

© Copyright Microsoft Corporation. Todos los derechos reservados.

**PARA USO SOLAMENTE COMO PARTE DEL PROGRAMA MICROSOFT VIRTUAL TRAINING DAYS. ESTOS MATERIALES NO ESTÁN
AUTORIZADOS PARA SU DISTRIBUCIÓN, REPRODUCCIÓN O CUALQUIER OTRO USO POR PARTE DE PERSONAS AJENAS A MICROSOFT.**



Microsoft Security Virtual Training Day: Security, Compliance, and Identity Fundamentals



**Describa los conceptos de seguridad,
cumplimiento e identidad**

Objetivos de aprendizaje

- Describir los conceptos de seguridad y cumplimiento
- Describir los conceptos de identidad

Objetivo de aprendizaje: Describir los conceptos de seguridad y cumplimiento

El modelo de responsabilidad compartida

Identifique qué tareas de seguridad realiza el proveedor de nube y qué tareas de seguridad le corresponden a usted, el cliente.

Las responsabilidades varían en función del lugar donde se hospeda la carga de trabajo:

- Software como servicio (SaaS)
- Plataforma como servicio (PaaS)
- Infraestructura como servicio (IaaS)
- Centro de datos local (entorno local)

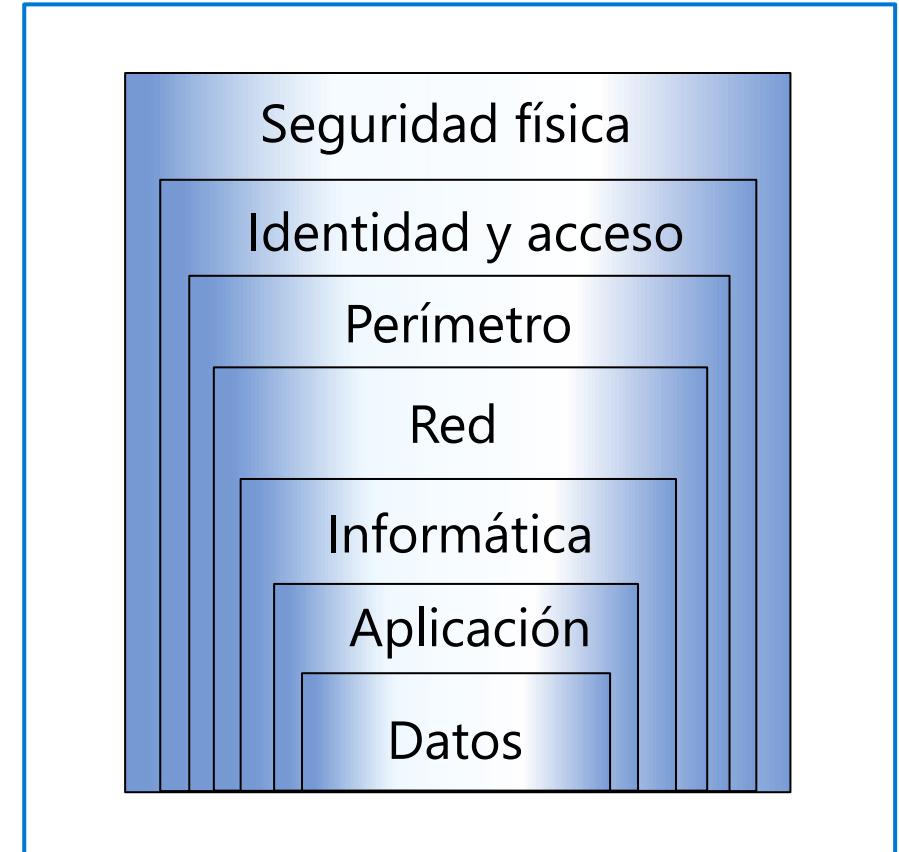
Responsabilidad	SaaS	PaaS	IaaS	Entorno local	
Información y datos	■	■	■	■	LA RESPONSABILIDAD SIEMPRE LE CORRESPONDE AL CLIENTE
Dispositivos (móviles y equipos)	■	■	■	■	LA RESPONSABILIDAD SIEMPRE LE CORRESPONDE AL CLIENTE
Cuentas e identidades		■	■	■	LA RESPONSABILIDAD VARÍA SEGÚN EL TIPO DE SERVICIO
Infraestructura de directorios e identidades		■	■	■	LA RESPONSABILIDAD VARÍA SEGÚN EL TIPO DE SERVICIO
Aplicaciones			■	■	LA RESPONSABILIDAD VARÍA SEGÚN EL TIPO DE SERVICIO
Controles de red			■	■	LA RESPONSABILIDAD VARÍA SEGÚN EL TIPO DE SERVICIO
Sistema operativo				■	LA RESPONSABILIDAD SE TRANSFERIRÁ A LOS PROVEEDORES DE NUBE
Hosts físicos				■	LA RESPONSABILIDAD SE TRANSFERIRÁ A LOS PROVEEDORES DE NUBE
Red física				■	LA RESPONSABILIDAD SE TRANSFERIRÁ A LOS PROVEEDORES DE NUBE
Centro de datos físico				■	LA RESPONSABILIDAD SE TRANSFERIRÁ A LOS PROVEEDORES DE NUBE

■ Microsoft ■ Cliente

Defensa en profundidad

La defensa en profundidad utiliza un enfoque en capas para la seguridad.

- Seguridad física, como la limitación del acceso a un centro de datos solo al personal autorizado.
- Seguridad de identidad y acceso, que controla el acceso a la infraestructura y el control de cambios.
- Seguridad perimetral, que incluye la protección distribuida de denegación de servicio (DDoS) para filtrar los ataques a gran escala.
- La seguridad de red puede limitar la comunicación entre recursos mediante la segmentación y los controles de acceso.
- Seguridad de nivel de cómputo, como proteger el acceso a máquinas virtuales.
- La seguridad de la capa de aplicación protege las aplicaciones contra las vulnerabilidades de seguridad.
- Los controles de seguridad de la capa de datos incluyen el cifrado para proteger los datos.



Confidencialidad, integridad, disponibilidad (CIA)

Confidencialidad

Se refiere a la necesidad de mantener confidenciales los datos de este tipo, como la información del cliente, las contraseñas o los datos financieros.

Integridad

Se refiere a mantener correctos los datos o mensajes.

Disponibilidad

Se refiere a poner los datos a disposición de quienes los necesiten.



El modelo de Confianza cero

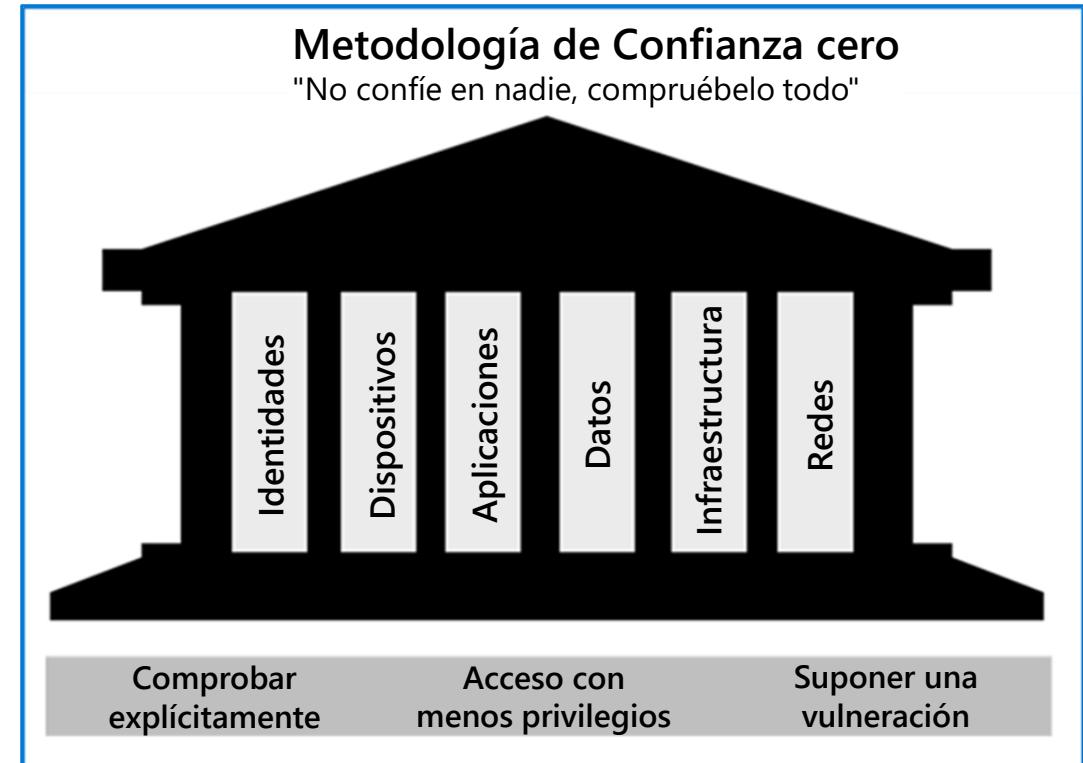
El modelo de Confianza cero opera bajo el principio de "No confíe en nadie, compruébelo todo".

Principios rectores de la Confianza Cero

- Comprobar explícitamente
- Acceso con menos privilegios
- Suponer la vulneración

Seis pilares fundamentales

- Las identidades pueden ser usuarios, servicios o dispositivos.
- Los dispositivos crean un gran superficie de ataque a medida que fluyen los datos.
- Las aplicaciones son la forma en que se consumen los datos.
- Los datos se deben clasificar, etiquetar y cifrar.
- La infraestructura representa un vector de amenazas.
- Las redes deben segmentarse.



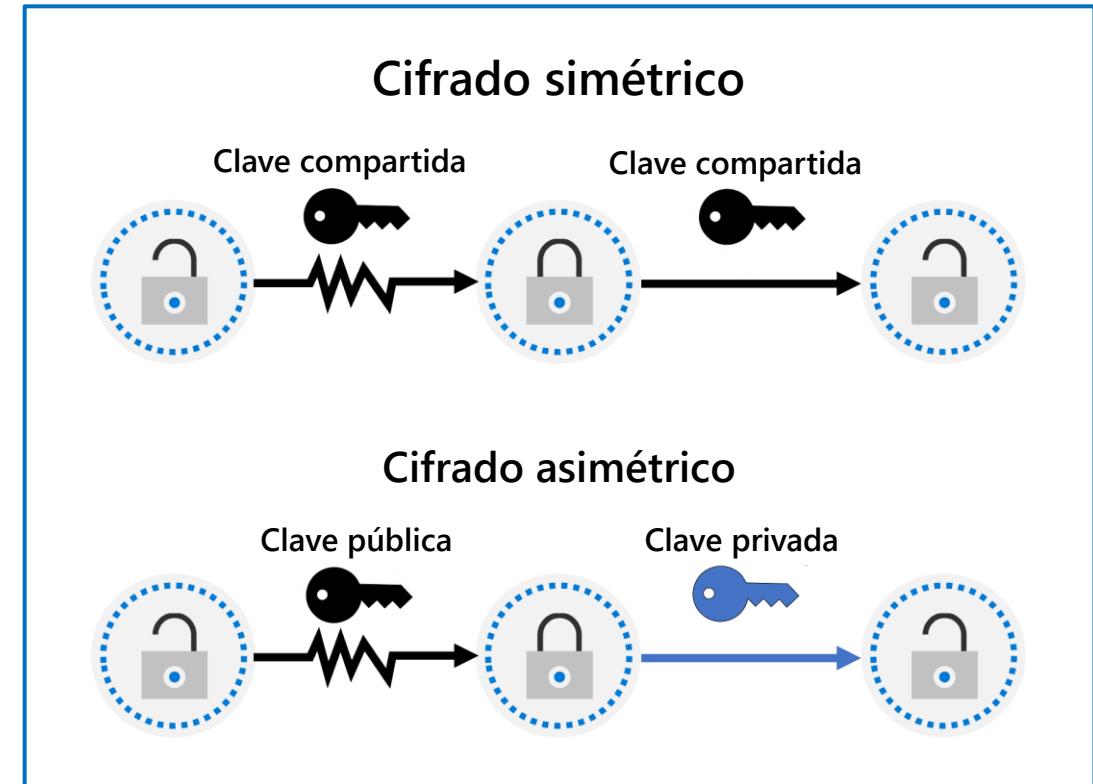
Cifrado

El cifrado es el proceso de hacer que los datos sean ilegibles e inutilizables para los espectadores no autorizados.

- Cifrado de datos en reposo
- Cifrado de datos en tránsito
- Cifrado de datos en uso

Dos tipos de cifrado de nivel superior:

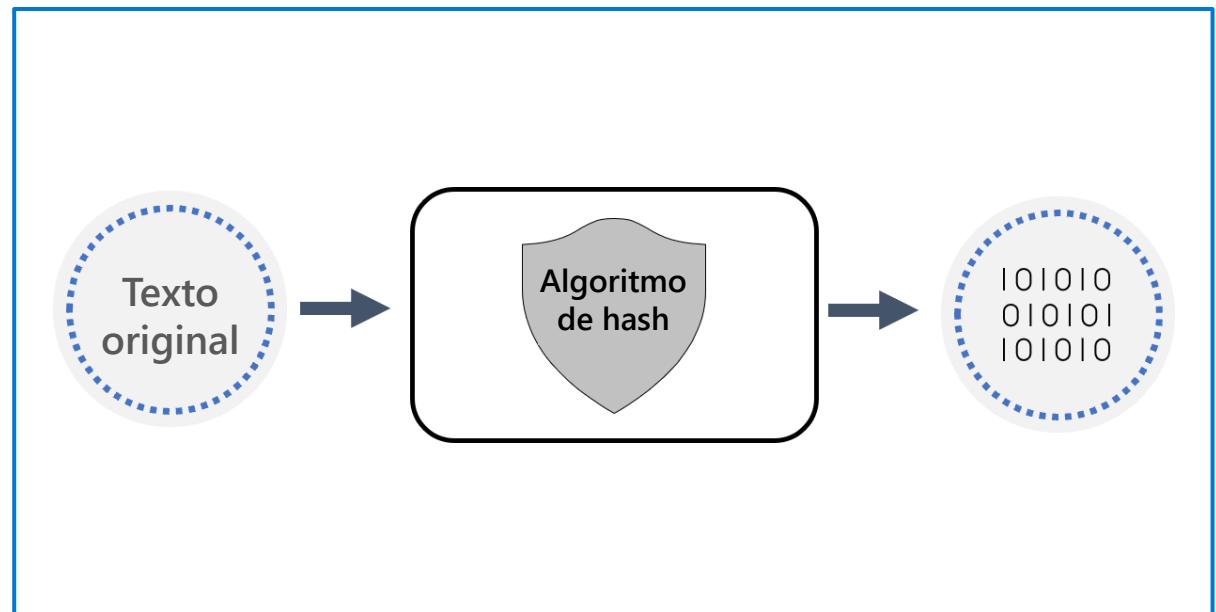
- Simétrico—utiliza la misma clave para cifrar y descifrar los datos.
- Asimétrico—utiliza una clave pública y un par de claves privadas.



Hash

Hash utiliza un algoritmo para convertir texto original en un valor de longitud fija único llamado valor hash.

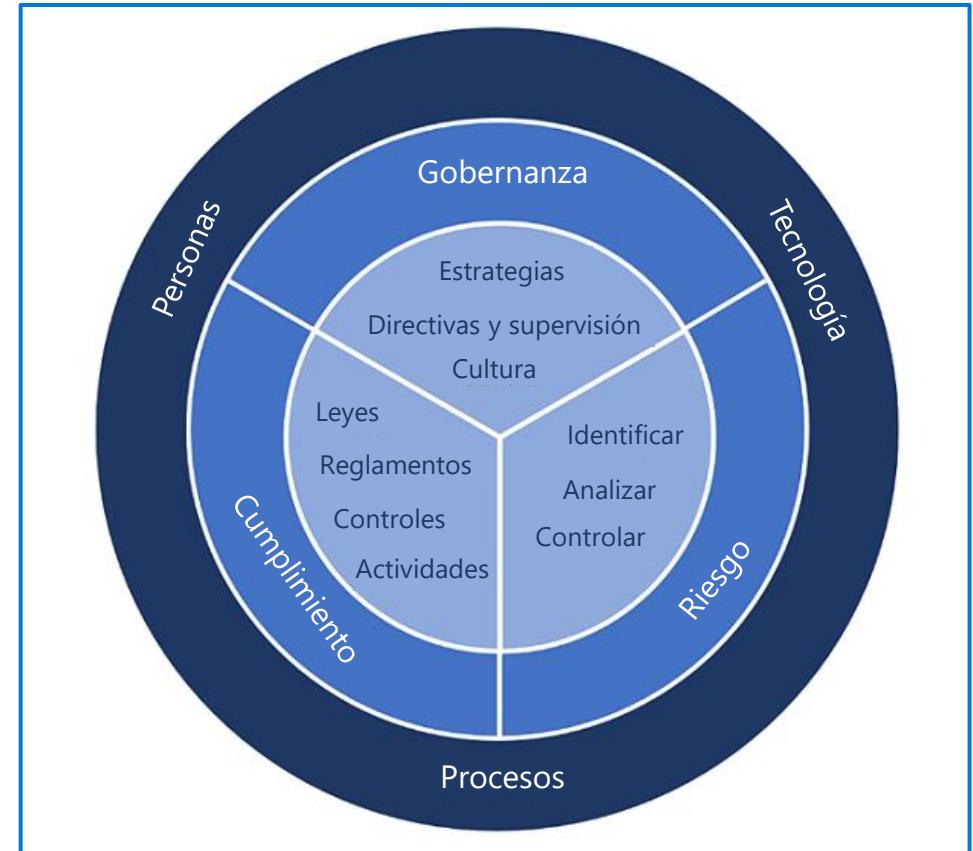
- Es determinista, por lo que la misma entrada produce la misma salida.
- Un identificador único de sus datos asociados.
- Es diferente del cifrado ya que el valor hash no se descifra posteriormente en el original.
- Se utiliza para almacenar contraseñas. La contraseña está "salada" para mitigar el riesgo de ataque de diccionario de fuerza bruta.



Conceptos de Gobernanza, cumplimiento y riesgo (GRG)

GRG ayuda a las organizaciones a reducir el riesgo y mejorar la eficacia del cumplimiento.

- **Gobernanza:** Las reglas, prácticas y procesos que una organización utiliza para dirigir y controlar sus actividades.
- **Gestión de riesgos:** El proceso de identificar, evaluar y responder a amenazas o eventos que pueden afectar los objetivos de la empresa o del cliente.
- **Cumplimiento:** Las leyes nacionales/regionales, estatales o federales o incluso las regulaciones multinacionales que una organización debe seguir.



Objetivo de aprendizaje: Describir los conceptos de identidad

Autenticación y autorización

Autenticación (AuthN)

La autenticación es el proceso de demostrar que una persona es quien dice ser. La autenticación **otorga acceso**.

Autorización (AuthZ)

La autorización determina el **nivel de acceso o los permisos** que una persona autenticada tiene a sus datos y recursos.



La identidad como el perímetro de seguridad principal

La identidad se ha convertido en el nuevo perímetro de seguridad que permite a las organizaciones proteger sus activos.

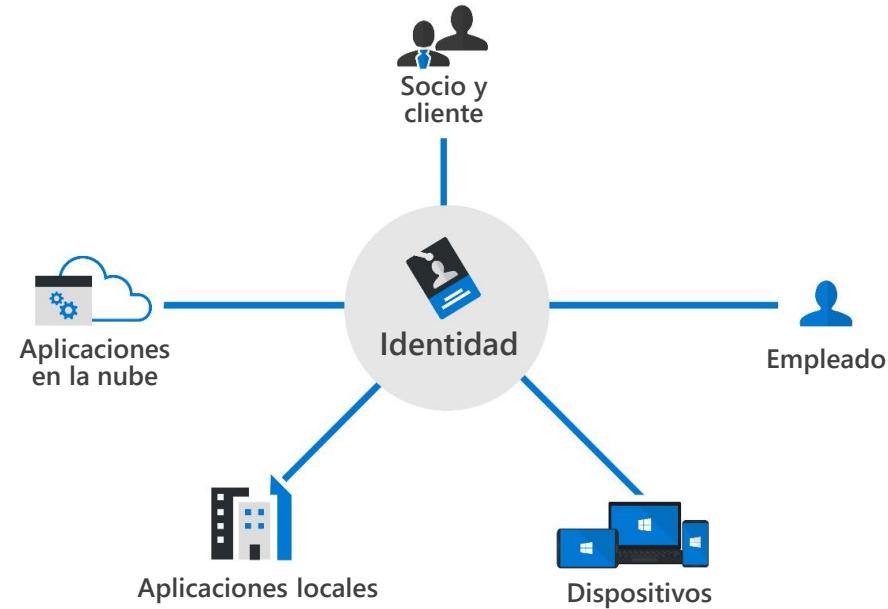
Una identidad es la forma en que se puede verificar y autenticar a alguien o algo y puede estar asociado con:

- Usuario
- Aplicación
- Dispositivo
- Otro

Cuatro pilares de una infraestructura de identidad:

- Administración
- Autenticación
- Autorización
- Auditoría

La identidad es el nuevo perímetro de seguridad



Autenticación moderna y el rol del proveedor de identidades

La autenticación moderna es un término genérico para los métodos de autenticación y autorización entre un cliente y un servidor.

-  En el centro de la autenticación moderna está el rol del **proveedor de identidades (IDP)**.
-  IDP ofrece servicios de autenticación, autorización y auditoría.
-  IDP permite a las organizaciones establecer directivas de autenticación y autorización, supervisar el comportamiento del usuario y mucho más.
-  Las capacidades fundamentales de un IdP y la "autenticación moderna" incluyen compatibilidad con métodos de autenticación seguros, inicio de sesión único, federación con otros IdP y más.
-  Microsoft Entra ID es un ejemplo de proveedor de identidades basado en la nube.

El concepto de servicios de directorio

Un servicio de directorio almacena los datos de directorio y los pone a disposición de usuarios, administradores, servicios y aplicaciones de la red.



Un directorio es una estructura jerárquica que almacena información sobre los objetos en la red.



Un servicio de directorio almacena los datos de directorio y los pone a disposición de usuarios, administradores, servicios y aplicaciones de la red.



El servicio más conocido de este tipo es Active Directory Domain Services (AD DS), un componente central en las organizaciones con infraestructura de TI local.



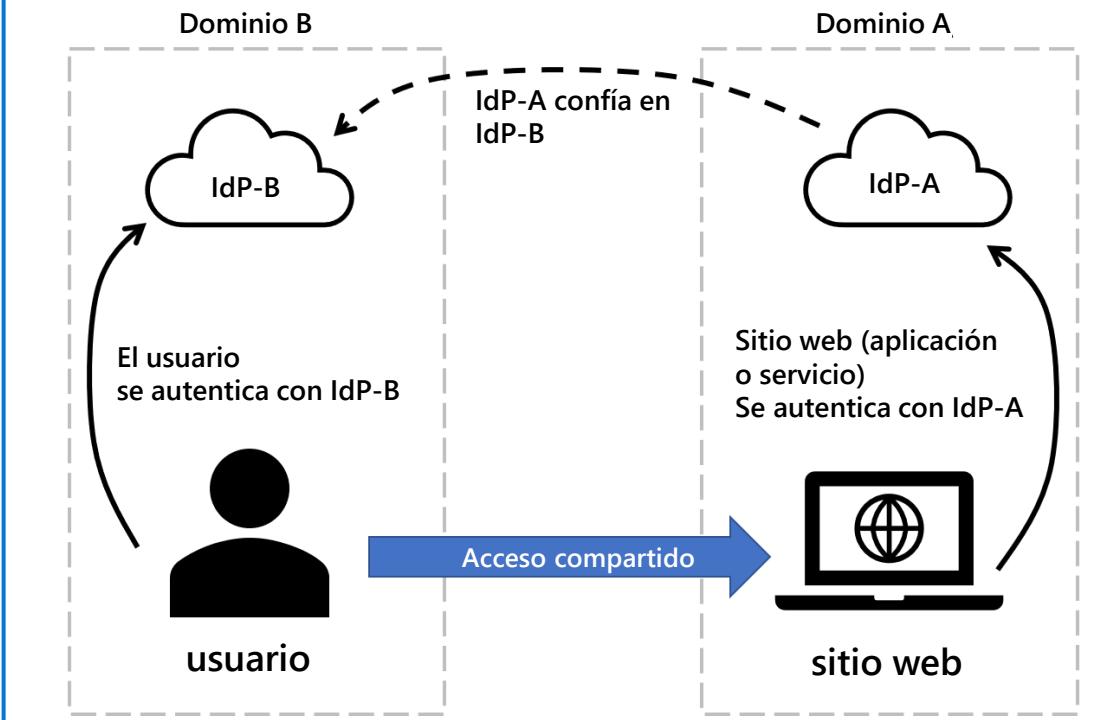
Microsoft Entra ID es la evolución de las soluciones de administración de identidades y acceso, que proporciona a las organizaciones una solución de identidad como servicio (IDaaS) para todas sus aplicaciones en la nube y locales.

El concepto de federación

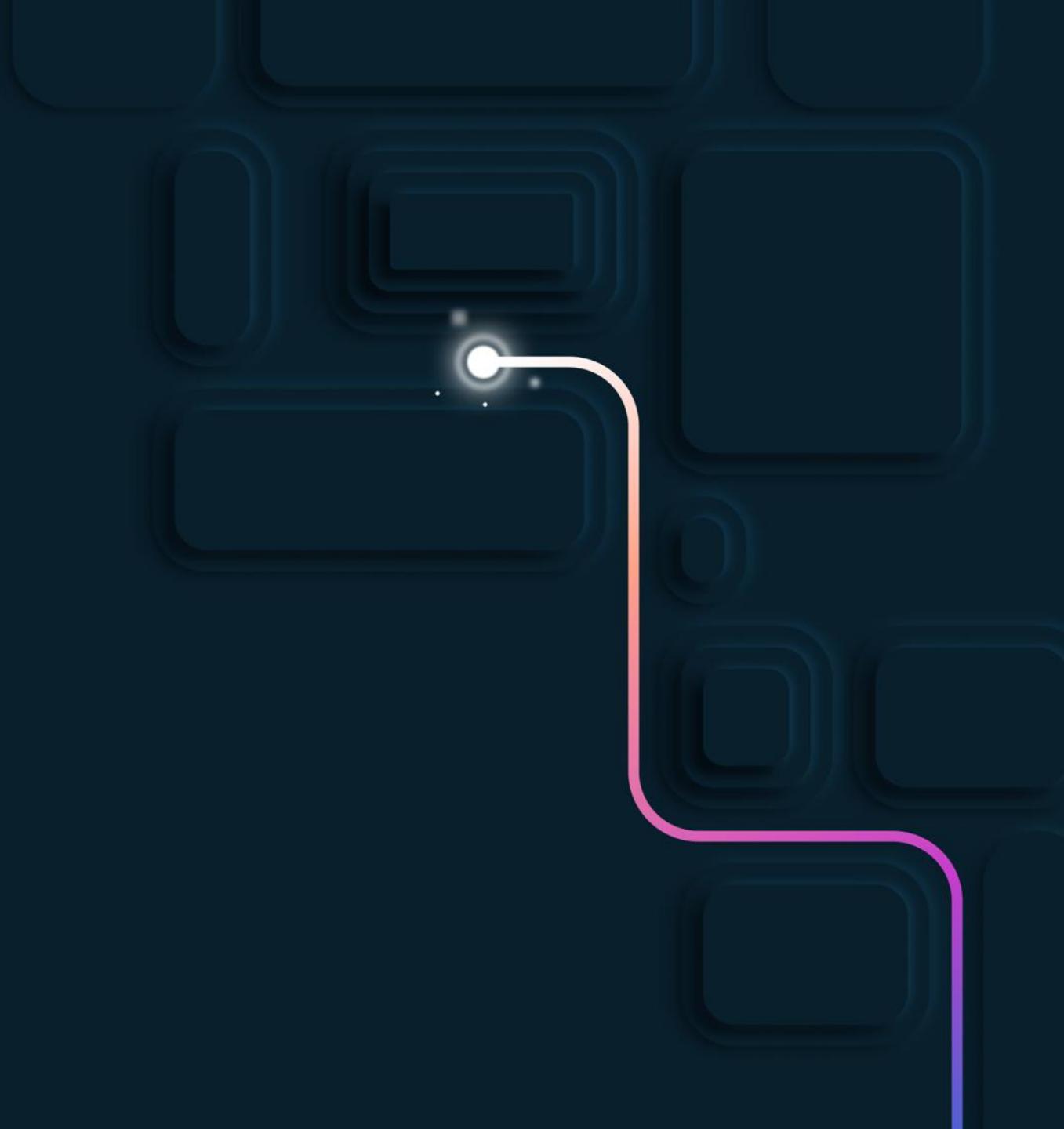
Una forma simplificada de pensar en la federación:

- El sitio web utiliza los servicios de autenticación del proveedor de identidades A (IdP-A).
- El usuario se autentica con el proveedor de identidades B (IdP-B).
- El IdP-A tiene una relación de confianza establecida con el IdP-B.
- Cuando el usuario inicia sesión en el sitio web, este puede confiar en sus credenciales y permitir el acceso.

Una forma simplificada de pensar en la federación



Describir las capacidades de Microsoft Entra



Objetivos de aprendizaje

- Describir los tipos de función e identidad de Microsoft Entra ID
- Describir las capacidades de autenticación de Microsoft Entra ID
- Describir las capacidades de administración de acceso de Microsoft Entra
- Describa las capacidades de gobernanza y protección de identidades de Microsoft Entra

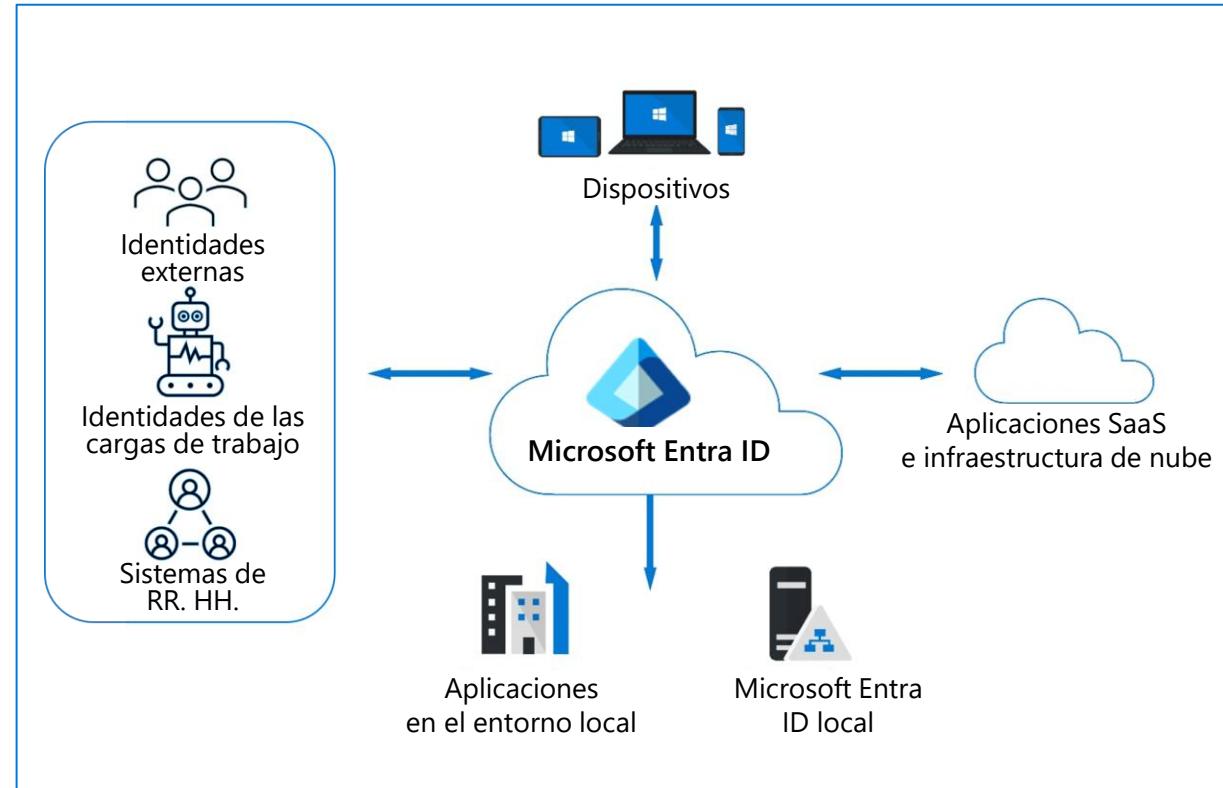


**Objetivo de aprendizaje: Describir los tipos
de función e identidad de Microsoft Entra ID**

Describir Microsoft Entra ID

Servicio de administración de identidades y acceso basado en la nube de Microsoft.

- Las organizaciones pueden permitir que sus empleados, invitados y otros puedan iniciar sesión y acceder a los recursos que necesitan.
- Proporciona un sistema de identidad único para sus aplicaciones multinube y locales.
- Protege las identidades y credenciales de los usuarios, y cumpla con los requisitos de gobernanza de acceso de una organización.
- Los suscriptores de los servicios de Azure, Microsoft 365 o Dynamics 365 tienen acceso automático a Microsoft Entra ID.
- Puntuación de seguridad de identidad.



Tipos de identidad

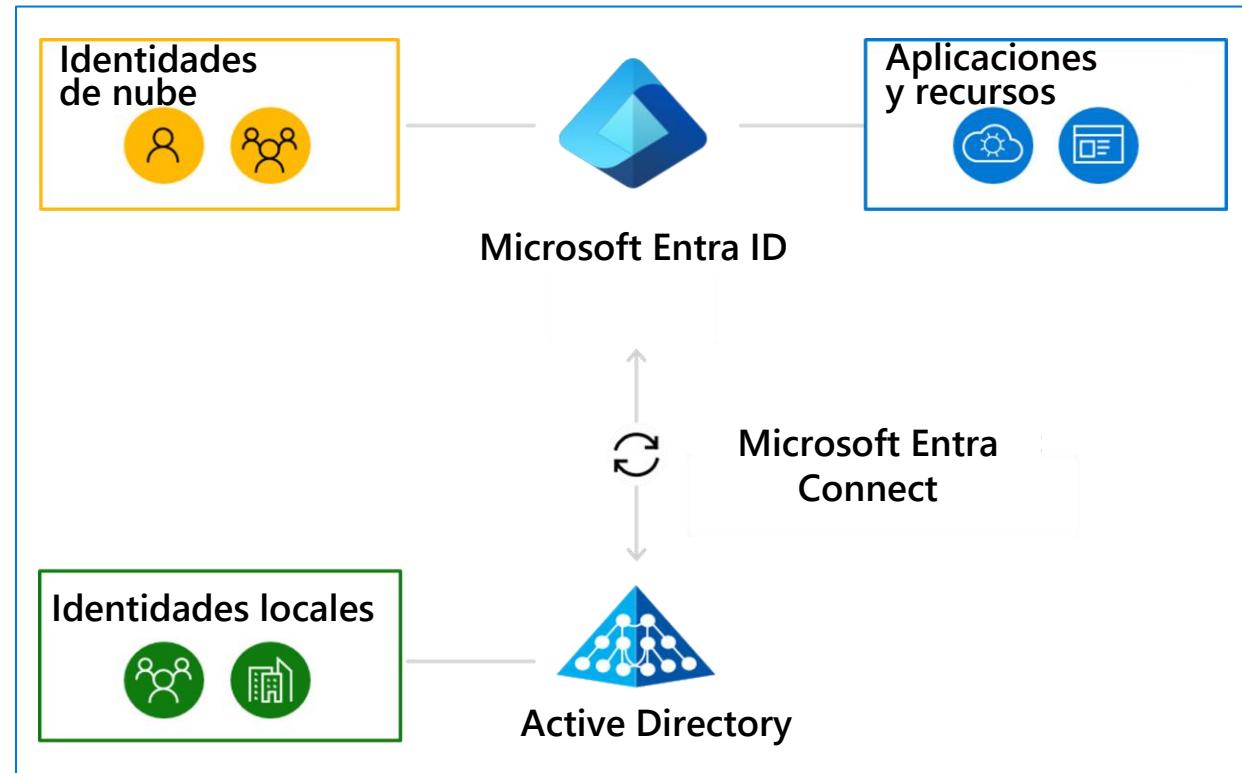
- **Identidades de los (usuarios) humanos**
 - Usuarios internos: Empleados
 - Usuarios externos: Invitados, socios, clientes, proveedores, consultores, etc.
- **Identidades de las cargas de trabajo:** Es una identidad asignada a una aplicación o un servicio.
 - Entidad de servicio: Es una identidad para una aplicación o servicio que usa Microsoft Entra ID para administrar las funciones de identidad y acceso; los desarrolladores de aplicaciones administran las credenciales.
 - Identidades administradas: Es una entidad de servicio administrada en Microsoft Entra ID que elimina la necesidad de que los desarrolladores de aplicaciones administren las credenciales.
- **Dispositivos**
 - Microsoft Entra ID registrado: Soporte para escenarios de traiga su propio dispositivo (BYOD) o dispositivo móvil.
 - Dispositivos unidos a Microsoft Entra ID: El dispositivo se unió a Microsoft Entra ID a través de una cuenta de organización (de propiedad de la organización).
 - Unión híbrida: Los dispositivos se unen a su Active Directory local y a Microsoft Entra ID, lo que requiere una cuenta de organización para iniciar sesión.



Identidad híbrida

Es una identidad de usuario común para la autenticación y autorización de recursos locales y en la nube.

- La identidad híbrida se logra de la siguiente manera:
 - Aprovisionamiento entre directorios: Un usuario que ya está en Active Directory se aprovisiona en Microsoft Entra ID.
 - Sincronización: Permite asegurarse de que la información de identidad de los usuarios y grupos locales coincida con la nube.
- Microsoft Entra Connect es un método de aprovisionamiento y sincronización para Microsoft Entra ID.



Demostración

- Configuración de usuario de Microsoft Entra ID



Objetivo de aprendizaje: Describir las capacidades de autenticación de Microsoft Entra ID

Métodos de autenticación de Microsoft Entra ID

Contraseñas (autenticación principal)

Autenticación basada en teléfono

- SMS (autenticación principal y secundaria)
- Voz (autenticación secundaria)

OATH: estándar sobre cómo se generan los códigos de contraseña de un solo uso (autenticación secundaria)

- Tokens de SW
- Tokens de HW

Sin contraseñas (autenticación principal y secundaria)

- Windows Hello
- Microsoft Authenticator
- FIDO2
- Certificados (autenticación principal)

Deficiente: Solo contraseña

123456

admin

quertyuiop

jP@ssword2024!

Bueno: Contraseña y...



SMS



Voz

Mejor: Contraseña y...



Notificaciones de inserción de Microsoft Authenticator



Tokens OTP de software



Tokens OTP de hardware



Mejor:
Sin contraseñas



Inicio de sesión en el teléfono de Microsoft Authenticator

El mejor: Resistente a phishing



Windows Hello para empresas



Clave de seguridad FIDO2



Autenticación basada en certificados (multifactor)



Llave de acceso en Microsoft Authenticator (vinculada a dispositivo)



Credencial de plataforma para macOS

Autenticación multifactor (MFA)

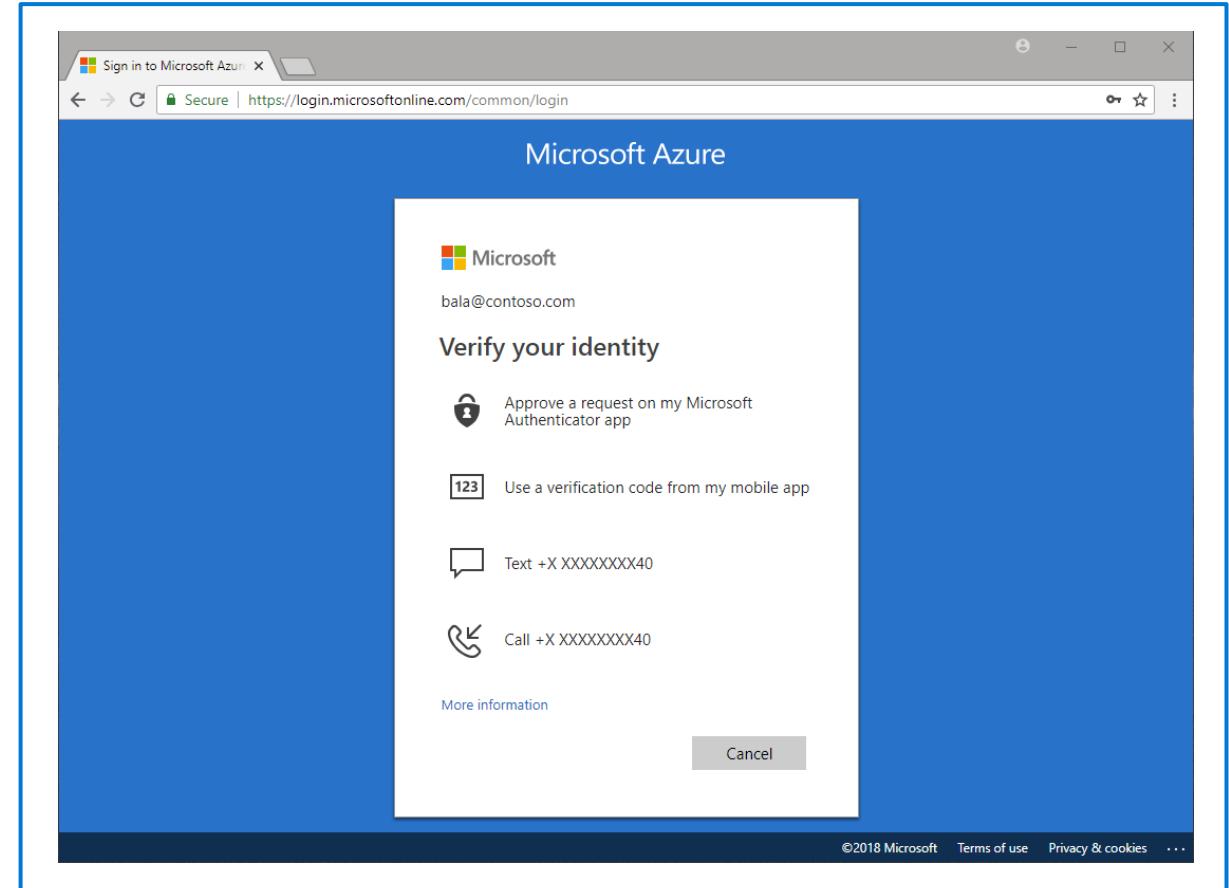
Mejora drásticamente la seguridad de una identidad, de una manera sencilla para los usuarios.

La MFA requiere más de una forma de verificación:

- Algo que usted sabe
- Algo que usted tiene
- Algo que es parte de usted

Valores predeterminados de seguridad

- Requiere que todos los usuarios completen la MFA según sea necesario.
- Obliga a los administradores a usar MFA.
- Aplica la MFA para todos los usuarios.



Capacidades de administración y protección de contraseñas

Reduzca el riesgo de que los usuarios establezcan contraseñas débiles.

- Lista global de contraseñas prohibidas.
- Listas personalizadas de contraseñas prohibidas.
- Protección contra la difusión de contraseñas.
- Se integra con un entorno de Active Directory local.

Custom smart lockout

Lockout threshold ⓘ 10

Lockout duration in seconds ⓘ 60

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

contoso
fabrikam
tailwind
michigan
wolverine
harbaugh
howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Demostración

- Métodos de autenticación y MFA



Objetivo de aprendizaje: Describir las capacidades de administración de acceso de Microsoft Entra

Acceso condicional

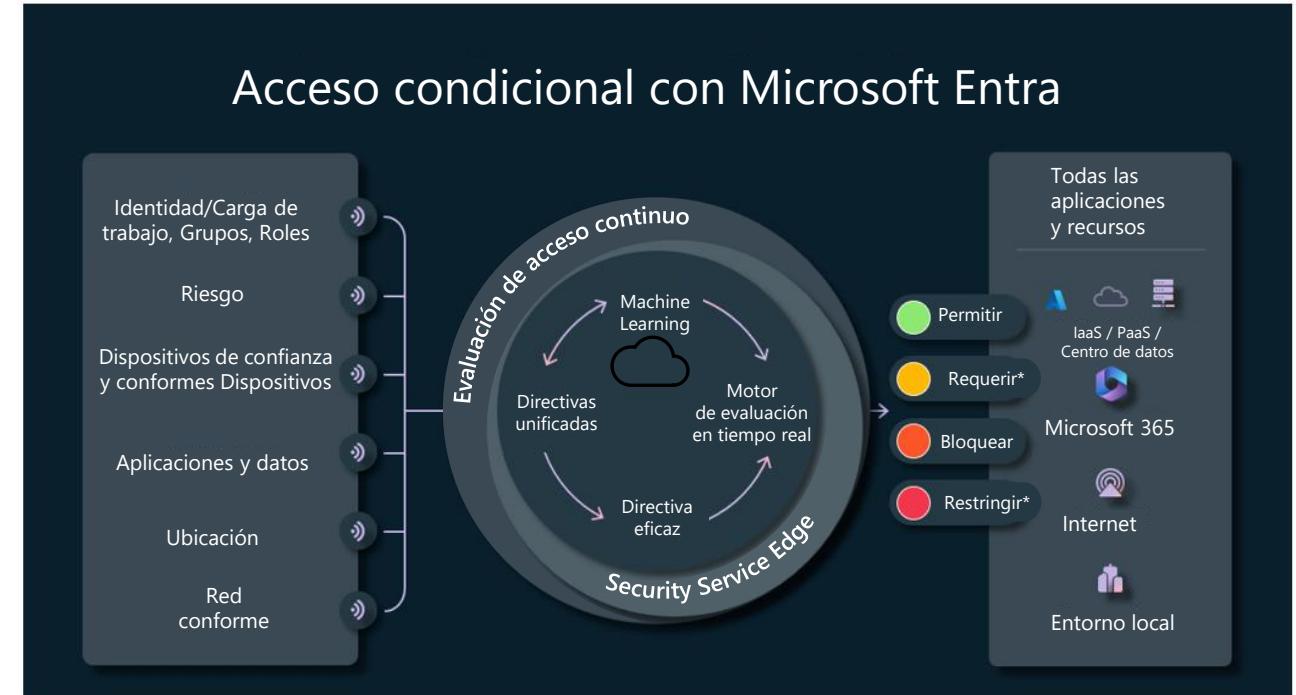
En su forma más simple, las directivas de acceso condicional (CA) son declaraciones “si-entonces”.

Las asignaciones determinan qué señales utilizar:

- Usuarios, grupos, identidades de carga de trabajo, roles de directorio
- Aplicaciones o acciones en la nube
- Detección de riesgos de inicios de sesión y usuario
- Dispositivo o plataforma de dispositivos
- Ubicación de la IP
- Más...

Los controles de acceso determinan cómo se aplica una directiva:

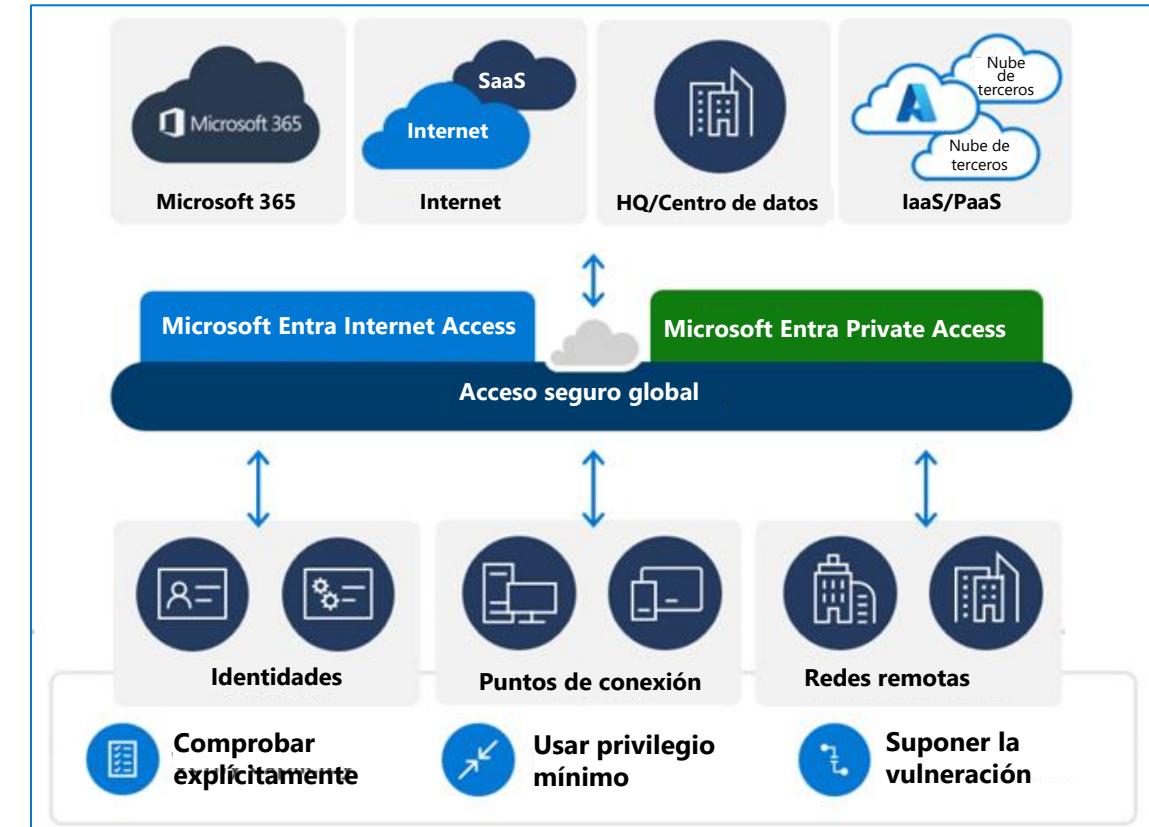
- Bloquear el acceso
- Conceder el acceso: Requiere que se cumplan una o más condiciones antes de conceder acceso.
- Control de sesiones: Permite una experiencia limitada.



Acceso seguro global de Microsoft Entra

El Acceso seguro global reúne los controles de acceso de red de Confianza cero, identidad y punto de conexión para proteger el acceso a cualquier aplicación o recurso, desde cualquier ubicación, dispositivo o identidad.

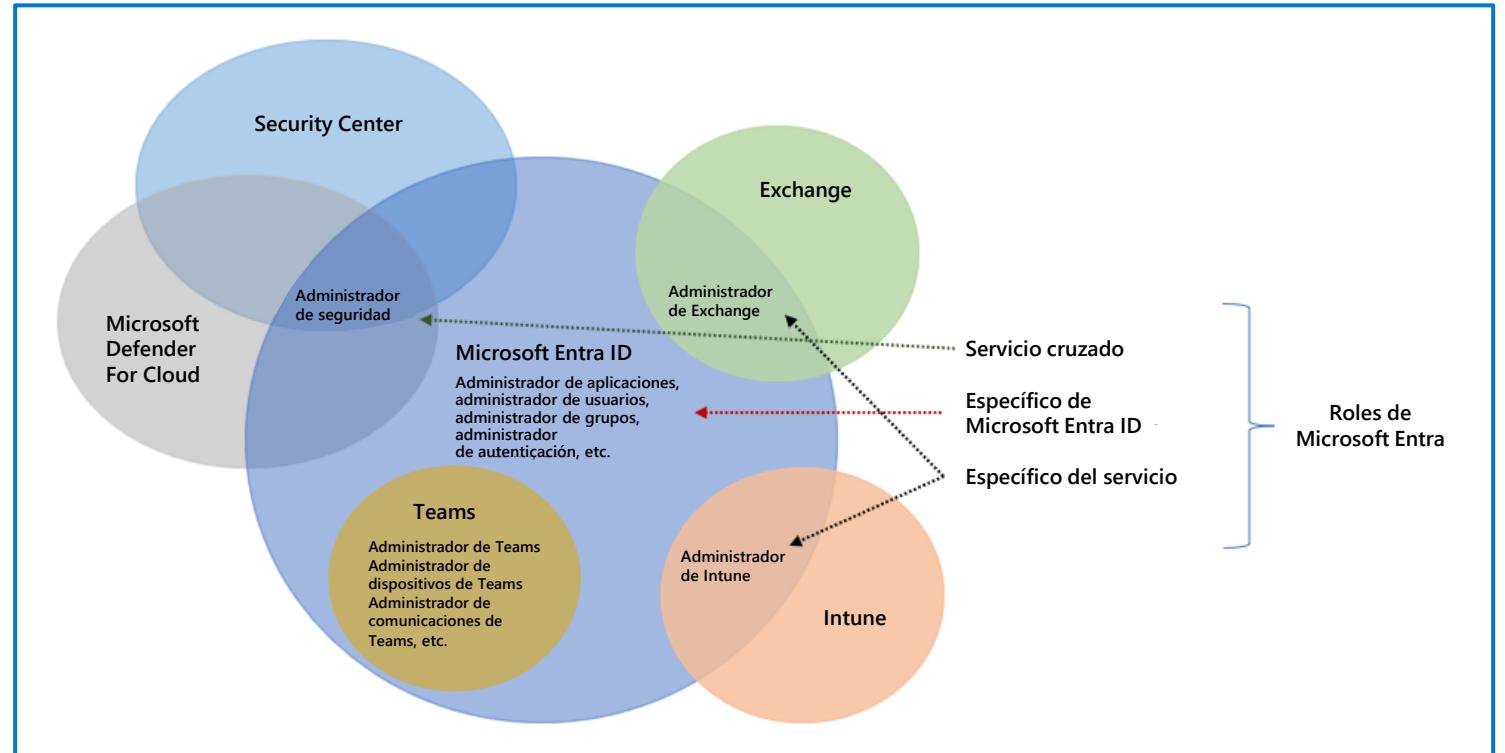
- **Microsoft Entra Internet Access** asegura el acceso a aplicaciones de SaaS, incluidos los servicios de Microsoft y las aplicaciones públicas de Internet.
- **Microsoft Entra Private Access** proporciona a sus usuarios acceso seguro a sus recursos privados y corporativos.



Roles y control de acceso basado en roles de Microsoft Entra

Los roles de Microsoft Entra controlan los permisos para administrar los recursos de Microsoft Entra.

- Roles integrados
- Roles personalizados
- Categorías de roles de Microsoft Entra:
 - Específico de Microsoft Entra
 - Específico del servicio
 - Servicio cruzado
- Conceda solo el acceso que los usuarios necesitan



Demostración

- Acceso condicional con Microsoft Entra



Objetivo de aprendizaje: Describa las capacidades de gobernanza y protección de identidades de Microsoft Entra

Gobernanza de identidades en Microsoft Entra

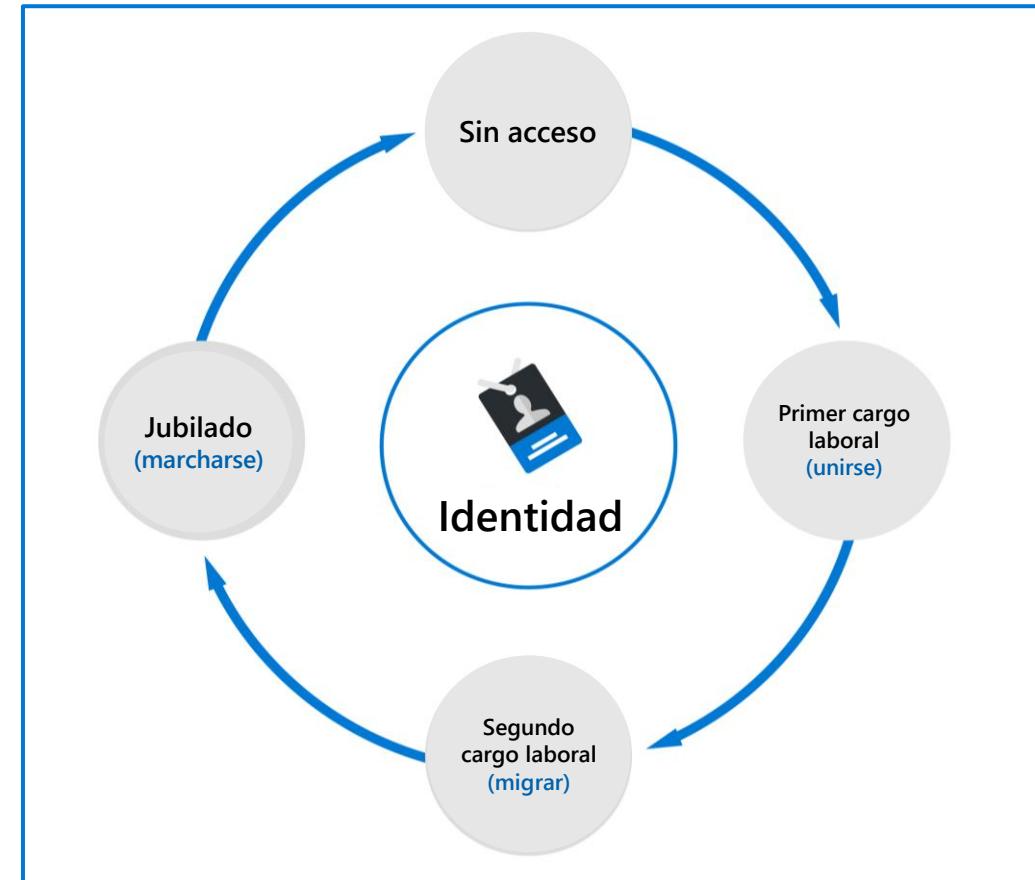
Asegúrese de que las personas correctas tengan el acceso correcto a los recursos adecuados.

Las tareas de gobernanza de identidades de Microsoft Entra

- Gobernanza del ciclo de vida de administración de identidades.
- Gobernanza del ciclo de vida de acceso.
- Acceso privilegiado seguro para la administración.

Ciclo de vida de la identidad

- Unir: Se crea una nueva identidad digital.
- Migrar: Se actualizan las autorizaciones de acceso.
- Marcharse: Es posible que sea necesario eliminar el acceso.



Revisiones de acceso

Revisiones de acceso

- Administre eficazmente las pertenencias a grupos, el acceso a aplicaciones empresariales y la asignación de roles.
- Garantice que solo las personas correctas tengan acceso a los recursos.
- Se utiliza para revisar y administrar el acceso tanto de usuarios como de invitados.

Revisiones de acceso en varias etapas

- Admite hasta tres etapas de revisión.
- Admite flujos de trabajo para cumplir con los requisitos de recertificación y auditoría que demandan varios revisores.
- Reduzca el número de decisiones de las que cada revisor es responsable.

Contoso

Please review users' access to the Finance Web app in FrickelsoftNET

Sarah Hoelzel, your organization requested that you approve or deny continued access for one or more users to the Finance Web app in the FinanceWeb access review. The review period will end on September 5, 2020.

Hi FinanceWeb team - please review the list of users who can access your FinanceWeb application. Help us remove any unwanted access from users that no longer work with the app. More information:
<https://finweb.contoso.com/access/reviews>

[Start review >](#)

Learn how to [perform an access review](#) and more about [Azure Active Directory access reviews](#).

[Privacy Statement](#)

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Facilitated by



Privileged Identity Management (PIM)

Administre, controle y supervise el acceso a recursos importantes en su organización.

-  Justo a tiempo, proporcionando acceso privilegiado solo cuando es necesario, y no antes.
-  Con límite de tiempo, mediante la asignación de fechas de inicio y de finalización que indican cuándo un usuario puede acceder a los recursos.
-  Basado en aprobación, que requiere una aprobación específica para activar los privilegios.
-  Visible, enviando notificaciones cuando se activen roles privilegiados.
-  Auditable, lo que permite descargar un historial completo del acceso.

Protección de identidades de Microsoft Entra

Detectar

- Clasifique el riesgo en tres niveles: bajo, medio y alto.
- Calcule el riesgo de inicio de sesión y el riesgo del usuario.

Investigar

- Informe de detecciones de riesgos
- Informe de inicios de sesión riesgosos
- Informe de usuarios riesgosos
- Informe de identidades de carga de trabajo riesgosas

Corregir

- Corrección automatizada
- Corrección manual

Exportar

- Exporte los datos de detección de riesgos a servicios de terceros para su posterior análisis.

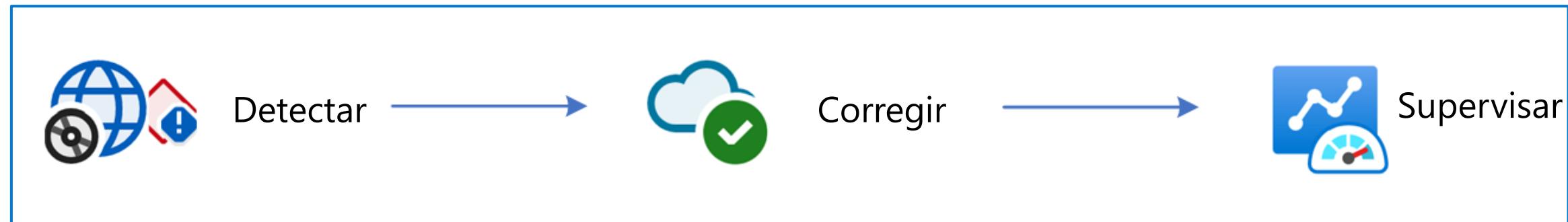
The screenshot shows a detailed view of a risky user in Microsoft Entra. The top navigation bar includes tabs for 'User's sign-ins', 'User's risky sign-ins' (which is selected), and 'User's risk detections'. Below the tabs, there are two main sections: 'Basic info' and 'Recent risky sign-ins'. The 'Basic info' section displays the following details:

User	Vjekoslav Vlasic
Roles	Limited admin
Username	vvlasic@woodgrove.ms
User ID	abcdefghijkl-xxxx-zzzz-1111-xxxxxxxxxx
Risk state	At risk
Risk level	Low
Details	-
Risk last updated	12/16/2021, 10:25:59 AM
Office location	[redacted]
Department	[redacted]
Mobile phone	[redacted]

Administración de permisos

Proporciona una visibilidad y control exhaustivos de los permisos para cualquier identidad y cualquier recurso en Microsoft Azure, Amazon Web Services (AWS) y Google Cloud Platform (GCP).

- Detectar: Evalúe los riesgos de los permisos mediante la evaluación de la brecha entre los permisos concedidos y los permisos utilizados.
- Corregir: Asigne permisos del tamaño adecuado en función del uso y conceda permisos a petición.
- Supervisar: Detecte actividades anómalas con alertas con tecnología de machine learning y genere informes forenses detallados.



Integración de Microsoft Entra con Seguridad de Microsoft Copilot

Experiencia independiente:

- Las funcionalidades de la experiencia independiente son consultas integradas.
- Use lenguaje natural para generar sus propias consultas.

Experiencia integrada:

- Compatible en el informe de los Usuarios riesgosos.
- Resuma el nivel de riesgo de un usuario, proporcione información y brinde recomendaciones para una mitigación rápida.

MICROSOFT ENTRA

[Explore a summary of a users active risk with Entra ID Protection.](#)

View a detailed summary of a Microsoft Entra ID users risk.

[Explore diagnostic log collection in Microsoft Entra](#)

View settings for diagnostic log collection and streaming of activity logs in Microsoft Entra ID

[Explore Microsoft Entra audit log details](#)

View changes to applications, groups, users, and licenses in Microsoft Entra ID

[Find group details in Microsoft Entra](#)

View Microsoft Entra ID group ownership and membership details

[Find sign-in logs in Microsoft Entra](#)

View Microsoft Entra ID sign-in log details including policy evaluation results, and details on the loc...

[Find user details in Microsoft Entra](#)

View contact information, authentication method registration, and account details for users in Micr...

[Investigate identity risks with Entra ID Protection](#)

View details of Microsoft Entra ID users with high, medium, or low risk of compromise

**Describir las capacidades de las soluciones
de seguridad de Microsoft (parte 1 de 3)**

Objetivos de aprendizaje

- Describir Seguridad de Microsoft Copilot
- Describir los servicios principales de seguridad de infraestructura en Azure

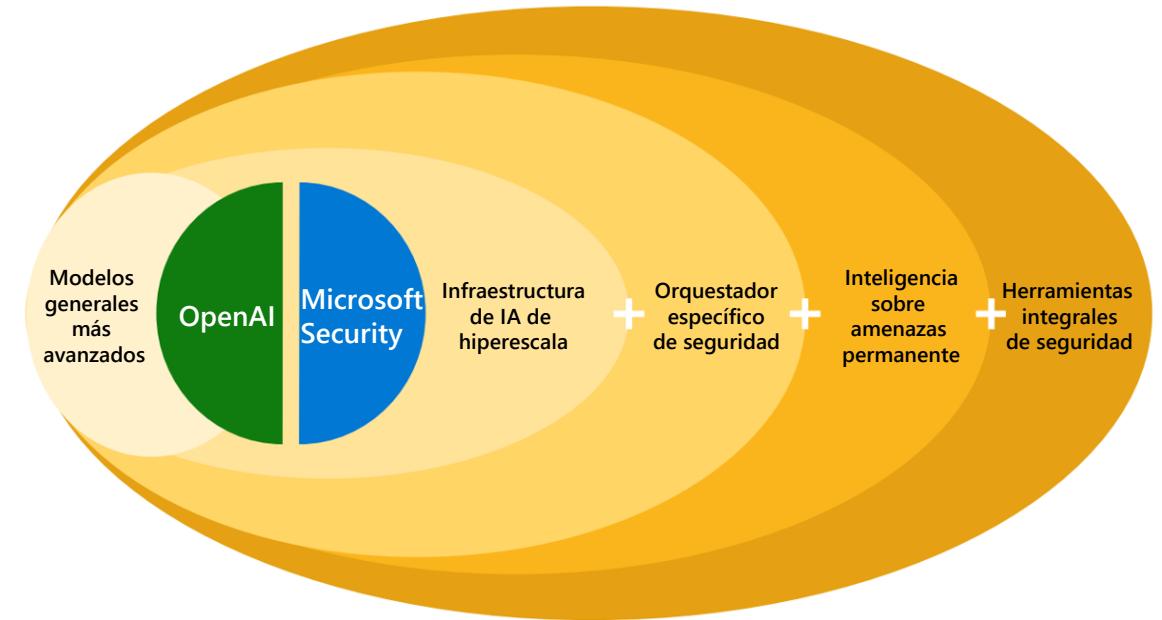


**Objetivo de aprendizaje: Describir Seguridad
de Microsoft Copilot**

Describir Seguridad de Microsoft Copilot: ¿Qué es?

Una herramienta de análisis de seguridad basada en la nube con tecnología de IA que permite a los analistas responder a las amenazas rápidamente, procesar señales a la velocidad de la máquina y evaluar la exposición al riesgo más rápidamente de lo que sería posible de otra manera.

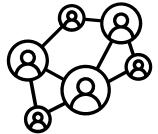
- Copilot combina potentes LLM con un modelo específico de seguridad de Microsoft.
- Copilot se integra con fuentes que son de Microsoft y no son de Microsoft.
- Copilot aprende a la velocidad de la máquina para ayudar a los analistas a identificar y responder a las amenazas emergentes.
- Los datos empresariales están protegidos con controles de seguridad y cumplimiento empresariales completos.



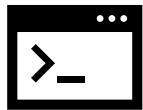
Describir Microsoft Security Copilot: casos de uso



Resumen del incidente. Extraiga alertas de seguridad complejas en resúmenes prácticos concisos.



Análisis del impacto. Evalúe el impacto potencial de los incidentes de seguridad para permitir tiempos de respuesta más rápidos y una toma de decisiones optimizada.



Ingeniería inversa de scripts. Analice scripts de línea de comandos complejos y tradúzcalos a lenguaje natural con explicaciones claras de las acciones.

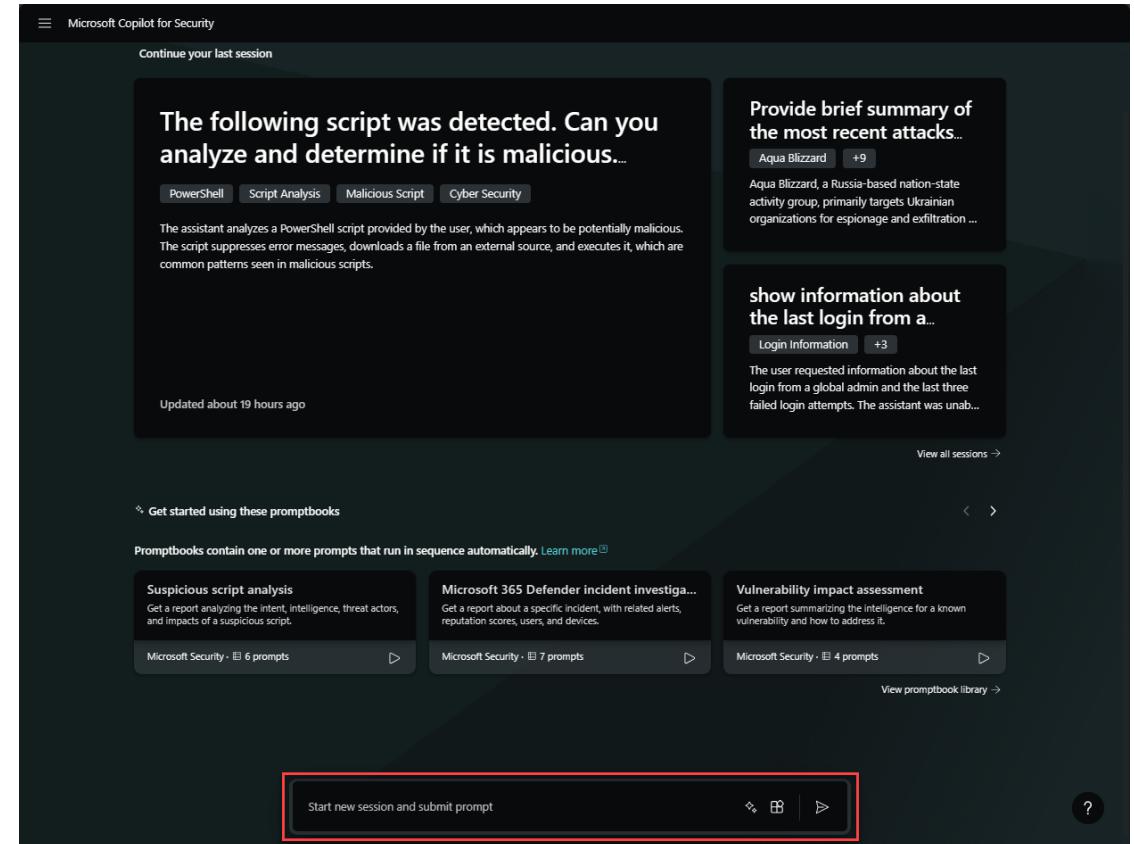


Respuestas guiadas. Guía práctica paso a paso para la respuesta ante incidentes, que incluye instrucciones para la clasificación, investigación, contención y corrección.

Describir Seguridad de Microsoft Copilot: Experiencia independiente

Experimente Copilot a través de un sitio exclusivo (experiencia independiente).

Los usuarios realizan solicitudes en lenguaje natural y reciben respuestas como texto, imágenes o documentos.



Describir Microsoft Security Copilot: experiencia integrada

Algunos productos de Microsoft integran Copilot directamente en su interfaz de usuario.

The screenshot shows the Microsoft 365 Defender Advanced hunting interface. On the left is a navigation sidebar with options like Home, Incidents & alerts, Hunting (Advanced hunting selected), Actions & submissions, Threat intelligence, Learning hub, Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Assets, and Devices. The main area is titled "Advanced hunting" and contains a "Query" section with a Kusto query:

```
1 let logonAttempts = DeviceLogonEvents  
2 | where ActionType == "LogonAttempted"  
3 | project Timestamp, DeviceId, AccountDomain;  
4 let credentialTheftEvents = DeviceEvents  
5 | where ActionType in ("AsrlsassCredentialTheftAudited", "AsrlsassCred  
6 | project Timestamp, DeviceId, InitiatingProcessAccountDomain;  
7 logonAttempts  
8 | join kind=inner credentialTheftEvents on $left.DeviceId == $right.De  
9 | summarize count() by AccountDomain  
10 | order by count_ desc  
11
```

Below the query is a message: "No results found in the specified time frame." To the right of the query is a "Security Copilot" pane with a red border, containing a history of queries and an "Ask a question to generate a query" input field at the bottom, also with a red border.

Describir la terminología de Microsoft Security Copilot

- **Sesión:** una conversación particular dentro de Microsoft Security Copilot.
- **Consulta:** una declaración o pregunta específica de un usuario dentro de una sesión.
- **Capacidad:** una función que Seguridad de Microsoft Copilot utiliza para resolver parte de un problema.
- **Complemento:** una colección de capacidades de un recurso en particular, como Microsoft Intune.
- **Orquestador:** se utiliza para componer habilidades juntas, a fin de responder a la consulta de un usuario.



La barra de consultas,
que se utiliza para
ingresar consultas.

Ejemplo: complementos y capacidades

Manage sources

Plugins Manage plugins
Turn on or create your own plugins to give Copilot access to the security services and websites you use. [Learn more](#)

All (60) On (11) Off (49)

Microsoft ⚡

- Azure Firewall** Preview
Intrusion Detection and Prevention System (IDPS) signature analysis and fleet-wide IDPS attack investigation
- Azure Web Application Firewall** Preview
SQL injection block summaries, XSS block summaries, top WAF rules summaries and top malicious IP summaries
- Microsoft Defender External Attack Surface Management**
Attack surfaces, vulnerable assets, and attack surface insights

Show 11 more ▾

← Search

SYSTEM CAPABILITIES

Capabilities are based on the plugins you have set up.

AZURE FIREWALL Preview

- Get details on an IDPS signature**
Expand on the description of an IDPS signature in the Azure Firewall logs.
- Get top IDPS signature hits**
Retrieve the top IDPS signature hits for an Azure Firewall.
- Search across firewalls for an IDPS signature**
Look for a given IDPS signature across your tenant, subscription, or resource group.
- Secure your environment using IDPS**
Generate recommendations to secure your environment using Azure Firewall's IDPS feature.

Describa cómo Seguridad de Microsoft Copilot procesa las solicitudes de consultas



Describa los elementos de una consulta eficaz

Objetivo

¿Cuál es la información relacionada con la seguridad específica que necesita?

"Deme información sobre el incidente 18718..."



Contexto

¿Por qué la necesita y cómo usará la información?

"... para un informe que puedo enviar a mi gerente"



Expectativas

¿En qué formato o para qué público quiere que la respuesta se adapte?

"Compile la información en una lista, con un breve resumen"



Fuente

¿Existe un complemento, información u origen de datos que Seguridad de Copilot debiera usar?

"Busque en los incidentes de Defender"

Habilitar Seguridad de Copilot

1. Aprovisione la capacidad de Copilot
 - i. Seguridad de Microsoft Copilot se vende como una oferta de consumo.
 - ii. Aprovisione unidades informáticas de seguridad (SCU), la potencia informática utilizada para ejecutar Copilot.
2. Configure el entorno predeterminado
 - i. Asigne la capacidad de las SCU.
 - ii. Establezca la ubicación geográfica para el almacenamiento de datos.
 - iii. Configure las opciones de uso compartido de datos.
3. Asigne permisos de roles

Home > Microsoft Copilot for Security compute capacities >
Set up your Copilot capacity ...

Basics Review + Create

This capacity will provide the computing power that drives the Microsoft Copilot for Security experience.

Project Details

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Capacity details

Name your capacity and select a location

Capacity name * ⓘ Enter a name
This name must be unique and contain only lowercase letters and numbers with no spaces.

Prompt evaluation location * ⓘ United States (US)

If this location is busy, allow Copilot to evaluate prompts anywhere in the world (recommended for optimal performance).

Capacity region ⓘ US East

Security compute units

Security compute units provide the computing power that drives the Security Copilot experience (\$4 per unit). Read more about [security_capacity_units](#) and the recommended number based on your organization's size and probable usage.

Security compute units per hour * ⓘ 1 Estimated monthly cost \$2880/month

I acknowledge that I have read, understood, and agreed to the [Terms and Conditions](#)

[Previous](#) [Next](#) [Review + create](#)

Demostración

- Seguridad de Microsoft Copilot: Explore la experiencia independiente

Objetivo de aprendizaje: Describir los servicios principales de seguridad de infraestructura en Azure

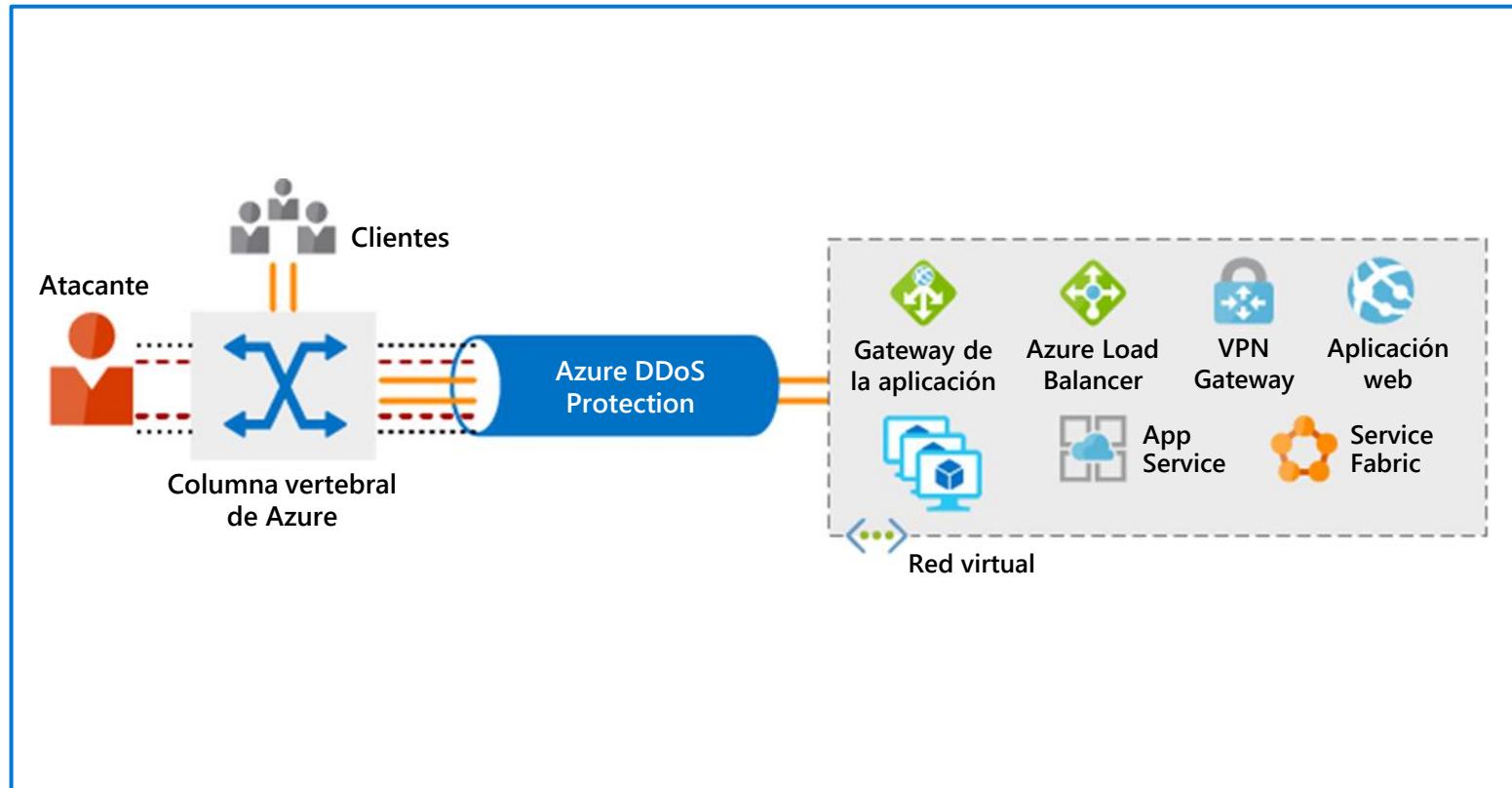
Protección contra ataques de denegación de servicio distribuido (DDoS) de Azure

Denegación de servicio distribuido (DDoS)

- Ataques que hacen que los recursos no respondan.

Azure DDoS Protection

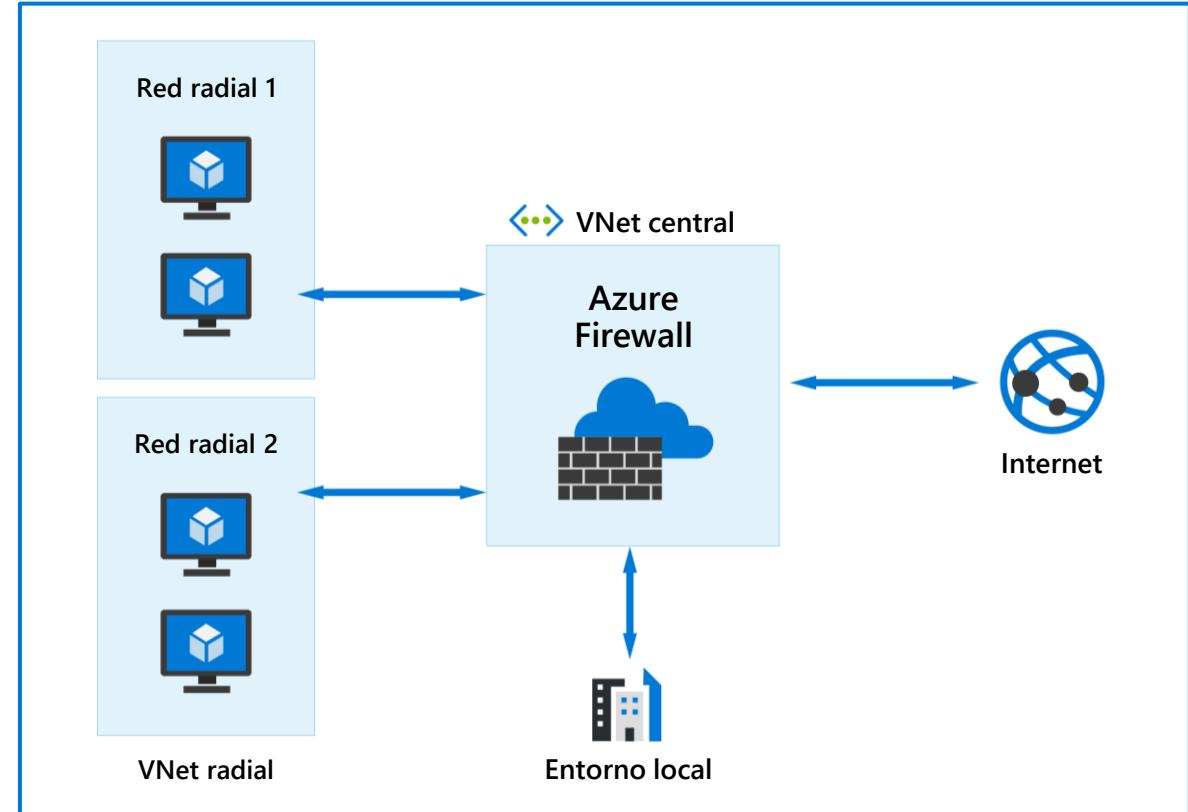
- Analiza el tráfico de red y descarta cualquier cosa que parezca un ataque de DDoS.
 - Supervisión del tráfico siempre activa.
 - Ajuste adaptable en tiempo real.
 - Telemetría, supervisión y alertas de protección de DDoS.



Azure Firewall

Azure Firewall protege los recursos de su red virtual (VNet) de Azure de los atacantes.

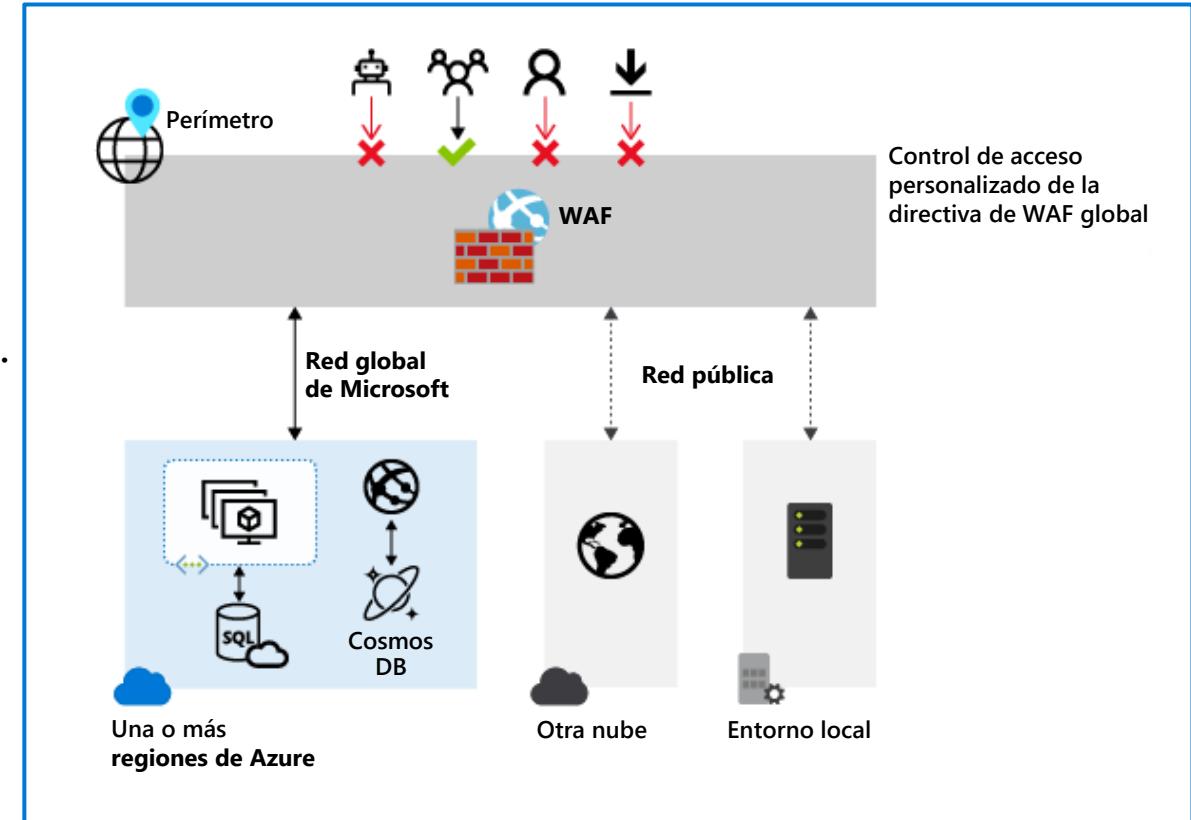
- Cree reglas para el filtrado de red que otorgan o rechazan el acceso.
- Use el feed de la Inteligencia sobre amenazas de Microsoft para alertar o filtrar el tráfico desde/hacia direcciones IP y dominios maliciosos conocidos.
- Todas las direcciones de IP de tráfico de red virtual salientes se traducen a la IP pública de Azure Firewall para dificultar que los atacantes ataquen los dispositivos de la red interna.
- Integración con Microsoft Copilot para seguridad
- Y mucho más...



Web Application Firewall (WAF)

Protección centralizada de sus aplicaciones web frente a las vulnerabilidades y ataques más comunes.

- Protección contra amenazas e intrusiones
- Protege sus aplicaciones web de ataques de DDoS.
- Corrige una vulnerabilidad conocida en un solo lugar.
- Integración con Microsoft Copilot para seguridad
- Y más...



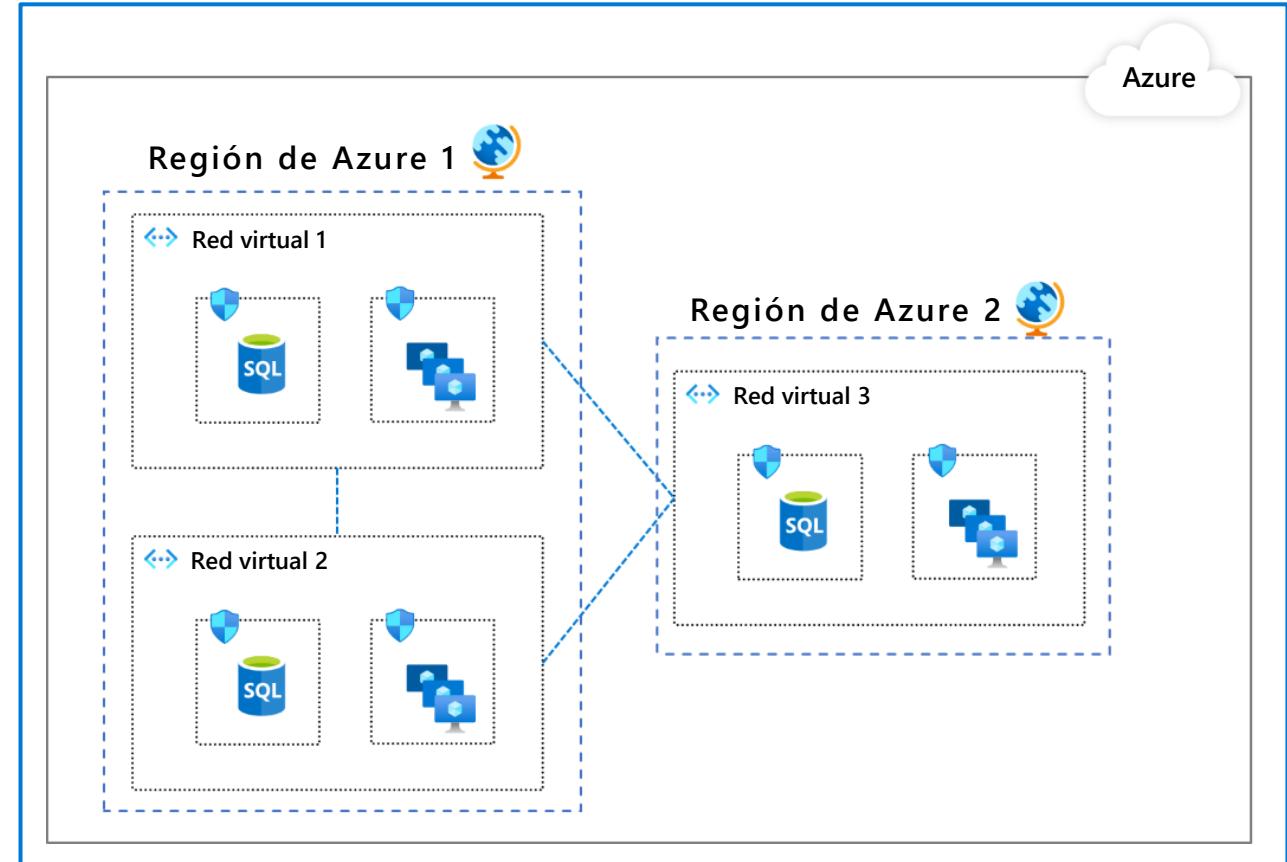
Segmentación de red y Azure Virtual Network (VNet)

Razones para usar la segmentación de la red

- Capacidad de agrupar activos relacionados.
- Aislamiento de recursos.
- Directivas de gobernanza establecidas por la organización.

Red virtual (VNet) de Azure

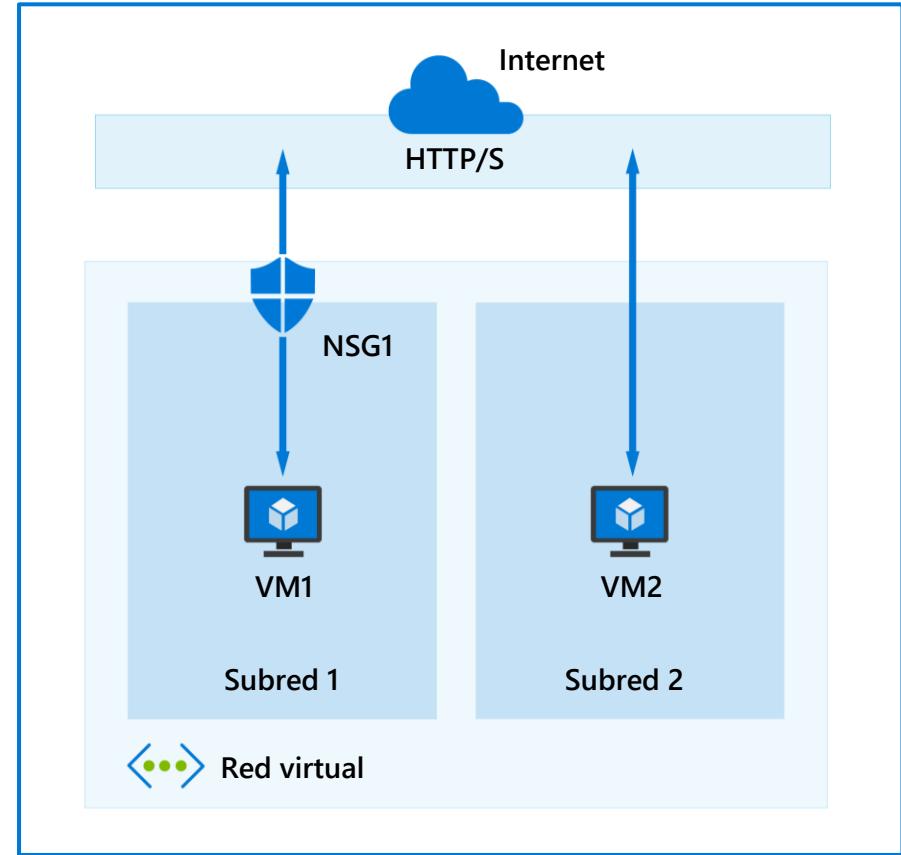
- Contención de recursos en el nivel de red, sin tráfico permitido a través de VNet o tráfico entrante a VNet.
- La comunicación debe aprovisionarse explícitamente.
- Controle cómo los recursos de una red virtual se comunican con otros recursos, Internet y las redes locales.



Grupos de seguridad de red (NSG) de Azure

Filtre el tráfico de red entre recursos de Azure en una red virtual de Azure.

- Un NSG se compone de reglas de seguridad entrantes y salientes que aceptan o rechazan el tráfico.
- Un NSG puede contener muchas reglas que se procesan en función de su prioridad asignada.
- Cuando se crea un NSG, incluye reglas entrantes y salientes predeterminadas.
- No puede quitar las reglas predeterminadas, pero puede sustituirlas creando nuevas reglas con prioridades más altas.



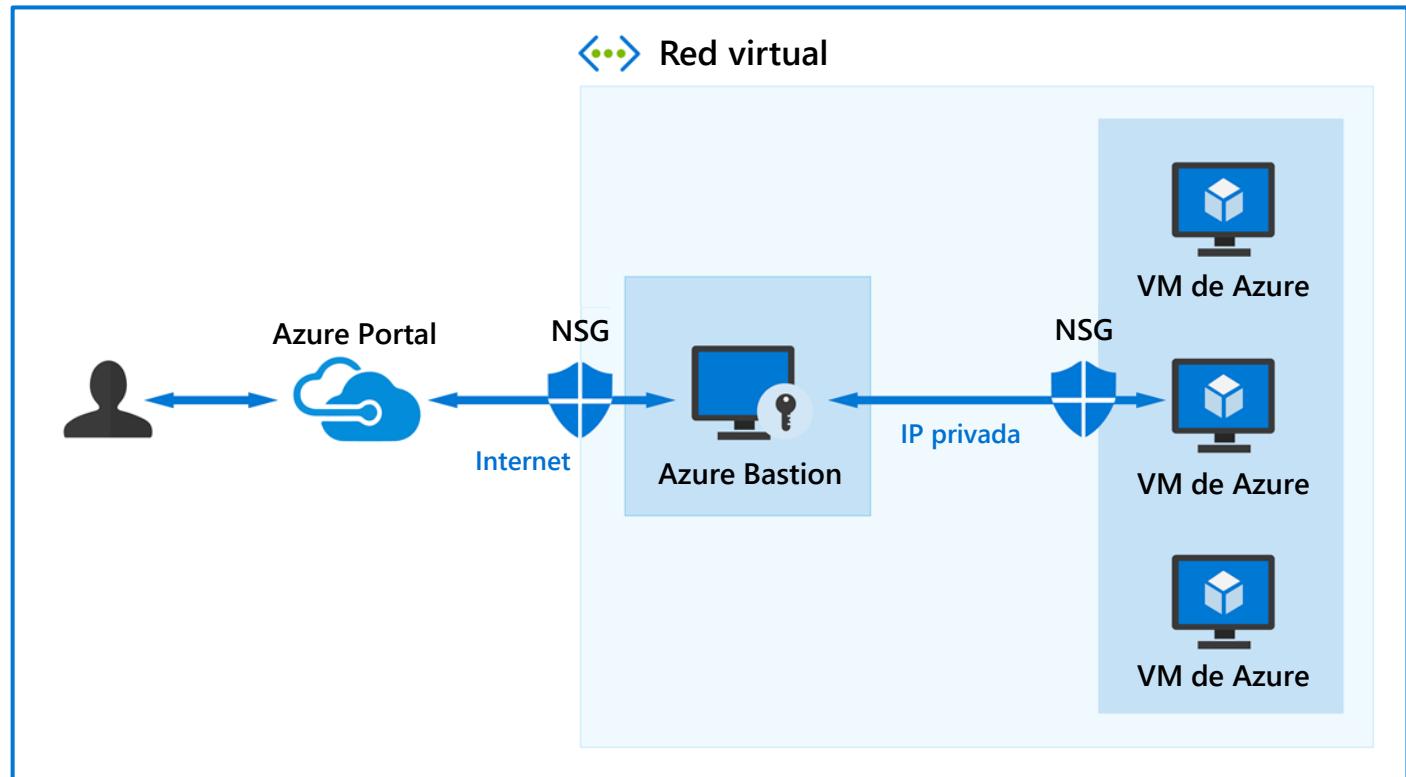
Demostración

- Grupos de seguridad de red (NSG) de Azure

Azure Bastion

Azure Bastion ofrece conectividad segura a sus máquinas virtuales (VM) desde el portal de Azure.

- Protocolo de escritorio remoto (RDP) y Secure Shell (SSH) directamente en el portal de Azure.
- Transite por los firewalls corporativos de forma segura.
- No se requiere una IP pública en una VM de Azure.
- No es necesario administrar grupos de seguridad de red (NSG).
- Protege contra el escaneo de puertos.
- Protege contra vulneraciones de día cero.

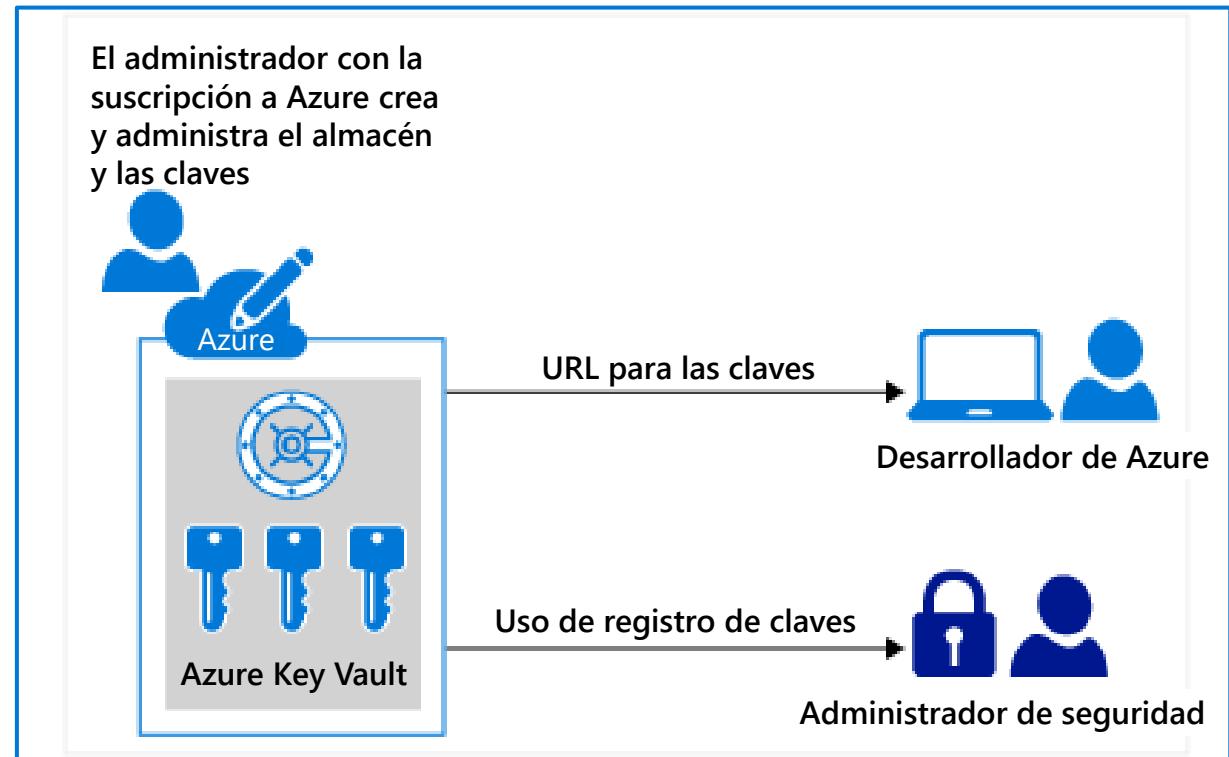


Azure Key Vault

Un servicio en la nube para almacenar y acceder de forma segura a secretos, como claves de API, contraseñas, certificados o claves criptográficas.

Beneficios de Key Vault

- Centralizar los secretos de aplicaciones.
- Almacenar los secretos y las claves de forma segura.
- Supervisar el acceso y el uso.
- Administración simplificada de secretos de aplicaciones.
- Dos niveles:
 - Estándar: Cifrado basado en software.
 - Premium: Claves protegidas por el módulo de seguridad de hardware (HSM).



**Describir las capacidades de las soluciones
de seguridad de Microsoft (parte 2 de 3)**

Objetivos de aprendizaje

- Describir las capacidades de administración de seguridad en Azure
- Describir las capacidades de Microsoft Sentinel



Objetivo de aprendizaje: Describir las capacidades de administración de seguridad en Azure

Microsoft Defender for Cloud

Es una plataforma de protección de aplicaciones nativa de la nube (CNAPP) con un conjunto de medidas y prácticas de seguridad diseñadas para proteger las aplicaciones basadas en la nube de diversas ciberamenazas y vulnerabilidades.

Administración de la postura de seguridad en la nube (CSPM)

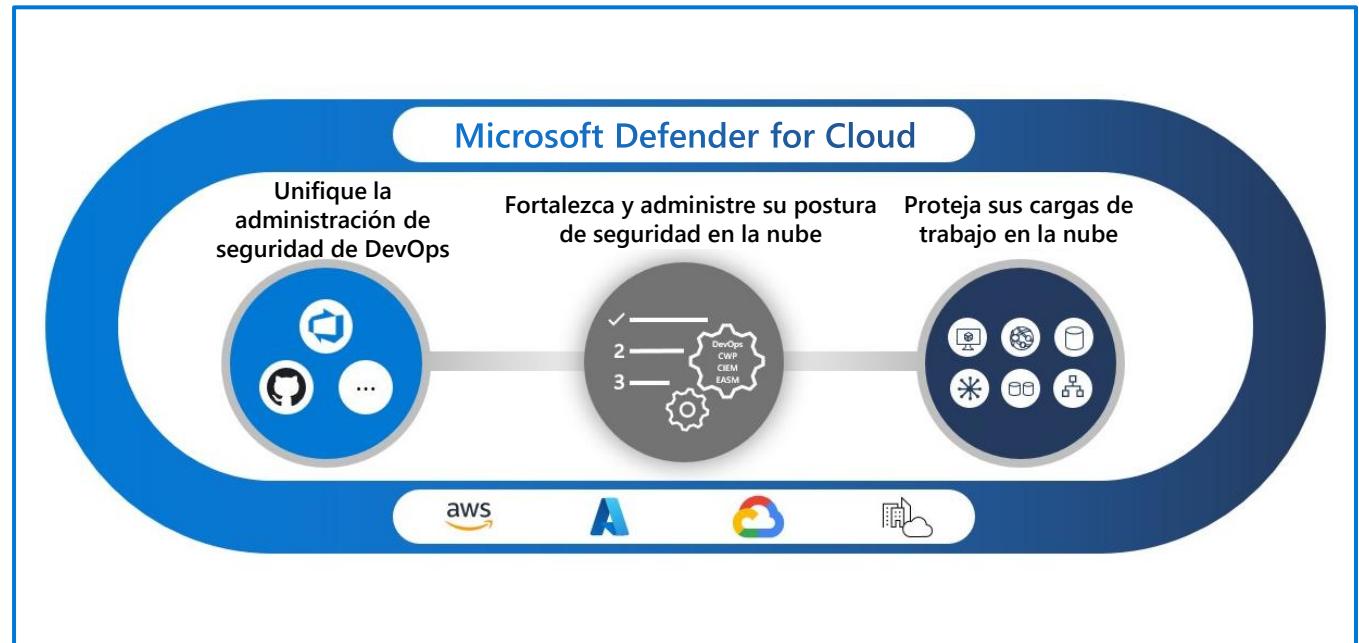
Presenta las acciones que puede tomar para evitar filtraciones.

Plataforma de protección de cargas de trabajo en la nube (CWPP)

Ofrece protecciones específicas para servidores, contenedores, almacenamiento, bases de datos y otras cargas de trabajo.

Operaciones de seguridad y desarrollo (DevSecOps)

Unifica la administración de la seguridad en el nivel de código en entornos con varias nubes y varias canalizaciones.



Cómo las directivas e iniciativas de seguridad mejoran la postura de seguridad en la nube

Iniciativas de seguridad

- Una colección de directivas.
- Se asignan a recursos, suscripciones y más.

Comparativa de seguridad en la nube de Microsoft (MCSB)

- Iniciativa de seguridad predeterminada en Defender for Cloud.
- Proporciona procedimientos recomendados y recomendaciones para mejorar la seguridad de sus cargas de trabajo, datos y servicios en Azure y otras nubes.

Microsoft Defender for Cloud

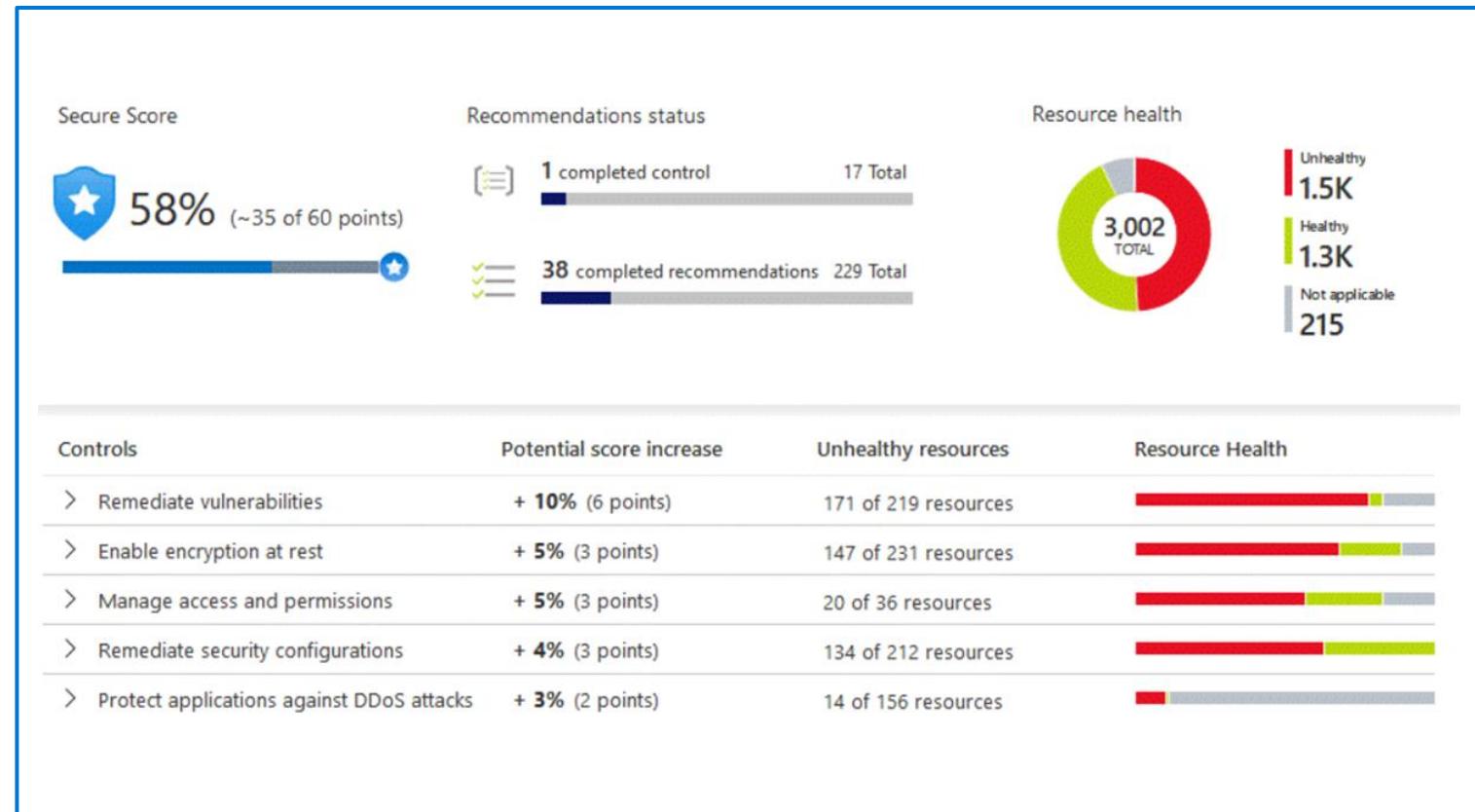
- Evalúa continuamente su entorno con MCSB y otras iniciativas de seguridad.

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. On the left, there's a sidebar with navigation links like Home, Microsoft Defender for Cloud, General, Overview, Getting started, Recommendations, Security alerts, Inventory, Cloud Security Explorer (Preview), Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, Regulatory compliance, Workload protections, Firewall Manager, DevOps Security (Preview), Management, Environment settings, Security solutions, and Workflow automation. The main area has a header "Microsoft Defender for Cloud | Regulatory compliance" and a sub-header "Showing subscription 'Azure Pass - Sponsorship'". It features a search bar and several buttons: Download report, Manage compliance policies, Open query, Compliance over time workbook, Audit reports, and Compliance offerings. A message says, "You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above." Below this is a section titled "Microsoft cloud security benchmark (preview)" with a progress bar showing "48 of 59 passed controls". To its right is a section titled "Lowest compliance regulatory standards" with three items: SOC TSP (13/13), PCI DSS 3.2.1 (43/43), and ISO 27001 (20/20). Further down is a poll asking, "Is the regulatory compliance experience clear to you? Yes or No". A red box highlights the "Microsoft cloud security benchmark" link. At the bottom, it says "Microsoft cloud security benchmark is applied to the subscription Azure Pass - Sponsorship" and lists three categories: NS. Network Security (with a red error icon), IM. Identity Management (with a green success icon), and PA. Privileged Access (with a green success icon).

Administración de la postura de seguridad en la nube (CSPM)

Visibilidad y recomendaciones

- Evalúa continuamente sus recursos, sus suscripciones y su organización en busca de problemas de seguridad.
- Agrega todos los hallazgos en una única puntuación de seguridad.
- Ofrece recomendaciones de fortalecimiento sobre cualquier error de configuración y debilidad de seguridad identificada.
- Proporciona visibilidad y recomendaciones en todo el entorno multinube.
- Incorpora capacidades de Seguridad de Microsoft Copilot en la página de recomendaciones.



Plataforma de protección de cargas de trabajo en la nube (CWPP)

Los planes de CWPP ofrecen características de seguridad mejoradas para sus cargas de trabajo.

- Detección y respuesta de puntos de conexión
- Análisis de vulnerabilidades
- Seguridad multinube
- Seguridad híbrida
- Alertas de protección contra amenazas
- Controles de acceso y aplicaciones

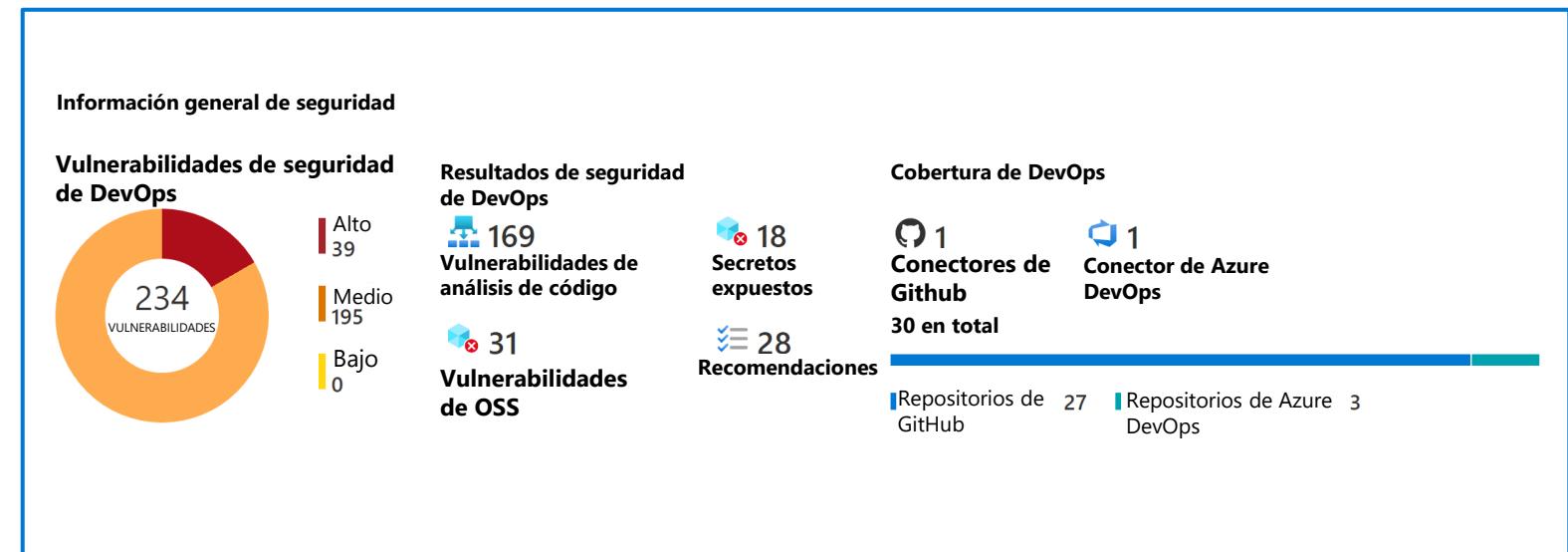
 Enable the enhanced security features of Microsoft Defender for Cloud. [Learn more >](#)

Enhanced security off	Enable all Microsoft Defender for Cloud plans
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Secure score	✓ Secure score
✗ Just in time VM Access	✓ Just in time VM Access
✗ Adaptive application controls and network hardening	✓ Adaptive application controls and network hardening
✗ Regulatory compliance dashboard and reports	✓ Regulatory compliance dashboard and reports
✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)	✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
✗ Threat protection for supported PaaS services	✓ Threat protection for supported PaaS services

Operaciones de seguridad y desarrollo (DevSecOps)

Capacita a los equipos de seguridad para que administren la seguridad de las operaciones de desarrollo (DevOps) en entornos de varias canalizaciones.

- Visibilidad unificada de la postura de seguridad de DevOps.
- Fortalezca las configuraciones de los recursos de la nube en el ciclo de vida de desarrollo.
- Priorice la corrección de problemas críticos en el código.



Demostración

- Microsoft Defender for Cloud



Objetivo de aprendizaje: Describir las capacidades de Microsoft Sentinel

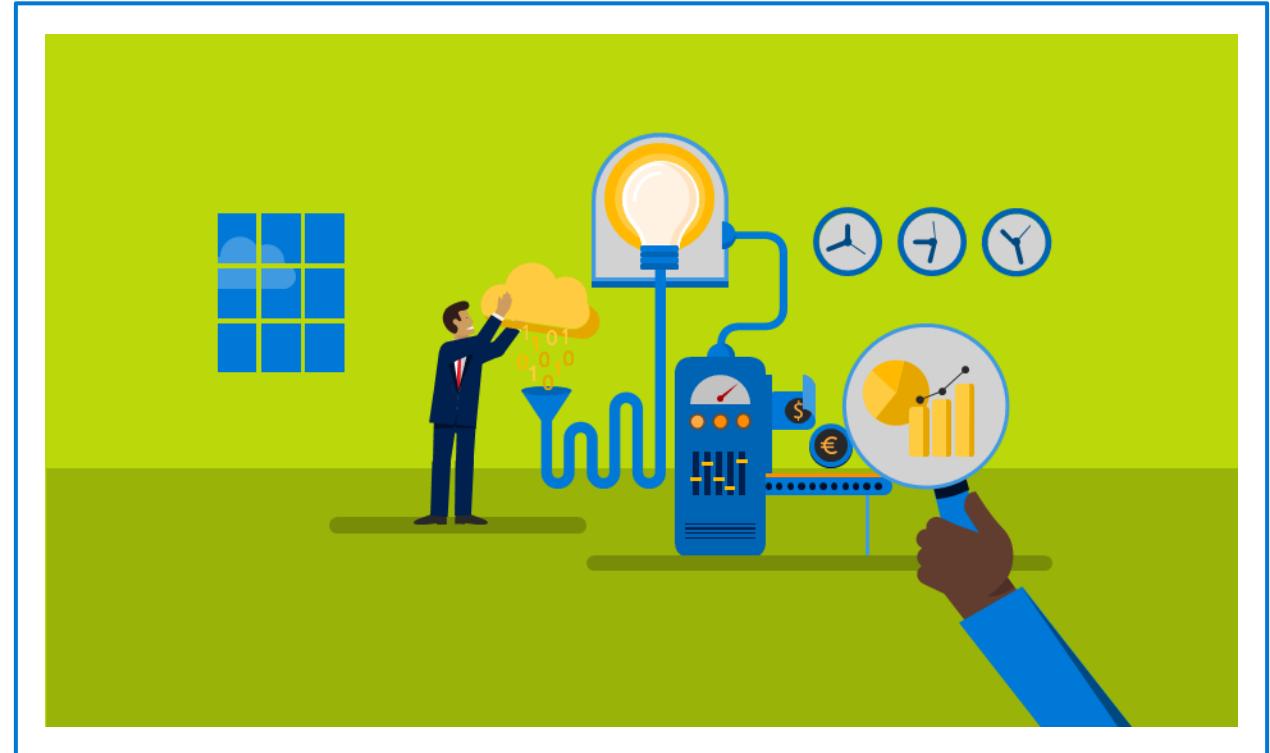
SIEM y SOAR

Administración de eventos e incidentes de seguridad (SIEM)

- Recopila datos de todo el patrimonio digital.
- Analiza y busca correlaciones o anomalías.
- Genera alertas e incidentes.

Coordinación, automatización y respuestas de seguridad (SOAR)

- Toma alertas de muchos orígenes, como sistemas de SIEM.
- Desencadena flujos de trabajo y procesos automatizados basados en acciones.
- Ejecuta tareas de seguridad que mitigan el problema.



Detección y mitigación de amenazas de Microsoft Sentinel

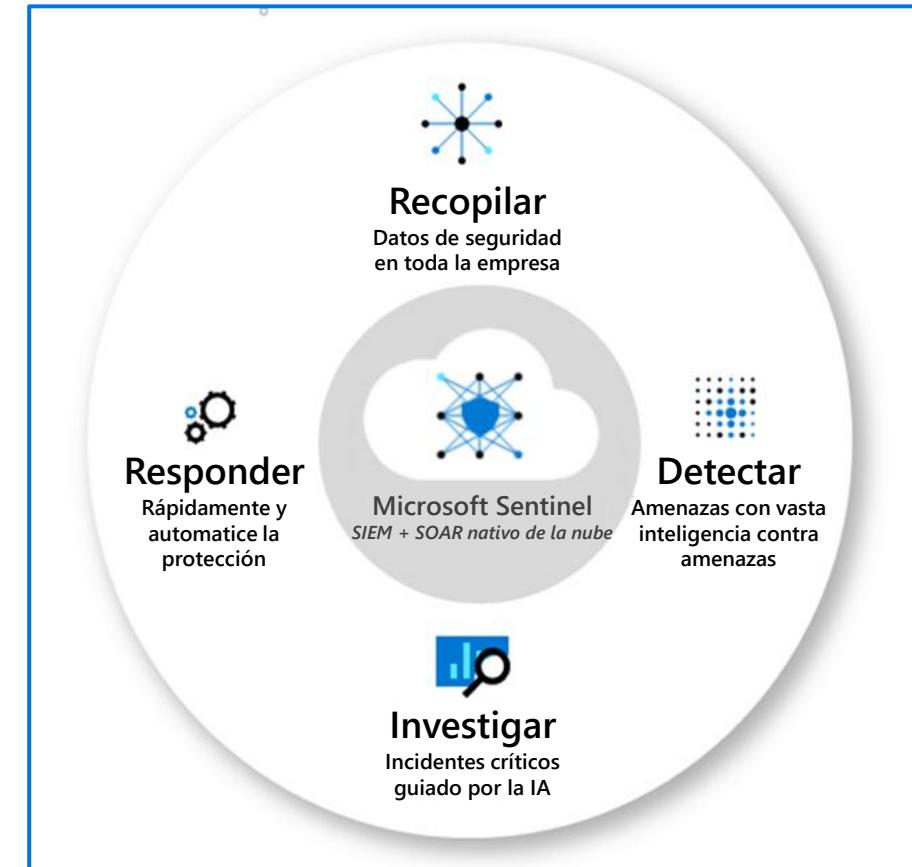
Recopile datos a escala de nube, en todos los usuarios, dispositivos, aplicaciones e infraestructura, tanto locales como en varias nubes.

Detecte las amenazas previamente descubiertas y minimice los falsos positivos mediante el análisis y la inteligencia contra amenazas sin igual.

Investigue las amenazas con IA y busque de forma proactiva actividades sospechosas a escala, aprovechando décadas de trabajo de ciberseguridad en Microsoft.

Responda rápidamente a los incidentes con la orquestación integrada y la automatización de tareas de seguridad comunes.

Ahora se puede acceder a Microsoft Sentinel desde el portal de Microsoft Defender, que ofrece la plataforma de operaciones de seguridad unificadas de Microsoft.



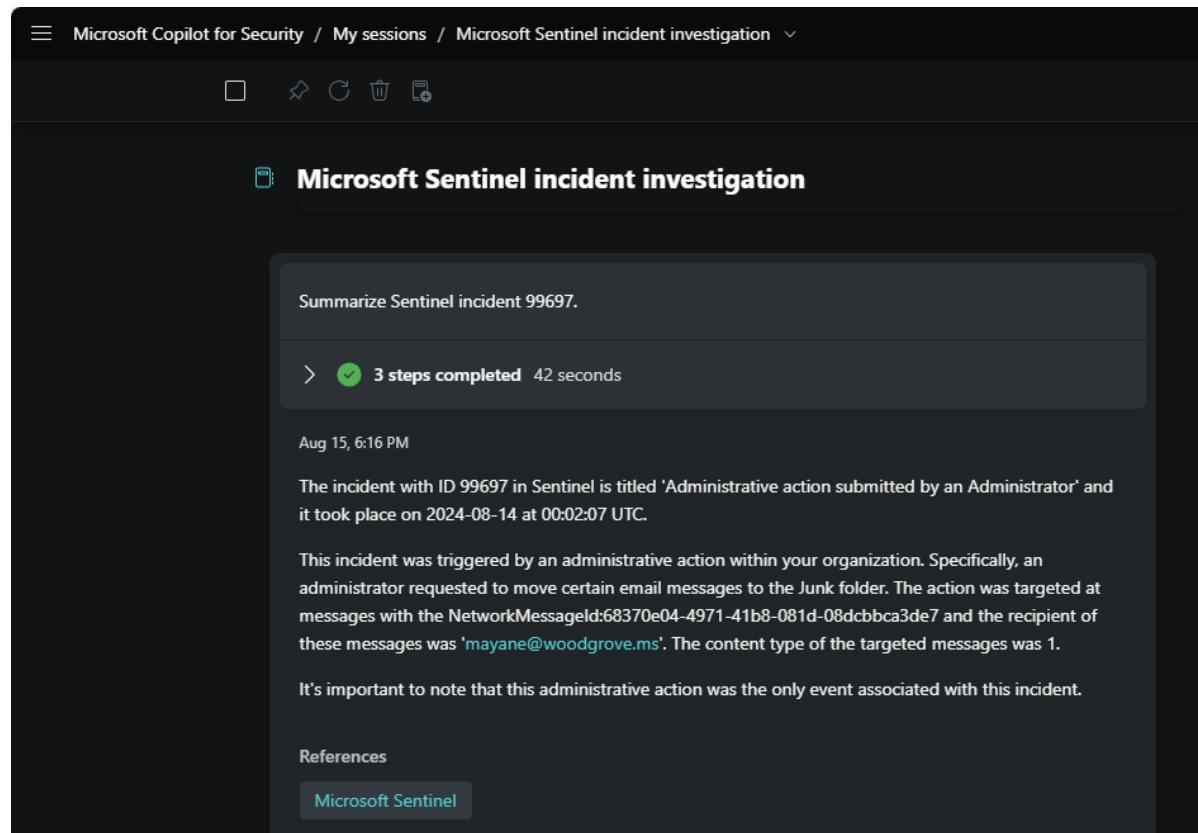
Integración de Seguridad de Microsoft Copilot con Microsoft Sentinel

Complementos de Copilot:

- Microsoft Sentinel
- Lenguaje natural para KQL para Microsoft Sentinel

Integración de Copilot admitida a través de:

- Experiencia independiente
- Experiencia integrada en el portal de Microsoft Defender



Demostración

- Microsoft Sentinel

Describir las capacidades
de las soluciones de seguridad
de Microsoft (parte 3 de 3)



Objetivos de aprendizaje

- Describir la protección contra amenazas con Microsoft Defender XDR



**Objetivo de aprendizaje: Describir la protección
contra amenazas con Microsoft Defender XDR**

Microsoft Defender XDR

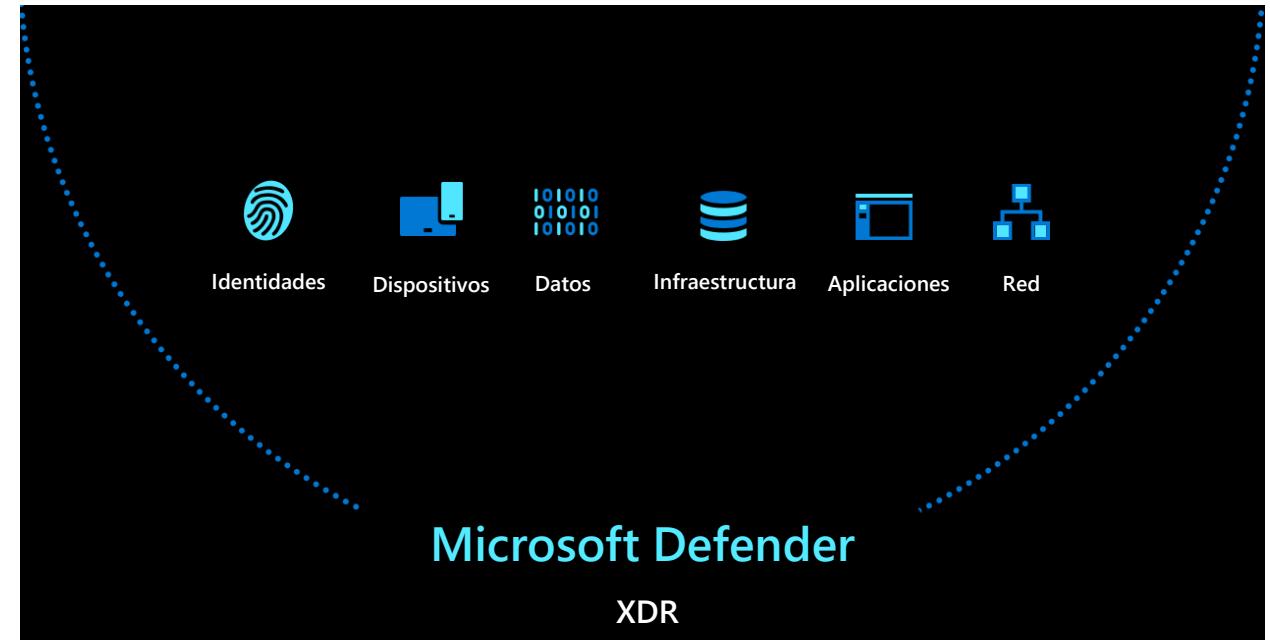
Un conjunto unificado de defensa empresarial que coordina de forma nativa la detección, prevención, investigación y respuesta en su entorno para proporcionar protección integrada contra todos los ataques sofisticados.

Defender incluye:

- Microsoft Defender para punto de conexión
- Microsoft Defender para Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Administración de vulnerabilidades de Microsoft Defender

Portal de Microsoft Defender XDR

- Ofrece una plataforma de operaciones de seguridad unificada.
- Incluye Defender XDR, Microsoft Sentinel y mucho más.



Integración con Seguridad de Microsoft Copilot:

- Habilitado a través de complementos
- Experiencia independiente e integrada

Microsoft Defender para Office 365

Integración perfecta en su suscripción de Office 365 que proporciona protección contra las amenazas que llegan por correo electrónico, vínculos, archivos adjuntos o herramientas de colaboración.

Prevenir y detectar

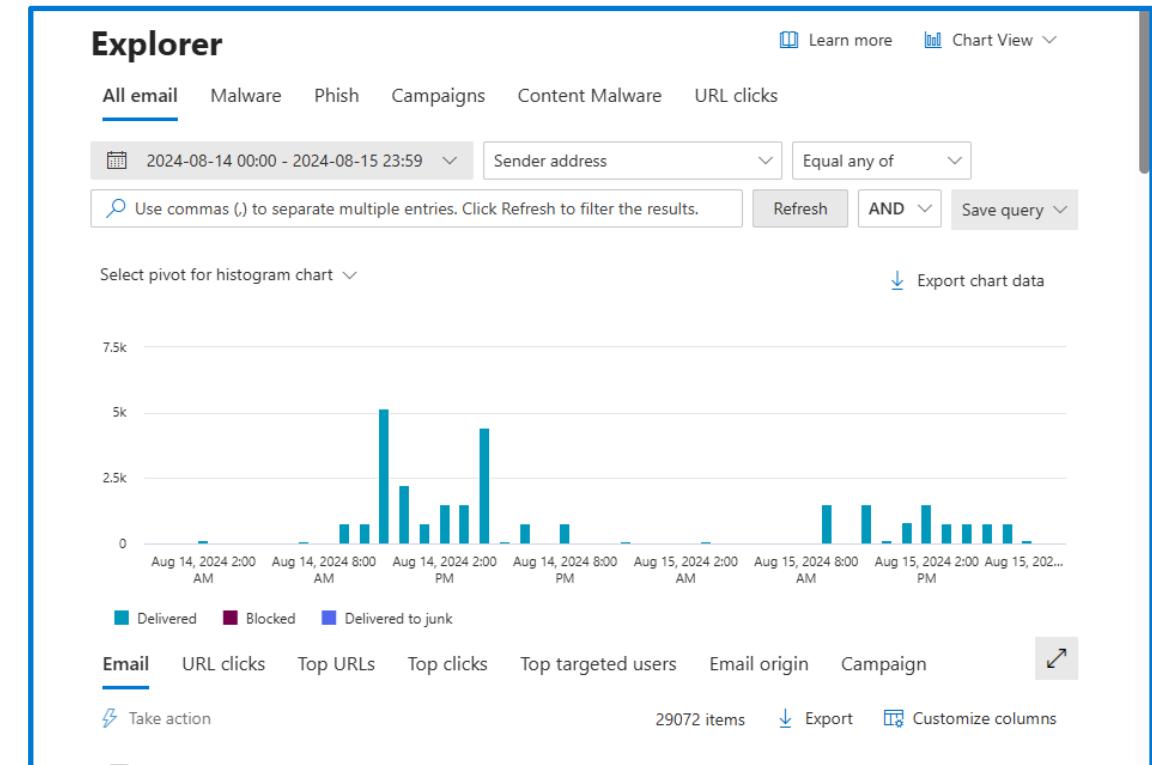
- Directivas antimalware, antispam y antiphishing
- Datos adjuntos seguros
- Capacitación de simulación de ataque
- Más...

Investigar

- Búsqueda de registro de auditoría
- Seguimiento de mensajes
- Explorer
- Más...

Responder

- Purga automática de hora cero (ZAP)
- Investigación y respuesta automatizadas
- Más...



Microsoft Defender para punto de conexión

Microsoft Defender para punto de conexión es una plataforma diseñada para ayudar a las redes empresariales a proteger los puntos de conexión.

Microsoft Defender para punto de conexión



Administración
de amenazas
y vulnerabilidades



Reducción de
la superficie
expuesta
a ataques



Protección
de última
generación



Detección
y respuesta
de puntos
de conexión



Investigación
y corrección
automatizadas



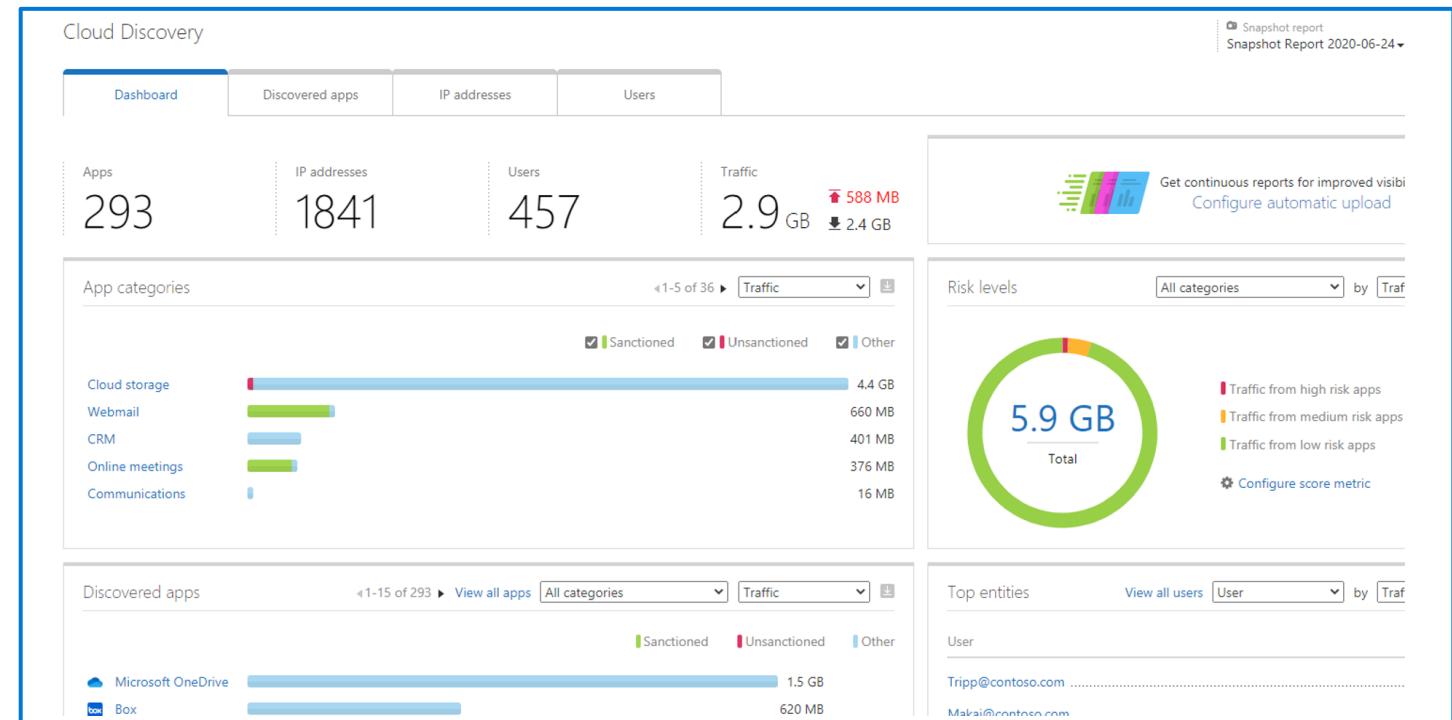
Expertos
en amenazas
de Microsoft

Configuración, administración y API centralizadas

Microsoft Defender for Cloud Apps

Proporciona visibilidad enriquecida a los servicios en la nube, control sobre el recorrido de los datos y análisis sofisticado para identificar y combatir las ciberamenazas en todos sus servicios de nube de Microsoft y de terceros.

- Detección de aplicaciones de SaaS
- Protección de la información
- Administración de la posición de seguridad de SaaS (SSPM)
- Protección contra amenazas avanzada
- Protección de aplicación a aplicación



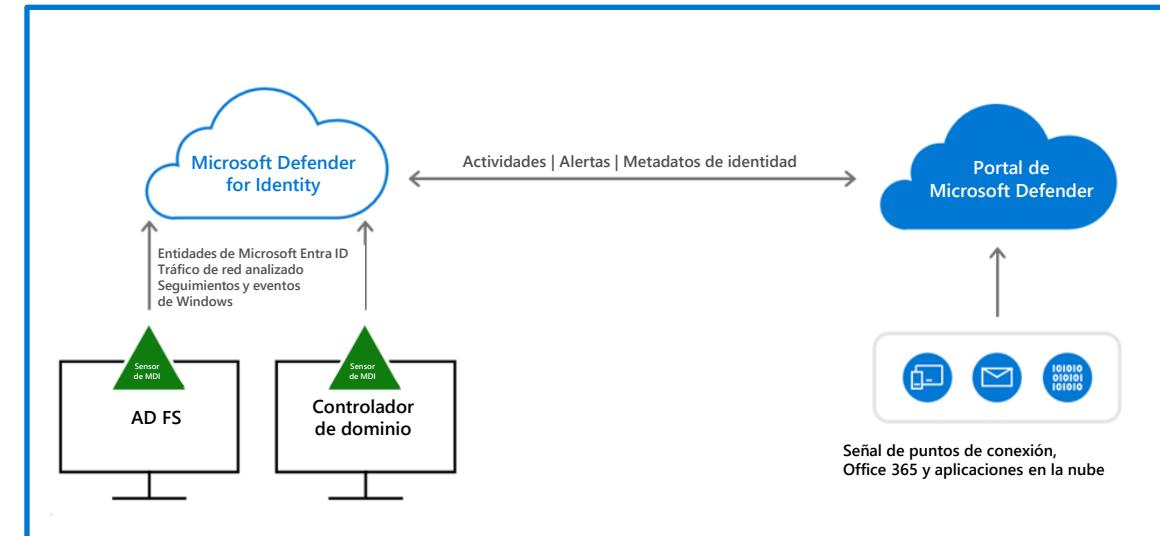
Demostración

- Microsoft Defender for Cloud Apps

Microsoft Defender for Identity

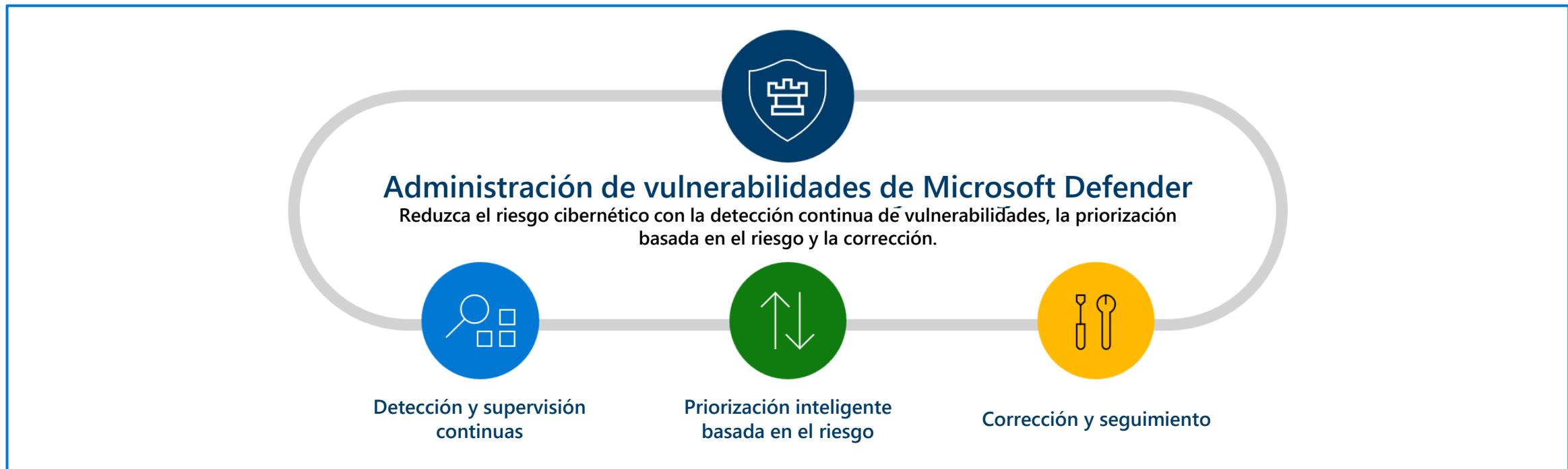
Una solución de seguridad basada en la nube que usa señales de sus servidores de infraestructura de identidades locales para detectar amenazas y elabora informes sobre problemas con identidades fáciles de vulnerar.

- Los sensores basados en software instalados en su infraestructura de identidades local envían señales al servicio de Defender for Identity.
- Defender for Identity usa señales para proporcionar detección y respuesta ante amenazas de identidad (ITDR) que permiten a los profesionales de la seguridad lo siguiente:
 - Evaluar proactivamente su postura de identidad
 - Detectar amenazas usando análisis en tiempo real e inteligencia de datos
 - Investigue las alertas y las actividades del usuario
 - Acciones de corrección
- El portal de Microsoft Defender les proporciona a los equipos de seguridad una plataforma unificada de operaciones de seguridad para investigar y responder a los ataques.



Administración de vulnerabilidades de Microsoft Defender

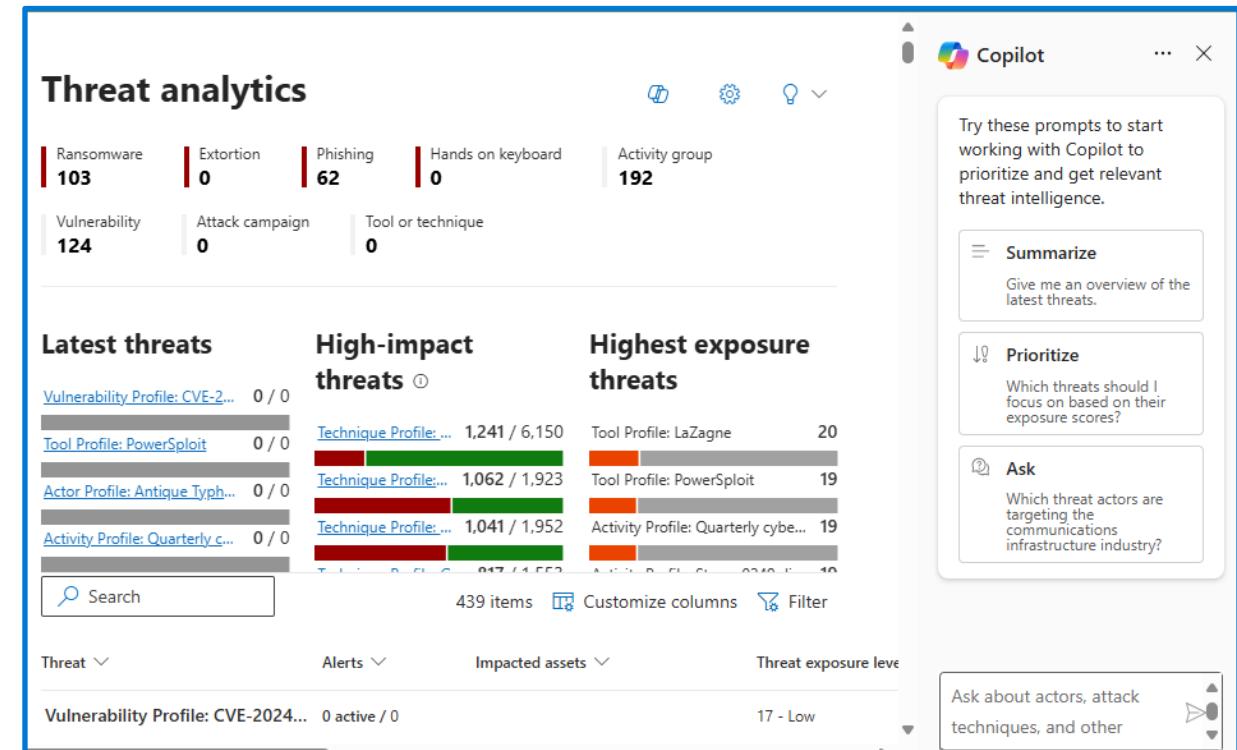
Ofrece visibilidad de activos, evaluaciones inteligentes y herramientas de corrección integradas para Windows, macOS, Linux, Android, iOS y dispositivos de red.



Inteligencia sobre amenazas de Microsoft Defender

Agrupa y enriquece orígenes de datos de inteligencia crítica sobre amenazas y se integra con Seguridad de Microsoft Copilot para ayudar al analista de seguridad mientras clasifica, investiga y corrige las vulnerabilidades.

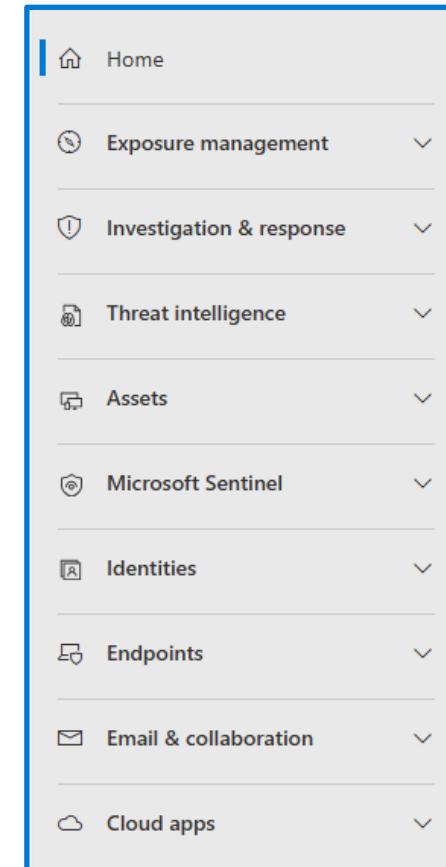
- Análisis de amenazas: Permite entender cómo las amenazas emergentes afectan el entorno de su organización.
- Perfiles de inteligencia: Es una fuente definitiva de conocimiento de Microsoft que se puede compartir sobre actores de amenazas rastreados, herramientas maliciosas y vulnerabilidades.
- Explorador de inteligencia: Es donde los analistas pueden analizar rápidamente nuevos artículos destacados y realizar búsquedas para recopilar inteligencia.
- Proyectos de inteligencia: Los usuarios pueden crear proyectos que organicen indicadores de ataque (IOC) a partir de una investigación y contengan artefactos asociados y un historial detallado.



Portal de Microsoft Defender

El portal de Microsoft Defender ofrece una plataforma de operaciones de seguridad unificada.

- Lo mejor de SIEM, XDR, la administración de la postura y la inteligencia sobre amenazas con IA generativa avanzada como una sola plataforma.
- Combina protección, detección, investigación y respuesta a amenazas en toda la organización y todos sus componentes, en un solo lugar.



Integración de Copilot con Microsoft Defender XDR

La integración con Copilot se experimenta a través de las experiencias independiente e integrada.

Experiencia independiente:

- Habilite complementos para admitir la integración con Microsoft Defender XDR.
- Las capacidades del sistema actúan como consultas integradas.
- Use el libro de consultas integrado para investigación de incidentes de Defender o cree el suyo propio.

Manage sources

Plugins

Microsoft Defender XDR
Alerts and incidents

Files

Natural language to KQL for Microsoft Defender XDR
Query-generating capability (for Defender)

SYSTEM CAPABILITIES

MICROSOFT DEFENDER XDR

Analyze a file
Inspect a file using available information, including API calls, certificates...

Generate an identity summary
Get identity insights, security concerns and potential anomalies

Generate an incident report
Get a report about an attack and your response, including who took act...

Generate guided response
Get step-by-step response recommendations for an incident.

List incidents and related alerts
Get the list of incidents or find specific incidents.

How can Copilot for Security help?

Integración de Copilot con Microsoft Defender XDR (continuación)

La integración con Copilot se experimenta a través de las experiencia independiente e integrada.

Experiencia integrada:

- Resumen de incidentes
- Respuestas guiadas
- Análisis de scripts
- Lenguaje natural para consulta de KQL
- Informes de incidentes
- Análisis de archivos
- Resumen de dispositivos e identidades

The screenshot shows the Microsoft Defender XDR interface with a Copilot sidebar. The main pane displays an incident summary for a high-severity "Plaid Rain" activity involving execution and lateral movement on one endpoint. The sidebar on the right provides a detailed "Incident summary" and a "Guided response".

Incident summary
Sep 10, 2024 4:16 PM
The high severity incident "Plaid Rain activity with multi-stage incident involving Execution & Lateral movement on one endpoint reported by multiple sources" occurred between 2024-04-11 09:54:44 UTC and 2024-04-11 13:34:44 UTC. The incident was attributed to the threat actor PLAID RAIN. This incident

Guided response
Sep 10, 2024 5:02 PM
Completed recommendations 0/4
Status: All

Demostración

- El portal de Microsoft Defender XDR



Describir las capacidades de Microsoft
Priva y Microsoft Purview

Objetivos de aprendizaje

- Describir el Portal de confianza de servicios y las capacidades de privacidad de Microsoft Priva.
- Describir las soluciones de seguridad de datos de Microsoft Purview.
- Describir las soluciones de cumplimiento de datos de Microsoft Purview.
- Describir las soluciones de gobernanza de datos de Microsoft Purview.

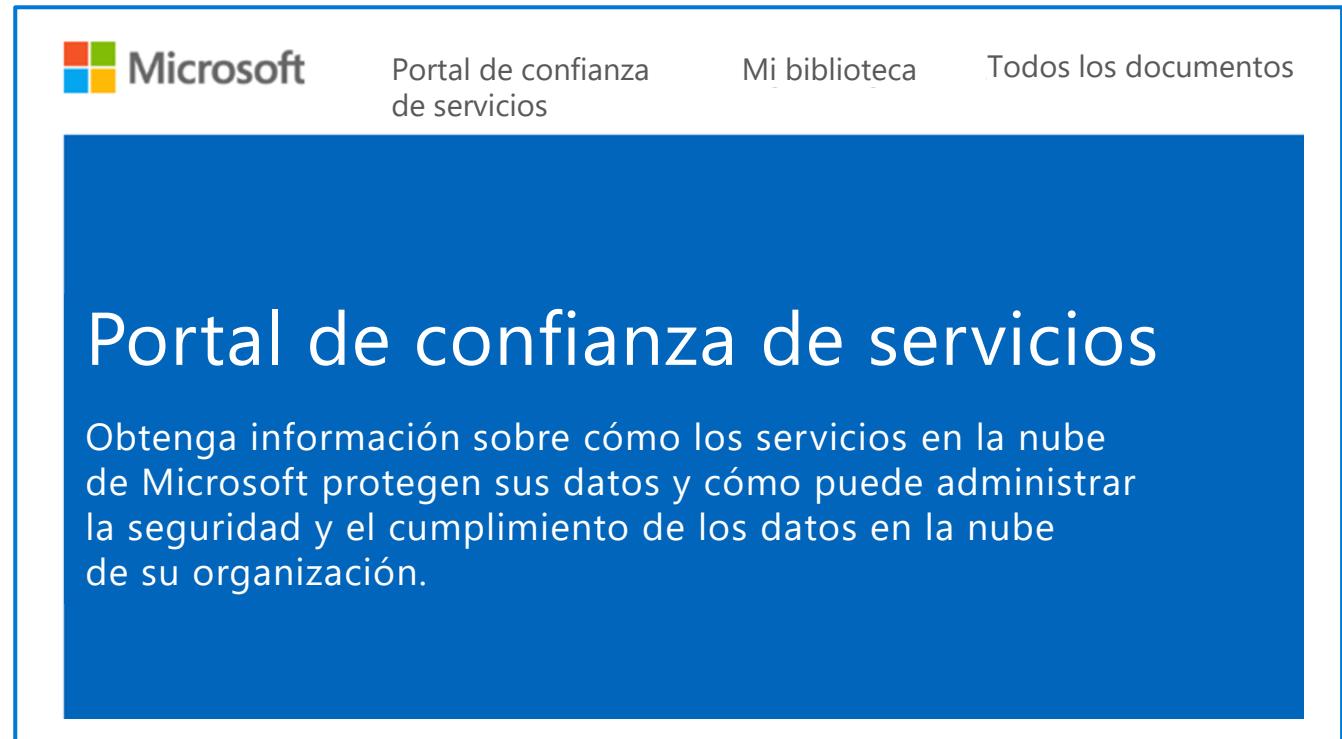


Objetivo de aprendizaje: Describir el Portal de confianza de servicios y las capacidades de privacidad de Microsoft Priva.

Portal de confianza de servicios de Microsoft

Sitio de Microsoft para publicar informes de auditoría y otra información relacionada con el cumplimiento asociada con los servicios en la nube de Microsoft.

- Certificaciones, reglamentos y estándares
- Informes, documentos técnicos y artefactos
- Recursos regionales y de la industria
- Recursos para su organización



Demostración

- Portal de confianza de servicios

Principios de privacidad de Microsoft

-  Control: le daremos a usted, el cliente, el control de sus datos y su privacidad con herramientas fáciles de utilizar y opciones claras.
-  Transparency: seremos transparentes con respecto a la recopilación y el uso de datos para que todos puedan tomar decisiones informadas.
-  Seguridad: protección de los datos que se confían a Microsoft con seguridad y cifrado sólidos.
-  Firmes protecciones legales: respeto de las leyes de privacidad locales y lucha por la protección legal de la privacidad como un derecho humano fundamental.
-  Sin segmentación basada en contenido: no utilizaremos su correo electrónico, chat, archivos u otro contenido personal para enviarle anuncios.
-  Beneficios para usted: cuando Microsoft recopila datos, estos se usan para beneficiarlo a usted, el cliente, y para mejorar sus experiencias.

Microsoft Priva

Ayuda a las organizaciones a proteger sus datos personales y crear un lugar de trabajo resiliente a la privacidad.

Administración de riesgos de privacidad:

Visibilidad de los datos de su organización y plantillas de directivas para reducir riesgos.

Solicitudes de derechos de los interesados:

Herramientas de automatización y flujo de trabajo para cumplir con las solicitudes de datos.

Administración de consentimiento: Realice un seguimiento eficaz del consentimiento del consumidor en todo su patrimonio de datos.

Análisis de rastreadores: Automatice la identificación de tecnologías de seguimiento en múltiples propiedades web, impulsando el cumplimiento de la privacidad del sitio web.

Evaluaciones de privacidad: Automatice la detección, documentación y evaluación del uso de datos personales en todo su panorama de datos.



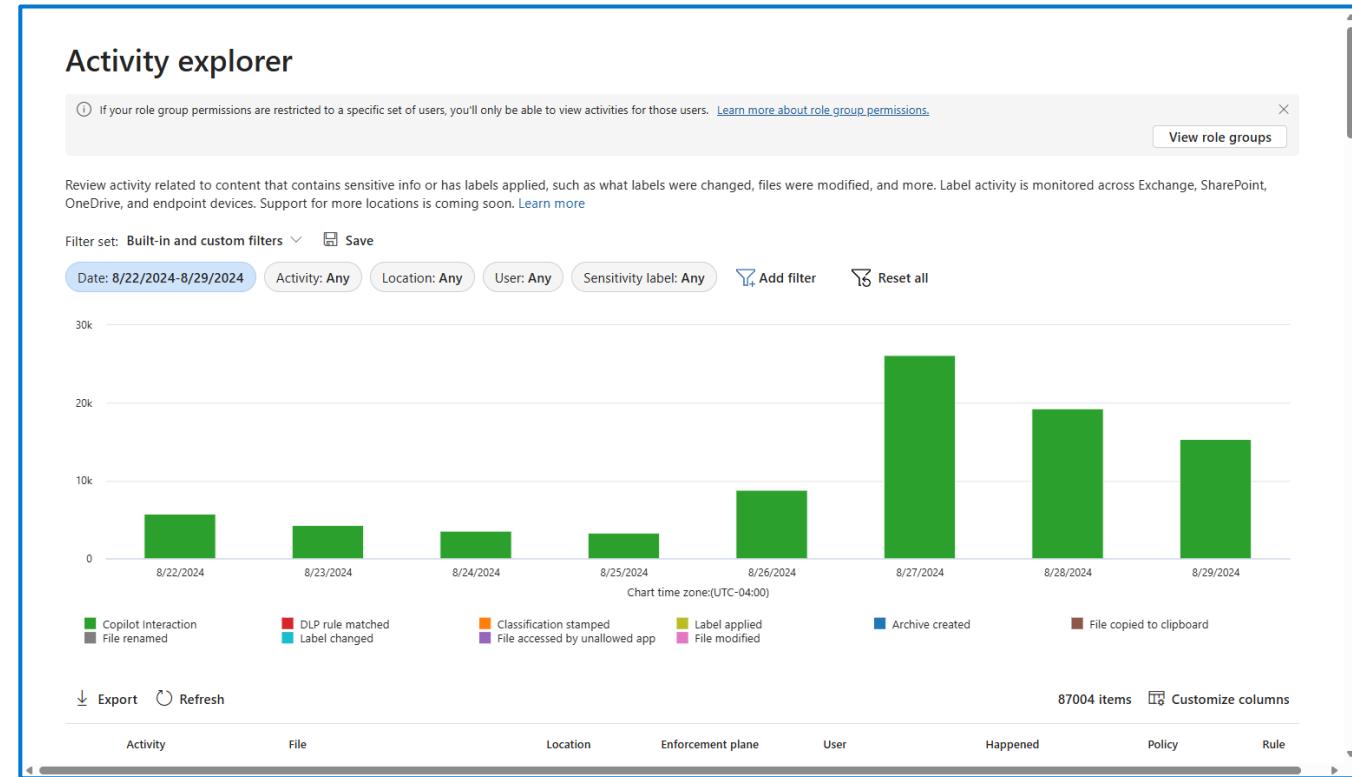


Objetivo de aprendizaje: Describir las soluciones de seguridad de datos de Microsoft Purview

Clasificación de datos en la Protección de la información de Microsoft Purview

Identifique la información importante en su patrimonio y asegúrese de que los datos se manejen de acuerdo con los requisitos de cumplimiento.

- Tipos de información confidencial
- Clasificadores de coincidencia exacta de los datos (EDM)
- Clasificadores entrenables: Clasificadores preentrenados y clasificadores entrenables personalizados.
- Explorador de contenido: Una instantánea de los elementos con una etiqueta de confidencialidad, una etiqueta de retención o que se han clasificado como un tipo de información confidencial
- Explorador de actividades: Supervise lo que se está haciendo con el contenido etiquetado en toda la organización



Directivas y etiquetas de confidencialidad

Las etiquetas de confidencialidad son:

- Personalizables
- Texto sin formato
- Persistentes

Las etiquetas de confidencialidad pueden:

- Cifrar
- Marcar el contenido (marca de agua)
- Aplicar automáticamente etiquetas
- Proteger el contenido en contenedores
- Extenderse a aplicaciones/servicios de terceros
- Clasificar contenido sin protección

Directivas de etiquetas

- Elija los usuarios y grupos que pueden ver las etiquetas.
- Aplique una etiqueta predeterminada a todos los correos electrónicos y documentos nuevos.
- Exija justificaciones para los cambios de etiqueta.
- Exija a los usuarios que apliquen una etiqueta (etiquetado obligatorio).
- Vincule a los usuarios a páginas de ayuda personalizadas.

Confidential - Finance

Name
Confidential - Finance

Display name
Confidential - Finance

Description for users
This file was automatically labeled because it contains confidential data.

Description
Documents with this label contain sensitive data.

Scope
File, Email

Encryption
Encryption

Content marking
Watermark: CONFIDENTIAL FINANCIAL DATA

Auto-labeling for files and emails
Automatically apply the label

Auto-labeling for schematized data assets (preview)
None

Demostración

- Etiquetas de confidencialidad

Prevención de pérdida de datos (DLP) de Microsoft Purview

Identifique, supervise y proteja los elementos confidenciales en:

- Servicios de Microsoft 365: OneDrive for Business, SharePoint Online, Exchange Online y aplicaciones de Office 365.
- Microsoft Teams: Mensajes de chat y canales de Teams.
- Dispositivos: Windows 10, Windows 11 y macOS.
- Microsoft Defender for Cloud Apps.
- Repositorios locales.
- Power BI.

Las medidas de protección que pueden tomar las directivas de DLP son:

- Mostrar una sugerencia de directiva emergente.
- Bloquear el uso compartido de elementos confidenciales con o sin opción de anulación.
- Trasladar datos en reposo a una ubicación de cuarentena segura.
- Para el chat de Teams, no se mostrará la información confidencial.

Integración de Seguridad de Copilot:

- Experimente la integración con Copilot a través de la experiencia independiente e integrada.
- La experiencia integrada admite el resumen de alertas.

Your message was blocked because it contains sensitive data

- U.S. Social Security Number (SSN)
- International Classification of Diseases (ICD-10-CM)
- International Classification of Diseases (ICD-9-CM)

This item is protected by a policy in your organization.

Here's what you can do

Override the policy and send the message, or report this to your admin if you think the message was blocked in error.

Override and send.

Type your justification

Report this to my admin. It doesn't contain sensitive data.

Cancel

Confirm

Gestión de riesgos internos de Microsoft Purview

Ayuda a las organizaciones a identificar, investigar y abordar los riesgos internos, como filtraciones de datos, robo de propiedad intelectual, fraude, uso de información privilegiada y más.

Flujo de trabajo de la gestión de riesgos internos

- Cree **directivas** para definir qué indicadores de riesgo se examinan.
- Las **alertas** se generan automáticamente mediante indicadores de riesgo que coinciden con las condiciones de la directiva.
- **Clasifique** las alertas con el estado "necesita revisión".
- Los casos se crean para alertas que requieren una revisión e **investigación** más profundas.
- Los revisores pueden tomar **medidas** rápidamente para resolver el caso.



Integración con Seguridad de Copilot

- Integración a través de la experiencia independiente e integrada.
- La experiencia integrada admite el resumen de alertas.

Protección adaptable en Microsoft Purview

La Protección adaptable de Microsoft Purview usa machine learning (ML) para identificar los riesgos más críticos y aplicar controles de protección de forma proactiva y dinámica.

Según los niveles de riesgo en la Gestión de riesgos internos, la Protección adaptable de Microsoft Purview aplica controles de:

- Prevención de pérdida de datos
- Administración del ciclo de vida de los datos de Microsoft Purview (versión preliminar)
- Acceso condicional de Microsoft Entra (versión preliminar)

Mitigue los riesgos potenciales usando:

- Detección contextual
- Controles dinámicos
- Mitigación automatizada





**Objetivo de aprendizaje: Describir las soluciones
de cumplimiento de datos de Microsoft Purview**

Auditorías de Microsoft Purview

Ayude a las organizaciones a responder eficazmente a los eventos de seguridad, las investigaciones forenses, las investigaciones internas y las obligaciones de cumplimiento.

Auditoría (estándar)



- Registro y búsqueda de actividades auditadas:
- Habilitado de forma predeterminada
 - Miles de eventos de auditoría donde se pueden llevar a cabo búsquedas
 - Período de retención predeterminado de 90 días
 - Acceso mediante GUI, cmdlet y API

Auditoría (premium)

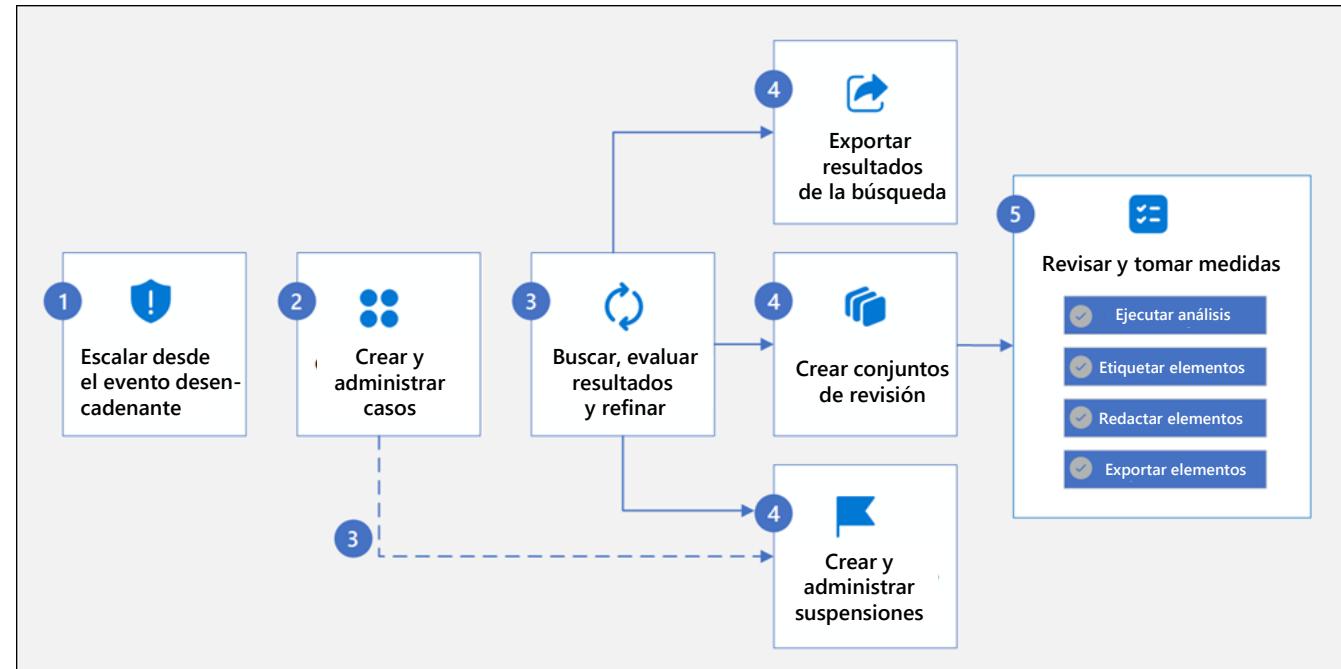


- Mejora las capacidades de Auditoría (estándar) con:
- Período de retención predeterminado de 1 año
 - Directivas de retención personalizadas
 - Información inteligente
 - Mayor acceso de ancho de banda a API

eDiscovery de Microsoft Purview

Es el proceso de identificar y entregar información electrónica que se puede usar como prueba en casos judiciales.

1. Los eventos desencadenantes inician la creación de un nuevo caso en eDiscovery (versión preliminar).
2. Cree y administre casos.
3. Busque las ubicaciones de contenido de su organización con las herramientas de búsqueda integradas.
4. Algunas acciones son:
 - Exportación de resultados de búsqueda
 - Creación de grupos de revisión
 - Creación de suspensiones
5. Revise y tome medidas en los conjuntos de revisión.
 - Ejecute análisis
 - Etiquete elementos
 - Exporte elementos



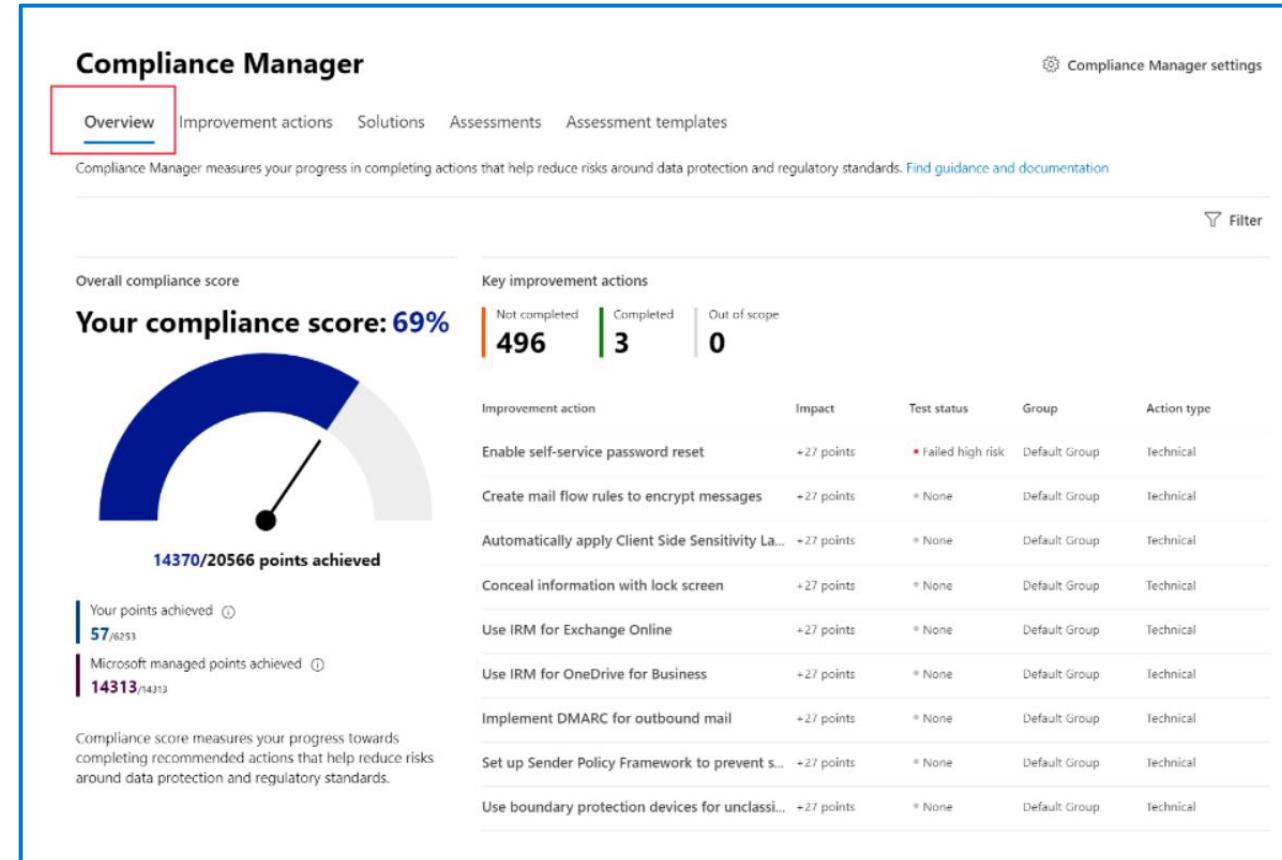
Administrador de cumplimiento

El Administrador de cumplimiento simplifica el cumplimiento y reduce el riesgo al proporcionar lo siguiente:

- Evaluaciones precompiladas basadas en estándares comunes
- Capacidades de flujo de trabajo para completar las evaluaciones de riesgos
- Acciones de mejora paso a paso
- Puntuación de cumplimiento, que muestra la postura general de cumplimiento

Elementos claves del Administrador de cumplimiento

- Controles
- Evaluaciones
- Normativas
- Acciones de mejora



Demostración

- Administrador de cumplimiento

Cumplimiento de las comunicaciones de Microsoft Purview

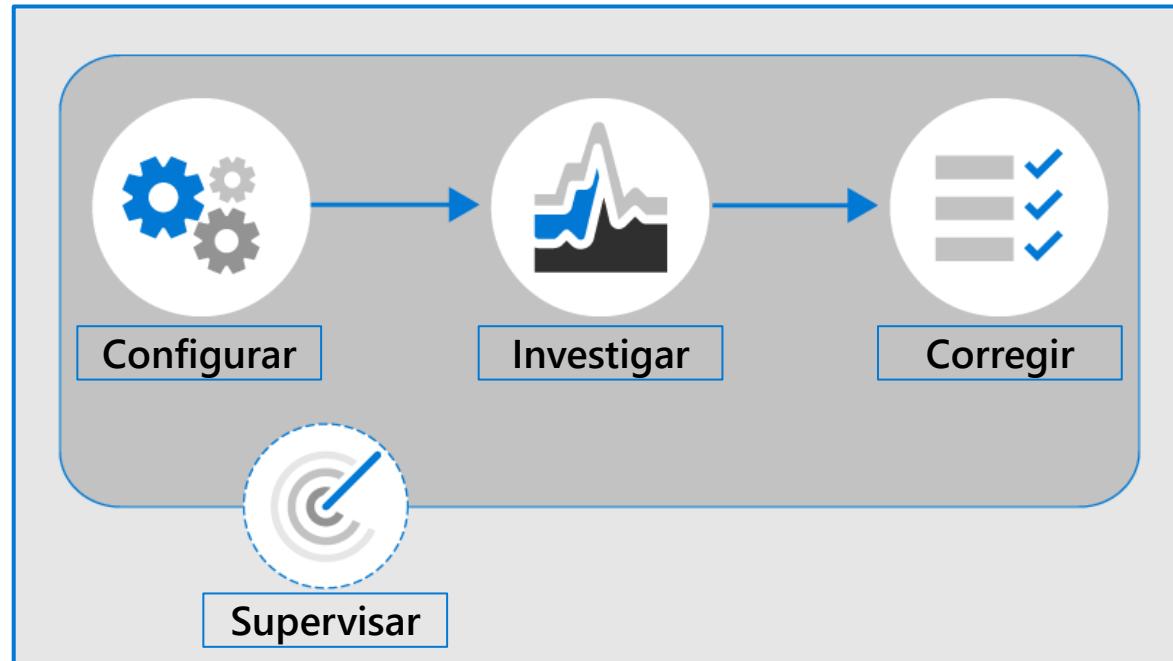
Detecte, capte y tome medidas sobre los mensajes inadecuados que pueden conducir a posibles incidentes de seguridad o cumplimiento de datos dentro de su organización.

Las directivas del Cumplimiento de las comunicaciones ayudan con lo siguiente:

- Directivas corporativas: Analice los mensajes para detectar inquietudes con respecto al lenguaje ofensivo o el acoso.
- Administración de riesgos: Analice la comunicación no autorizada sobre proyectos confidenciales.
- Cumplimiento normativo: Protéjase contra posibles operaciones con información privilegiada, lavado de dinero, etc.

Flujo de trabajo:

- Configurar directivas
- Investigar problemas
- Corregir problemas
- Supervisar continuamente



Integrado con Seguridad de Microsoft Copilot

Administración del ciclo de vida de los datos con directivas y etiquetas de retención

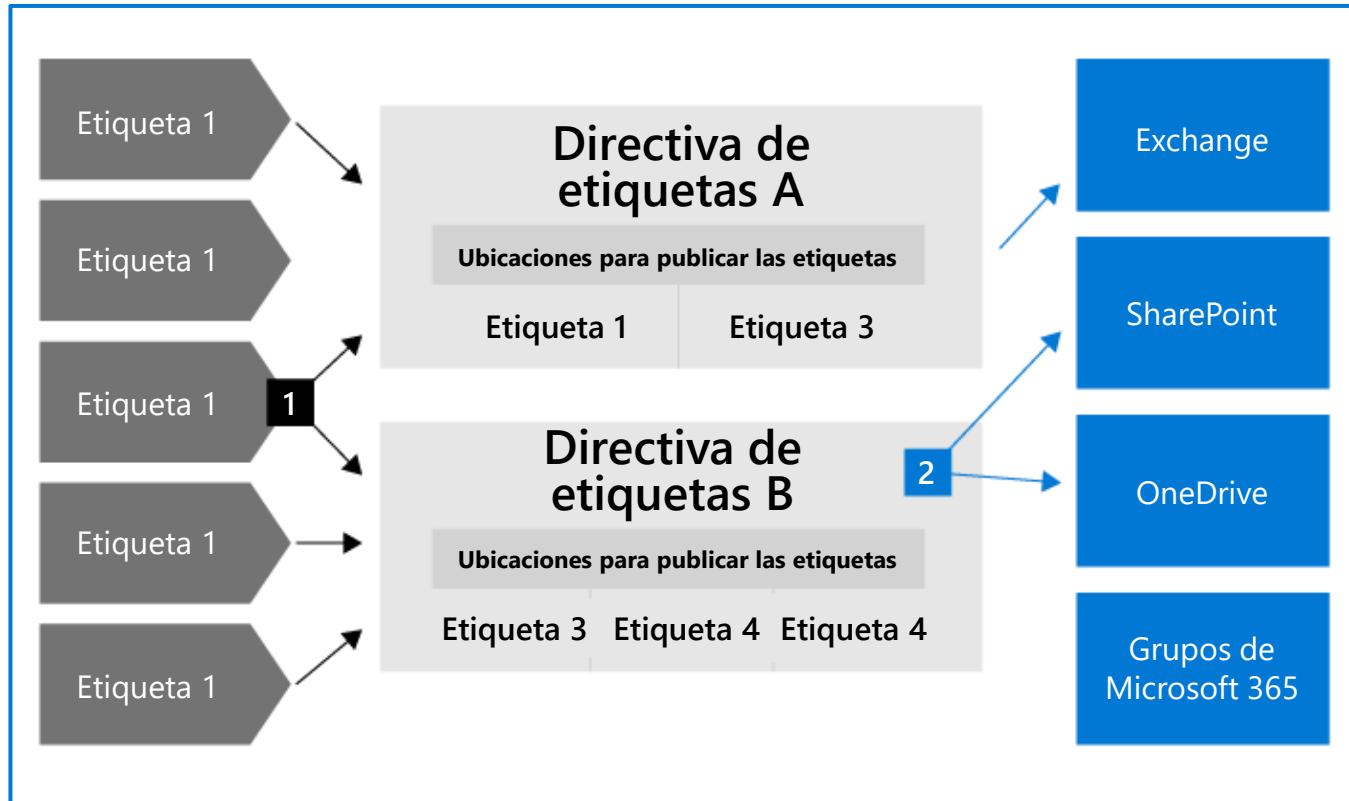
Administre y gobierne la información asegurándose de que el contenido se conserve solo durante el tiempo necesario.

Etiquetas de retención:

- Asignada en el nivel del elemento.
- Solo puede asignar una etiqueta a la vez.
- La configuración de retención viaja con el contenido.
- Se puede aplicar de forma automática.
- Admite una revisión de eliminación.
- Se publica a través de directivas de etiquetas.

Directivas de retención:

- Se asignan en el nivel del sitio o buzón.
- Se puede aplicar una sola directiva a varias ubicaciones o a ubicaciones o usuarios específicos.
- Los elementos heredan la configuración de retención de su contenedor.



Administración de registros de Microsoft Purview

Ayuda a las organizaciones a ocuparse de sus obligaciones legales y a demostrar el cumplimiento de las normativas.

- Para el contenido que se etiquetó como registro:
 - Se establecen restricciones para bloquear ciertas actividades.
 - Se registran las actividades.
 - La prueba de eliminación se conserva al final del período de retención.
- Para que los elementos se marquen como registros, un administrador debe configurar las etiquetas de retención.

During the retention period

Retain items even if users delete

Mark items as a record

Users won't be able to edit or delete emails, and only certain users will be able to change or remove the label. They won't be able to delete SharePoint or OneDrive files, but other actions are blocked or allowed based on whether the item's record status is locked or unlocked. [Learn more](#)

Mark items as a regulatory record

At the end of the retention period

Delete items automatically

We'll delete items from where they're currently stored.



**Objetivo de aprendizaje: Describir las soluciones
de gobernanza de datos de Microsoft Purview**

Beneficios de la gobernanza de datos

Para los consumidores de datos de toda la organización:

- Detección de datos: le ayuda a encontrar fácilmente los datos que necesita.
- Acceso seguro: facilita el acceso seguro a sus datos.
- Comprensión de los datos: proporciona lo que necesita saber sobre los datos.

Para los propietarios y administradores de datos:

- Selección y administración de datos: ayuda a entregar datos de alta calidad que son fáciles de entender y con acceso seguro para aplicaciones en toda la organización.
- Uso responsable de datos: ayuda a garantizar que sus datos los usen los usuarios previstos para los fines previstos.
- Análisis de impacto: comprenda las acciones sobre los datos que pueden afectar a sus datos.

Para directores de datos y partes interesadas de la directiva:

- Creación de valor de datos: maximice la creación de valor a partir de sus datos mientras reduce el gasto en operaciones.
- Estandarización de los recursos de datos: cree controles comunes en todos su patrimonio de datos con responsabilidad federada para que sus datos estén en buen estado y seguros.



Consumidores de datos

Encuentre y use rápidamente conjuntos de datos pertinentes y confiables a través de un flujo de trabajo de solicitud de acceso optimizado.



Propietarios de datos

Registre los activos de datos para su uso, administre las clasificaciones y el acceso y garantice estándares de alta calidad.



Administradores de datos

Garantice la calidad de los datos, detección de datos sin problemas, coherencia del glosario y linaje de los datos.



Oficina central de datos

Establezca y garantice directivas de gobernanza, metadatos activos, cumplimiento e información sobre el estado general de la gobernanza.

Catálogo de datos de Microsoft Purview

El objetivo del Catálogo de datos de Microsoft Purview es proporcionar una plataforma para la gobernanza de datos e impulsar la creación de valor empresarial en su organización.

- Organice los datos con **dominios empresariales** (ventas, finanzas, etc.) que permiten que los datos sean familiares y accesibles, y establezca objetivos y resultados clave (OKR) para vincular los objetivos empresariales con el catálogo de datos.
- Agrupe los activos relacionados en **productos de datos** para que los usuarios puedan encontrar fácilmente la imagen completa de los datos.
- Defina **elementos de datos críticos** y asocie reglas y directivas que colaboren con el **acceso a datos de autoservicio**, garantizando que los usuarios tengan acceso a los datos correctos.
- Habilite la **detección de datos** en toda la empresa con capacidades de búsqueda y exploración, con las eficiencias adicionales que ofrece Copilot en Purview para una interacción simple y rápida.