# Guía de Seguridad de las TIC
# CCN-STIC 1238

# Procedimiento de Empleo Seguro
# Microsoft Purview DLP


Septiembre 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: 083-26-125-X

Fecha de Edición: Septiembre 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 10:00:41 +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**

# ÍNDICE

# 1 INTRODUCCIÓN

1. Microsoft Purview Data Loss Prevention es una solución de seguridad que identifica y ayuda a evitar el uso compartido, la transferencia o el uso inseguro o inapropiado de datos confidenciales. Supervisa y protege la información confidencial en los sistemas locales, las ubicaciones basadas en la nube y los dispositivos de punto final.
2. También cumple con regulaciones como la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) y el Reglamento General de Protección de Datos (GDPR).
3. Forma parte de la solución de seguridad de datos Microsoft Purview, además de las soluciones de Data Governance y Compliance.
4. El producto ofrece una variedad de servicios, entre los que se incluyen:
   - Descubrimiento y clasificación automática de información sensible.
   - Monitorización y clasificación continua de información sensible.
   - Integración con otros servicios de Microsoft, como Microsoft Entra Protection y Microsoft Cloud App Security.
   - Política de creación customizable que sirve para forzar las medidas de protección de la información.
   - Alertas en tiempo real e informes sobre posibles brechas de información.
5. El producto usa DLP (Data Loss Prevention) policies para monitorizar las actividades que el usuario realiza sobre: elementos sensibles en reposo, elementos sensibles en tránsito y elementos sensible en uso, actuando de manera proactiva.
6. Detecta los elementos sensibles mediante un análisis profundo del contenido:
   - Para las coincidencias de datos primarios con palabras clave.
   - Mediante la evaluación de expresiones regulares.
   - Por validación de funciones internas.
   - Por coincidencias de datos secundarios que están en proximidad con la coincidencia de datos primarios.
7. Utiliza algoritmos de aprendizaje automático y otros métodos para detectar contenido que coincida con sus políticas de DLP.
8. Para obtener más información puede consultar la guía Obtenga más información acerca de la prevención contra la pérdida de datos [REF1].

## 2 OBJETO Y ALCANCE

9. El objetivo del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Purview DLP.

10. Este servicio se sitúa dentro de la familia DLP (Sistemas de prevención de fuga de datos) 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

11. 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.
12. El envío de los datos se relacionará mediante correo electrónico firmado digitalmente y a la cuenta que se ha proporcionado para el alta.
13. 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

14. 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

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. Se requiere la obtención de una licencia de Microsoft 365 E5.
16. Sólo los usuarios autorizados y con la licencia activa podrán acceder al producto. Más información en Microsoft 365 Licenses [REF3].

## 4.4 CONSIDERACIONES PREVIAS

17. 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

18. El producto forma parte de la solución Data Security del servicio Microsoft Purview, que se suma a las soluciones de Data Governance y Compliance Solutions.
19. 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 Microsoft Purview.
- API: Una señal compartida con otras soluciones de seguridad de Microsoft y otros sistemas externos.
- Location: Donde las políticas van a ser aplicadas (en la nube o punto de conexión).

# 5 FASE DE INSTALACIÓN

20. 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 Data Loss Prevention.

## 5.1 ALTA DEL SERVICIO EN LA NUBE

21. 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.

22. 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 MICRSOFT PURVIEW DATA LOSS PREVENTION

23. El proveedor proporciona documentación acerca de la activación para poder hacer uso de la funcionalidad del producto, consultar la sección “Antes de empezar” de la guía **Introducción a la prevención de pérdida de datos del punto de conexión** [REF4]**.**

# 6 FASE DE CONFIGURACIÓN

## 6.1 MODO DE OPERACIÓN SEGURO

24. 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]**.**
25. 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.
26. 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

27. 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.
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
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 [REF6].

## 6.3 ADMINISTRACIÓN DEL PRODUCTO

### 6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. 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.
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 365, la administración del producto se realiza de forma remota.
34. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure integrado y Purview. 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).

35. 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 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.

36. El producto utiliza la infraestructura de Microsoft 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)<br>Minúsculas (a - z)<br>Números (0 - 9)<br>Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } \| \ : ' , . ? / ` ~ " ( ) ; < ><br>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:<br>- Mayúsculas |

| | |
|---|---|
| | - Minúsculas<br>- Números<br>- 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**

37. 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]**.**

38. Para ampliar la información sobre los permisos en el portal, se puede consultar la información proporcionada por el fabricante en la guía **Permissions in the Microsoft Purview compliance portal** [REF8]**.**

## 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 AUDITORIA

### 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. 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 Micrososft 365 para auditar todos los eventos de generados por el producto.
49. Por lo tanto, todas las actividades monitorizadas del DLP son registradas en el Audit Log de Microsoft 365.
50. Dentro de la página de búsqueda de Audit log se puede visualizar el audit log deseado. La información que se muestra para cada audit log es la siguiente:

- 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 de la actividad. 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 y clasifica los registros de auditorías por las actividades que se auditan dentro de Microsoft 365. Se pueden buscar estos eventos realizando una búsqueda en los registros de auditoria en el portal de seguridad y conformidad, y seleccionando alguna de las siguientes categorías:

- Inicio y final de las funciones de auditoría. Estas funciones no aplican al producto, ya que, al ser un servicio alojado en la nube, esta funcionalidad esta siempre activada, por lo que ni el inicio ni el final pueden ser administrados.
- Cambios en las credenciales del usuario (estos eventos vienen de la integración con Entra ID).
- Cambios en la configuración del sistema. Añadir o remover puntos de conexión o cambios en las calves, genera eventos relacionados con los cambios de configuración con el objetivo de ser evaluados.
- Proceso de Login de personal autorizado (estos eventos vienen de la integración con Entra ID). Debido a la arquitectura y el modo de operación de la infraestructura de Azure, la plataforma usa capacidades de sesión y no hay eventos en el Logout. Los Logins (sign-ins) se almacenan con los siguientes estados:
    - Success: El Login ha sido exitoso.
    - Failure: Ha ocurrido un error a la hora de validar las credenciales debido al uso de un nombre de usuario o contraseña incorrectos.
    - Interrupted: La contraseña del usuario ha expirado y por lo tanto el inicio de sesión o la propia sesión han sido concluidas. Se le pregunta al usuario si quiere seguir identificado dentro del buscador para que futuras búsquedas sean más sencillas.

53. Los siguientes cambios en las directivas generarán eventos:

- Crear una directiva DLP: Cuando se crea una nueva directiva DLP.
- Actualizar una directiva DLP: Cuando una directiva DLP existente es actualizada.
- Eliminar una directiva DLP: Cuando se elimina una directiva DLP.

54. Borrado de eventos:

55. Los eventos no pueden ser eliminados. Los eventos se sobrescriben cuando los días establecidos en la política de retención son alcanzados (180 días).

56. Acciones de remediación. El producto puede crear reglas en las que las acciones de corrección se definen cuando se cumple una condición.

57. La administración de los registros solo la pueden realizar usuarios con un perfil administrativo (e.g. auditor/system roles administrador).

58. Para más información sobre el registro de actividad de prevención de pérdida de datos se debe consultar la guía **Registro de actividad de prevención de pérdida de datos** [REF9]**.**

### 6.11.2 ALMACENAMIENTO LOCAL

59. 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

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

## 6.12 BACKUP

61. 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

62. 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.

63. 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.

64. Microsoft Purview Data Loss Prevention ofrece un conjunto de funcionalidades específicas que deben implementarse conforme a los estándares de seguridad y las mejores prácticas recomendadas por el proveedor.

65. 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 POLÍTICAS DE SEGURIDAD PARA LA REGULACIÓN DE ACCIONES EN DLP

66. DLP supervisa las acciones que se están llevando a cabo sobre los elementos que usted ha determinado como sensibles y para ayudar a prevenir el intercambio involuntario de esos elementos.

67. DLP está habilitado para auditar y gestionar las actividades que los usuarios realizan en los elementos sensibles que se almacenan físicamente en dispositivos Windows 10, Windows 11 o macOS.

68. Para más información sobre políticas de seguridad y monitorización activa, se debe consultar la guía Obtener información sobre la **Prevención de pérdida de datos en punto de conexión** [REF10].

69. Si la opción “Auditar siempre la actividad de archivos para dispositivos” está activada, las actividades en cualquier archivo Word, PowerPoint, Excel, PDF y .csv se auditan siempre, aunque el dispositivo no esté sujeto a ninguna política.

70. Para más información sobre acciones realizadas en archivos Office, PDF y CSV que se auditan automáticamente, se debe consultar la guía **Configuración de la prevención de pérdida de datos de punto de conexión** [REF11]**.**

## 7.2 DISEÑAR UNA DIRECTIVA DE DLP

71. Diseñar una directiva consiste en definir claramente las necesidades empresariales, documentarlas en una instrucción de intención de directiva y, a continuación, asignarlas

a la configuración de la directiva, con el objetivo de proteger la información sensible de una organización contra accesos no autorizados, fugas o pérdidas accidentales.

72. Para más información sobre cómo diseñar una directiva de DLP se debe seguir al guía **Diseño de una directiva de prevención de pérdida de datos** [REF11].

## 7.3 ALERTAS DE DLP

73. Las directivas de Prevención de pérdida de datos de Microsoft Purview (DLP) se pueden configurar para generar alertas cuando se cumplen las condiciones de una directiva.

74. Para más información sobre la configuración de alertas DLP se debe consultar la guía **Introducción a las alertas de prevención de pérdida de datos** [REF13].

## 7.4 ANÁLISIS DE DLP

75. El análisis de prevención de pérdida de datos (DLP) de Microsoft Purview ayuda a los clientes a comprender los principales riesgos de protección de datos, puntos ciegos y oportunidades de mejora de directivas y posturas en su organización.

76. Puede ayudar a investigar estos riesgos mediante características inteligentes de Purview y mitigarlos en unos sencillos pasos.

77. Para más información sobre los análisis de detección de riesgos DLP se debe consultar la guía **Introducción al análisis de prevención de pérdida de datos** [REF14]**.**

# 8 REFERENCIAS


[REF1] Microsoft Purview Data Loss Prevention
https://learn.microsoft.com/es-es/purview/dlp-learn-about-dlp

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

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

[REF4] Introducción a la prevención de pérdida de datos del punto de conexión
https://learn.microsoft.com/es-es/purview/endpoint-dlp-getting-started#before-you-begin

[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] Registro de actividad de prevención de pérdida de datos
https://learn.microsoft.com/es-es/power-platform/admin/dlp-activity-logging

[REF10] Obtener información sobre la Prevención de pérdida de datos en punto de conexión
https://learn.microsoft.com/es-es/purview/endpoint-dlp-learn-about

[REF11] Configuración de la prevención de pérdida de datos de punto de conexión
https://learn.microsoft.com/es-es/purview/dlp-configure-endpoint-settings?tabs=purview

[REF12] Diseño de una directiva de prevención de pérdida de datos
https://learn.microsoft.com/es-es/purview/dlp-policy-design

[REF13] Introducción a las alertas de prevención de pérdida de datos
https://learn.microsoft.com/es-es/purview/dlp-alerts-get-started

[REF14] Introducción al análisis de prevención de pérdida de datos
https://learn.microsoft.com/es-es/purview/dlp-analytics-get-started?tabs=purview

# 9 ABREVIATURAS

| | |
|---|---|
| AD | Active Directory. |
| 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. |
| DLP | Prevención de perdida de datos. |
| ENS | Esquema Nacional de Seguridad. |
| GDPR | General Data Protection Regulation. |
| HIPAA | Health Insurance Portability and Accountability Act. |
| HTTP | Hyper Text Transfer Protocol. |
| MFA | Autenticación Multifactor. |
| NTP | Network Time Protocol. |
| RBAC | Control de Acceso Basado en Roles. |
| 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