labels

[REF14] Empiece a usar las etiquetas de confidencialidad
https://learn.microsoft.com/es-es/purview/get-started-with-sensitivity-labels

[REF15] Actividades de etiquetado que están disponibles en el Explorador de actividades
https://learn.microsoft.com/es-es/purview/data-classification-activity-explorer-available-events

[REF16] Introducción a las alertas de prevención de pérdida de datos
https://learn.microsoft.com/es-es/purview/dlp-alerts-get-started

9 ABREVIATURAS

CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación.
CSP	Cloud Service Provider
DLP	Data Loss Prevention
ENS	Esquema Nacional de Seguridad.
HTTP	Hyper Text Transfer Protocol.
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol
MFA	Autenticación Multifactor.
NTP	Network Time Protocol.
RBAC	Control de Acceso Basado en Roles.
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado)
TLS	Transport Layer Security.

PUBLICACIONES DE DEFENSA

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