Microsoft Security

Módulo 3 de SC-900T00-A: Describir las funcionalidades de las soluciones de seguridad de Microsoft

Lección 1: Describir las funcionalidades de seguridad básicas en Azure

Lección 1: Introducción

Al finalizar esta lección, podrá hacer lo siguiente:

Describir las funcionalidades de seguridad de Azure para proteger su red

Describir cómo Azure puede proteger sus máquinas virtuales

Describir cómo el cifrado en Azure puede proteger sus datos

DDoS

Distributed Denial of Service (DDoS)

Millones de dispositivos (computadores, dispositivos IoT, etc.) generan y envían -al mismo tiempo- solicitudes hacia un servidor. La sobrecarga lleva a que el servidor eventualmente se quede sin recursos para atender los pedidos.

"On October 21, 2016, the largest distributed denial of service (DDoS) attack took place, shutting down most of the Internet, including Twitter, Amazon, GitHub, and the New York Times.[1] The attack targeted Dyn, a company that services a large share of the internet's domain name system (DNS) infrastructure, and lasted for most of the day. The type of malware used for the attack, which leveraged IoT devices rather than computers, resulted in an extraordinarily malicious attack, "roughly twice as powerful as any similar attack on record."[2]
[…]
The perpetrators were able to access these IoT devices by hacking into them. Most of the IoT devices used for the Mirai botnet were running on default credentials. In fact, after the attack, the Mirai source code was posted online and included default credentials for more than 60 devices.[4]"

https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/

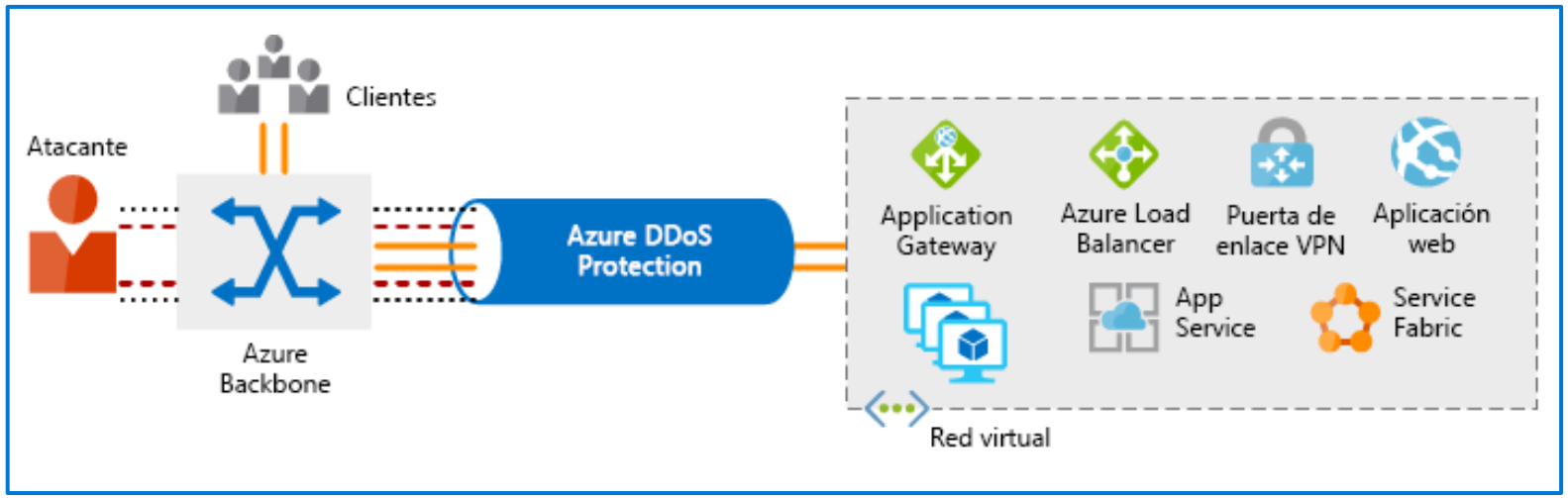
Azure DDoS Protection

Un ataque de denegación de servicio distribuido (DDoS) hace que los recursos no respondan.

Azure DDoS Protection analiza el tráfico de red y descarta cualquier cosa que parezca un ataque DDoS.

Niveles de Azure DDoS Protection:

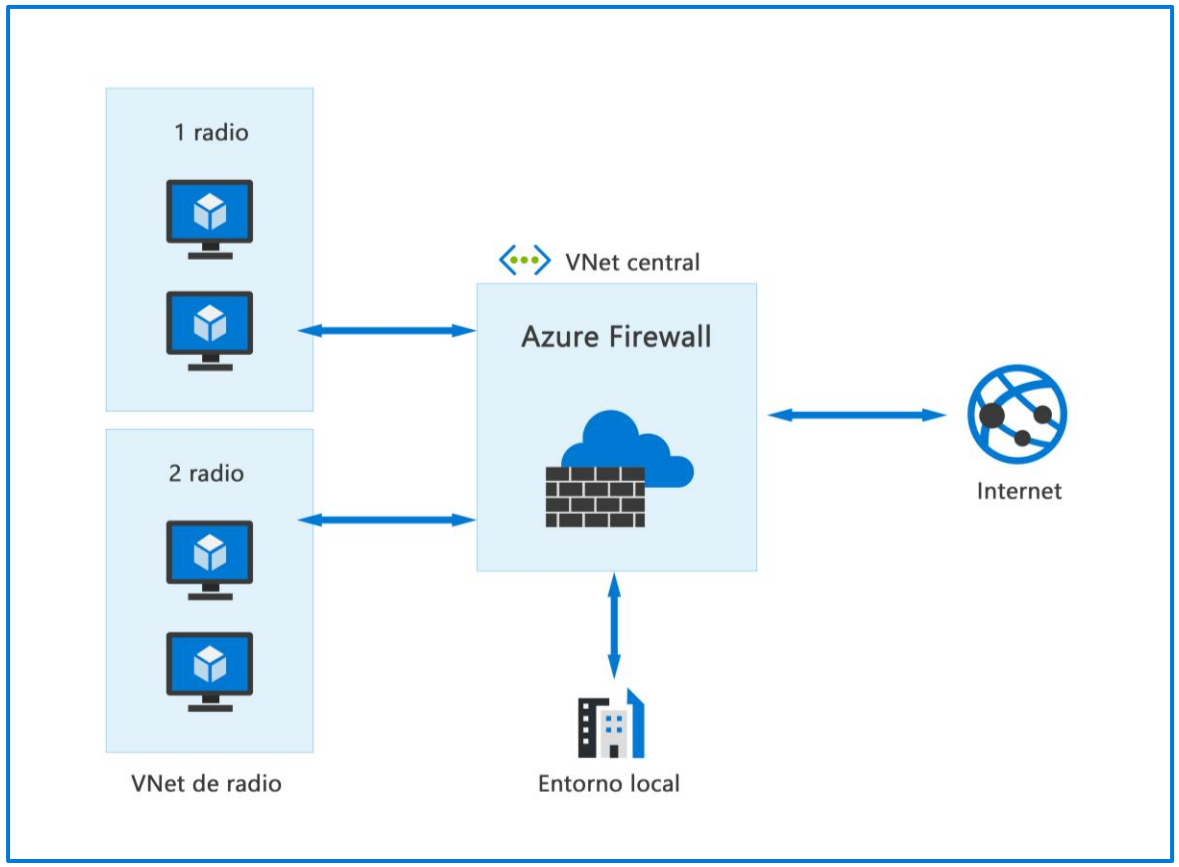
- Básico
- Estándar



Azure Firewall

Azure Firewall protege sus recursos de Azure Virtual Network (VNet o red virtual) de los atacantes. Las características incluyen las siguientes:

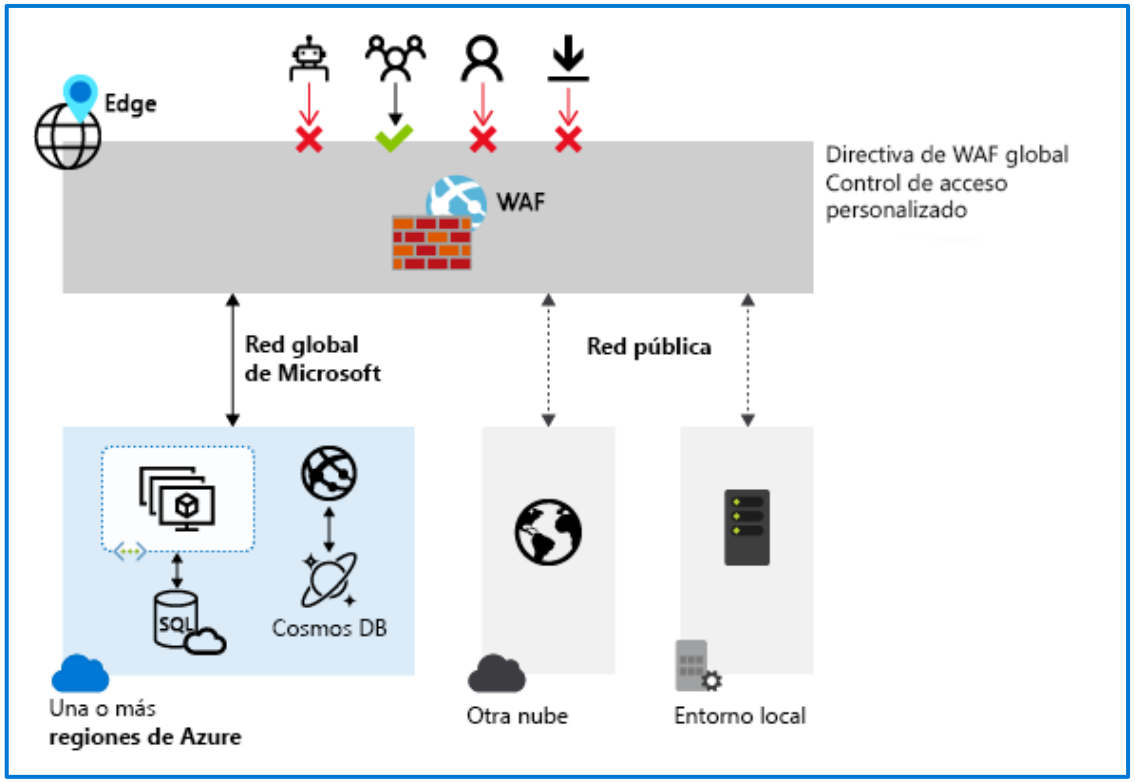
- Zonas de disponibilidad y alta disponibilidad integradas
- SNAT de salida y DNAT de entrada
- Inteligencia sobre amenazas
- Filtrado a nivel de red y de aplicación
- Varias direcciones IP públicas
- Integración con Azure Monitor



Firewall de aplicaciones web

El firewall de aplicaciones web (WAF) ofrece una protección centralizada de las aplicaciones web contra las vulnerabilidades de seguridad más habituales.

- Administración de seguridad más sencilla
- Mejora del tiempo de respuesta ante una amenaza de seguridad
- Revisión de una vulnerabilidad conocida en un lugar
- Protección frente a amenazas e intrusiones.



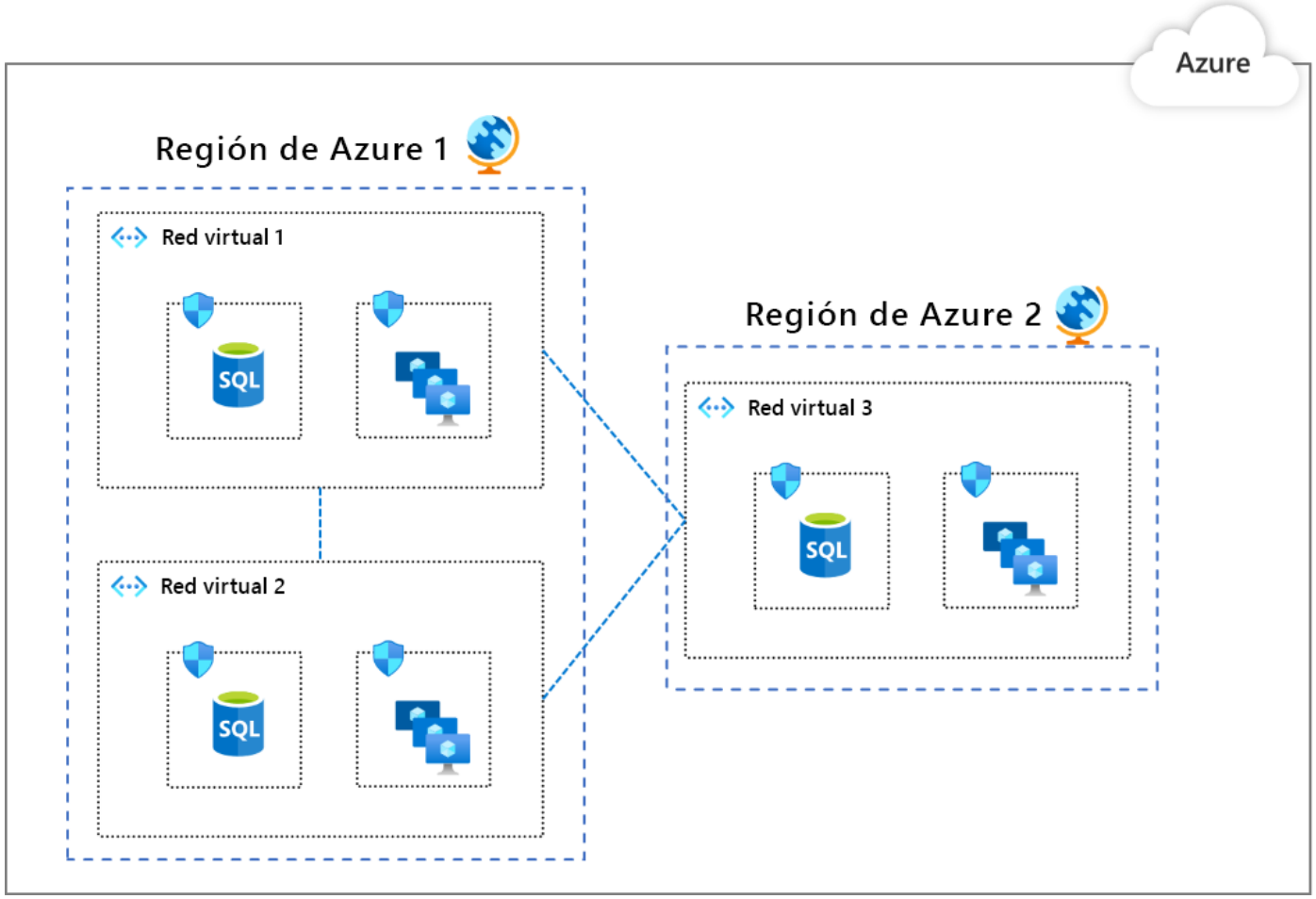
Segmentación de la red y Azure VNet

Razones para la segmentación de la red:

- La capacidad de agrupar activos relacionados
- El aislamiento de recursos.
- Las directivas de gobernanza establecidas por la organización.

Azure Virtual Network (VNet):

- Contención a nivel de red de los recursos sin que se permita el tráfico a través de VNets o de entrada a VNet.
- La comunicación tiene que estar aprovisionada explícitamente
- Controlar cómo se comunican los recursos de una VNet con otros recursos, con Internet y con las redes locales

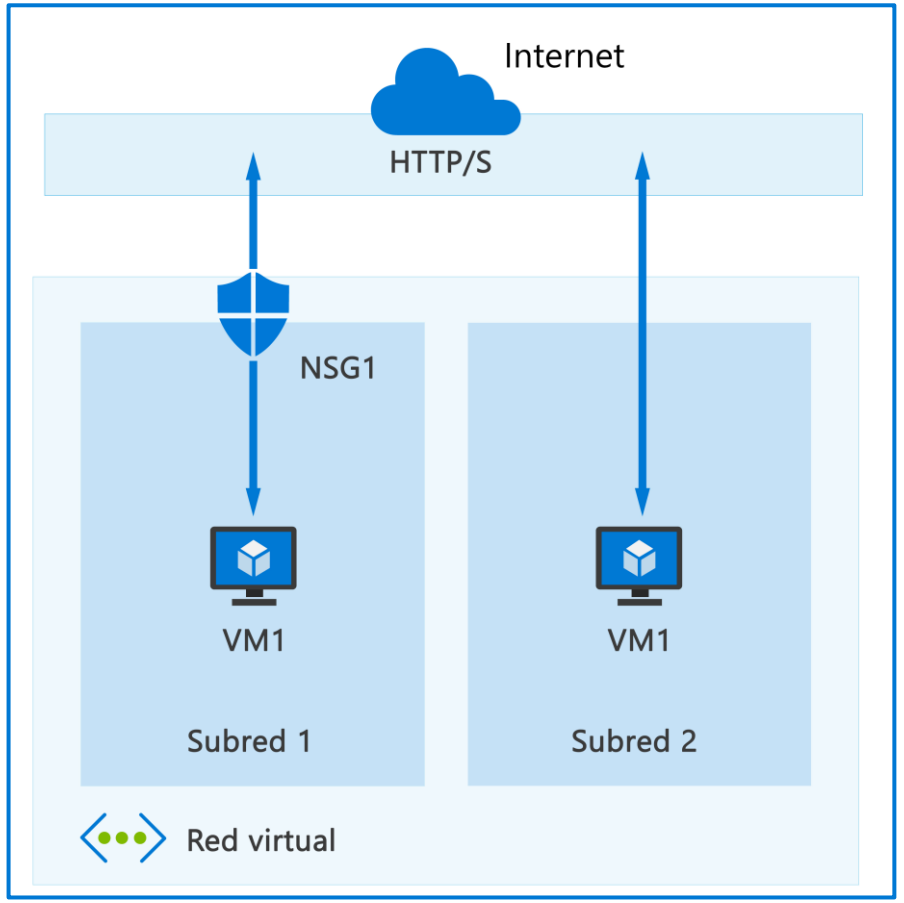


Grupos de seguridad de red de Azure

Un grupo de seguridad de red (NSG) le permite admitir o no el tráfico de red con los recursos de Azure que existen en Azure Virtual Network.

- Un NSG se puede asociar con varias interfaces de red o subredes en una red virtual.
- Un NSG se compone de reglas de seguridad de entrada y salida.
- Cada regla especifica una o varias de las siguientes propiedades:
  - Nombre
  - Prioridad
  - Origen o destino
  - Protocolo
  - Dirección
  - Intervalo de puertos
  - Acción
- Ejemplo de regla de entrada predeterminado con la etiqueta "DenyAllInbound"

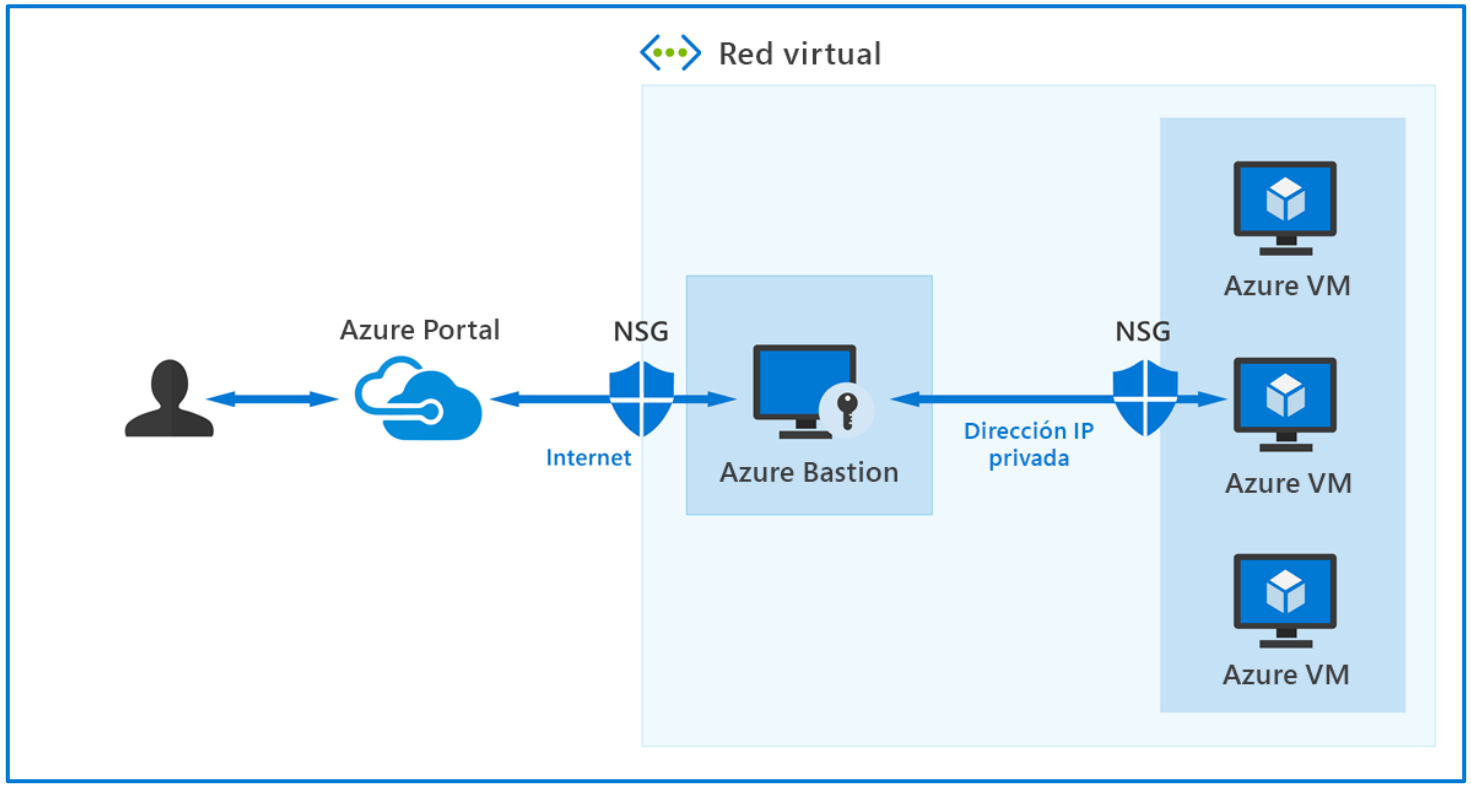
Prioridad	Origen	Puertos de origen	Destino	Puertos de destino	Protocolo	Acceso
6500	0.0.0.0 /0	0-65535	0.0.0.0/0	0-65535	Cualquiera	Cualquiera



Protección del acceso remoto a máquinas virtuales: Azure Bastion y acceso Just-In-Time

Azure Bastion: conectividad segura a sus máquinas virtuales desde el Azure Portal.

Acceso Just-In-Time: acceso seguro cuando se necesita.



Formas en que Azure cifra los datos y uso de Key Vault

Cifrado en Azure

Cifrado del servicio Azure Storage

Azure Disk Encryption

Cifrado de datos transparente (TDE)

¿Qué es Azure Key Vault?

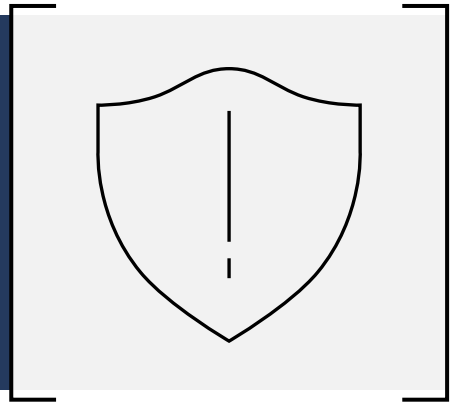
Administración de secretos

Administración de claves

Administración de certificados

Almacenar secretos protegidos con HW o SW

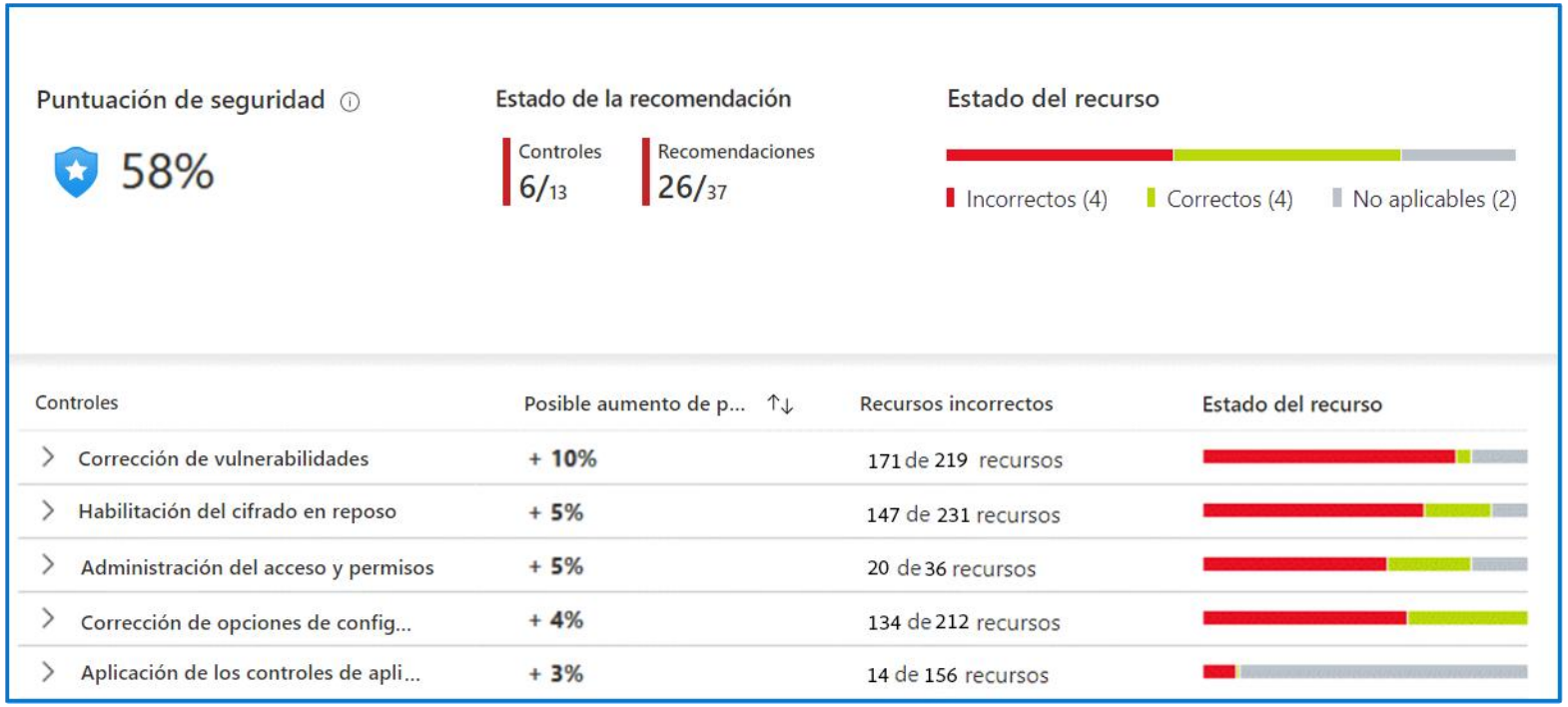
Lección 2: Describir las funcionalidades de administración de la seguridad de Azure



Microsoft Defender for Cloud

Su postura de seguridad de un vistazo

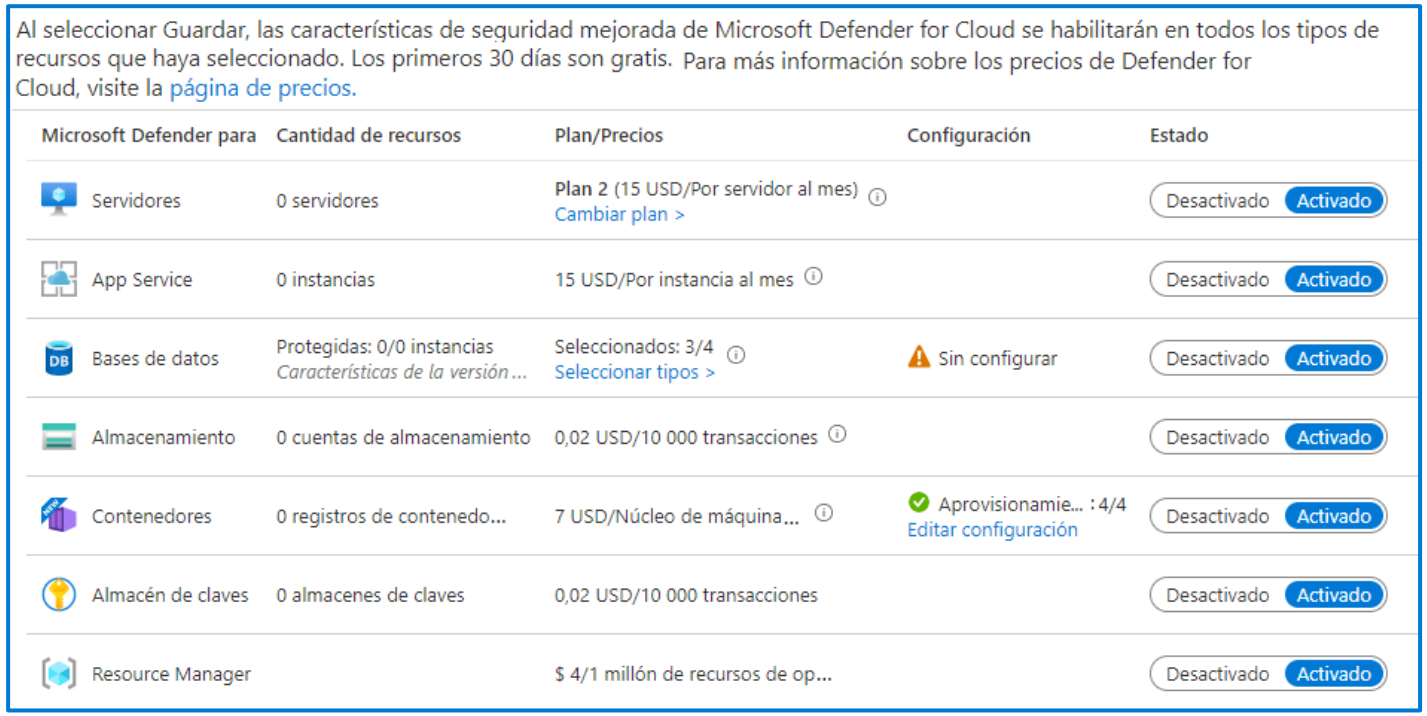
- **Evalúa continuamente los recursos, suscripciones y la organización en busca de problemas de seguridad.**
- Agrega todos los resultados en una sola puntuación.
- Recomendaciones de protección sobre cualquier error de configuración y puntos débiles de seguridad identificados.



Seguridad mejorada de Microsoft Defender for Cloud

Los planes de Microsoft Defender for Cloud ofrecen funciones de seguridad mejoradas para sus cargas de trabajo:

- Detección y respuesta de los puntos de conexión
- Examen de vulnerabilidades
- Seguridad en varias nubes
- Seguridad híbrida
- Alertas de protección contra amenazas
- Controles de acceso y aplicación

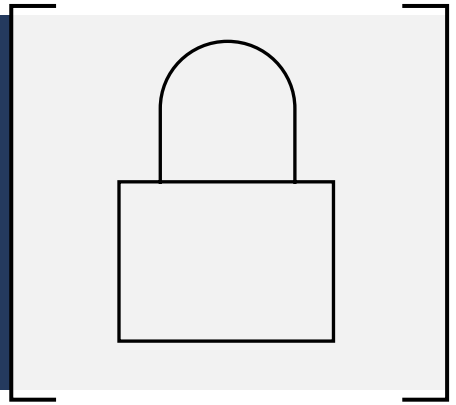


Azure Security Benchmark y líneas base de seguridad para Azure.

Azure Security Benchmark (ASB) **proporciona recomendaciones y procedimientos recomendados para mejorar la seguridad de las cargas de trabajo**, los datos y los servicios de Azure. ***Las líneas base de seguridad para Azure*** aplican las orientaciones desde el ASB al servicio específico para el que se definen. La siguiente imagen es un extracto de la línea base de seguridad para Azure AD.

Servicio	Control de Azure	Id. de Azure	Recomendación de banco de pruebas	Guía para clientes	Responsabilidad	Supervisión de Microsoft Defender for Cloud
Azure Active Directory	Seguridad de redes	NS-6	Simplificación de las reglas de seguridad de red	Use etiquetas de servicio de red virtual de Azure para definir los controles de acceso a la red en los grupos de seguridad de red o en el Azure Firewall configurado para sus recursos de Azure Active Directory. Puede utilizar etiquetas de servicio en lugar de direcciones IP específicas al crear reglas.	Cliente	No aplicable
Azure Active Directory	Seguridad de redes	NS-7	Servicio de nombres de dominio (DNS) seguro	Azure Active Directory no expone sus configuraciones de DNS subyacentes, Microsoft se encarga de mantener estas configuraciones.	Microsoft	No aplicable

Lección 3: Describir las funcionalidades de seguridad de Microsoft Sentinel



SIEM y SOAR

¿Qué es la administración de eventos e incidentes de seguridad?

Los sistemas SIEM son herramientas que las organizaciones utilizan para recopilar datos sobre el estado en su totalidad, incluidos la infraestructura, el software y los recursos. Realizan análisis, buscan correlaciones o anomalías y generan alertas e incidentes.

¿Qué es la respuesta automatizada de orquestación de seguridad?

Los sistemas SOAR reciben alertas de muchas fuentes, como los sistemas SIEM. **Después, los sistemas SOAR activan flujos de trabajo y procesos automatizados impulsados por acciones para ejecutar tareas de seguridad sencillas que mitiguen el problema**.

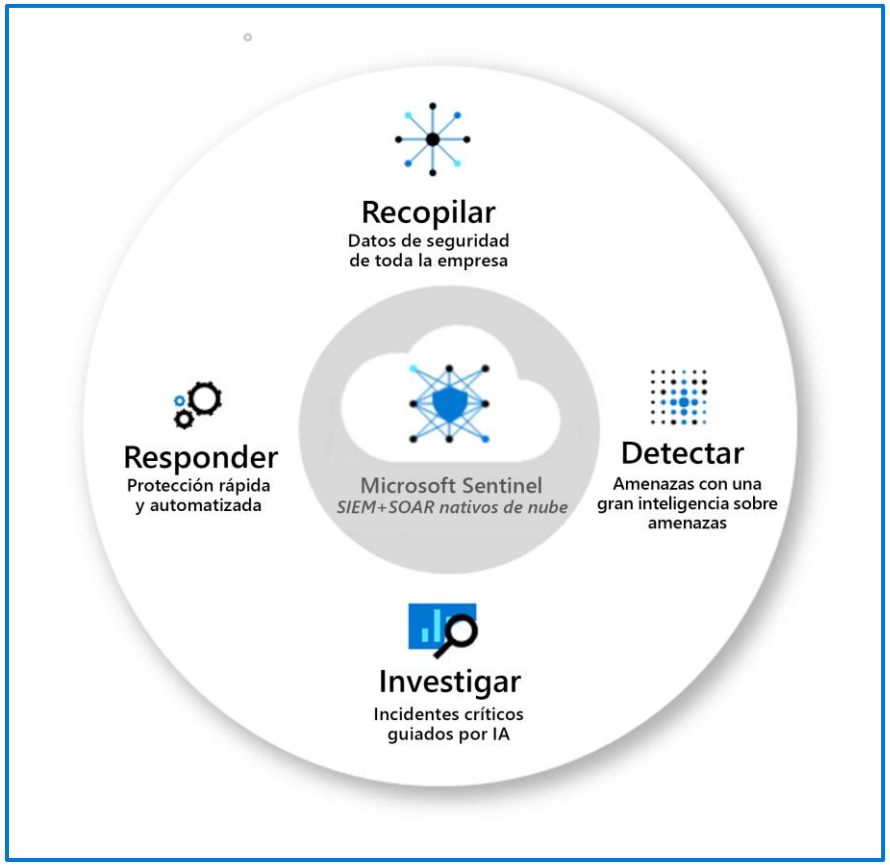
Microsoft Sentinel proporciona la administración integrada contra amenazas (diapositiva 1)

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

Detecte amenazas no detectadas previamente y minimice los falsos positivos mediante análisis y una inteligencia sobre amenazas incomparable.

Investigue amenazas con IA y busque actividades sospechosas a gran escala, gracias a décadas de trabajo de ciberseguridad en Microsoft.

Responda a los incidentes rápidamente con la orquestación y la automatización integradas de una seguridad común.



Microsoft Sentinel proporciona la administración integrada contra amenazas (diapositiva 2)

Conectar Microsoft Sentinel con sus datos: Utiliceconectores para las soluciones de Microsoft que proporcionan una integración en tiempo real.

Libros: Supervise los datos mediante la integración de Microsoft Sentinel con los libros de Azure Monitor.

Análisis: gracias a las alertas de análisis incorporadas, recibirá una notificación cuando se detecte algo sospechoso.

Administrar incidentes: Cuando se desencadena una alerta que ha habilitado, se crea un incidente.

Automatización y orquestación de seguridad: Integrar con Logic Apps para crear flujos de trabajo y cuadernos de estrategias.

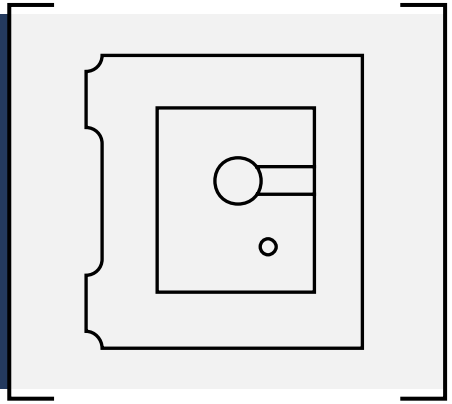
Cuadernos: Utilice cuadernos Jupyter para ampliar el ámbito de lo que puede hacer con los datos de Microsoft Sentinel.

Investigación: averigüe el ámbito de una posible amenaza contra la seguridad para identificar la causa principal.

Búsqueda: utilice herramientas de búsqueda y consulta, para buscar proactivamente las amenazas, antes de que se active una alerta.

Comunidad: Descargue el contenido del repositorio privado GitHub de la comunidad para crear libros personalizados, consultas de búsqueda y mucho más.

Lección 4: Describir la protección contra amenazas con Microsoft 365 Defender



Servicios de Microsoft 365 Defender

Microsoft 365 Defender

De manera nativa, coordina la detección, la prevención, la investigación y la respuesta frente a amenazas.

Protege identidades, puntos de conexión, aplicaciones, correo electrónico y colaboración.

Microsoft Defender for Cloud Apps

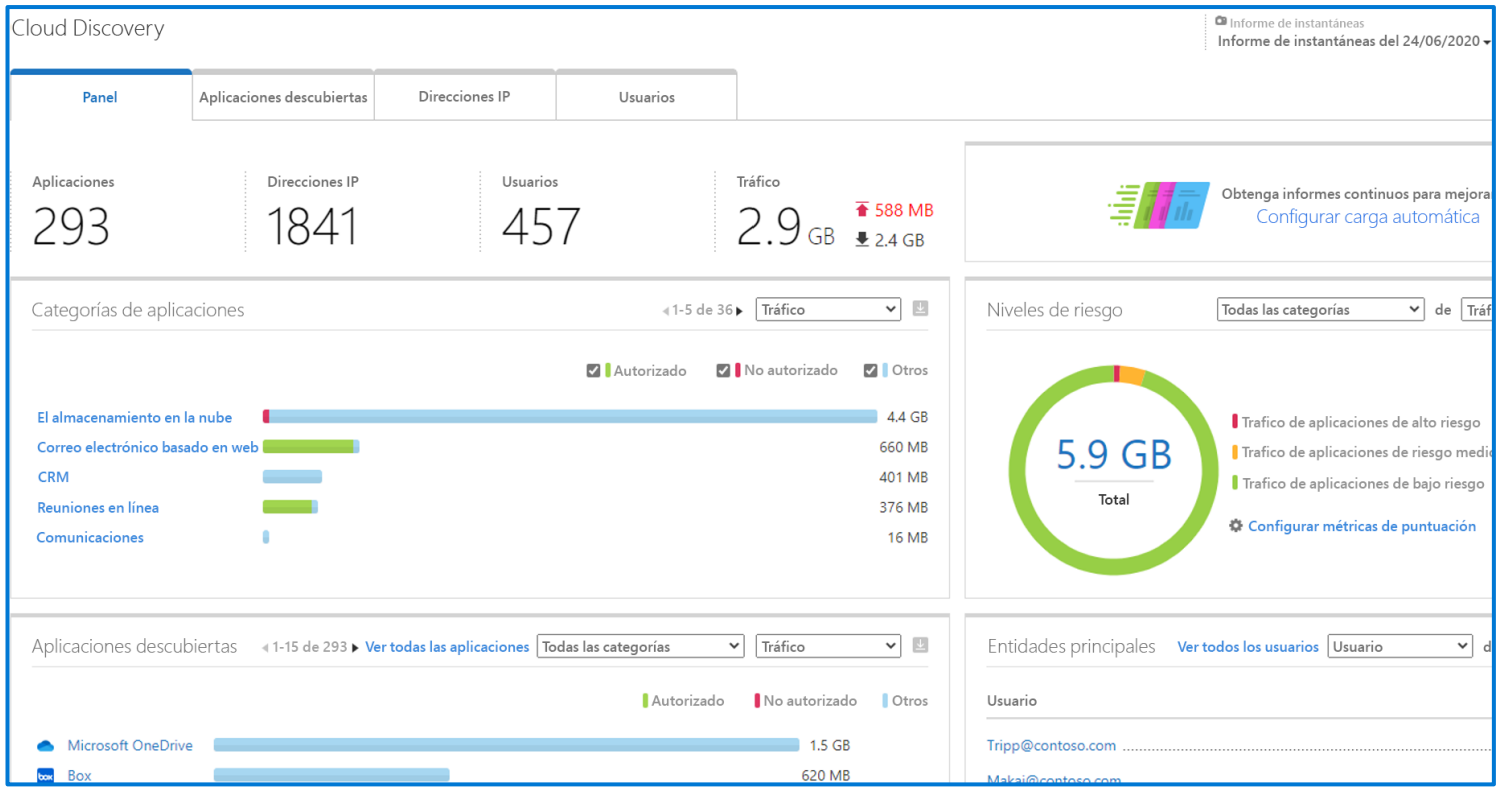
Microsoft Defender for Cloud Apps ofrece visibilidad enriquecida para los servicios en la nube**, control durante el trayecto de los datos y análisis sofisticados para identificar y combatir las ciberamenazas** en todos los servicios en la nube de Microsoft y de terceros.

El marco de Defender for Cloud Apps

- Detectar y controlar el uso de Shadow IT
- Proteger la información confidencial en cualquier lugar en la nube
- Protegerse frente a ciberamenazas y anomalías
- Evaluar el cumplimiento de las aplicaciones en la nube

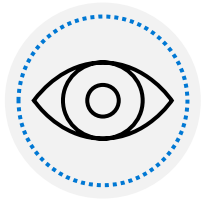
Office 365 Cloud App Security

Cloud App Discovery mejorada en Azure Active Directory



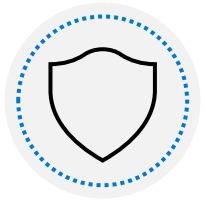
Microsoft Defender for Identity

Microsoft Defender for Identity se ocupa de las siguientes áreas principales



Supervisar y perfilar el comportamiento y las actividades de los usuarios

Defender for Identity supervisa y analiza las actividades del usuario y la información a través de la red, como los permisos y la pertenencia a grupos. De este modo, crea una base de referencia del comportamiento para cada usuario.

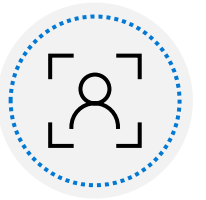


Proteger las identidades de los usuarios y reducir la superficie expuesta a ataques

Defender for Identity ofrece información valiosa sobre las configuraciones de identidad y los procedimientos recomendados de seguridad. Mediante informes de seguridad y análisis de los perfiles de usuario.

Identificar actividades sospechosas y ataques avanzados a lo largo de la cadena de eliminación de ciberataques

- Reconocimiento
- Credenciales en peligro
- Desplazamientos laterales
- Control de dominios



Investigar alertas y actividades de los usuarios

Defender for Identity está diseñado para reducir las alertas sonoras innecesarias al proporcionar solo alertas de seguridad relevantes e importantes en una escala de tiempo simple y en tiempo real del ataque organizativo.

Portal de Microsoft 365 Defender

El portal de Microsoft 365 Defender combina la protección, detección, investigación y respuesta a las amenazas de correo electrónico, colaboración, identidad y dispositivos, en un portal central.

- Visualización del estado de seguridad de la organización.
- Configuración de dispositivos, usuarios y aplicaciones.
- Recepción de alertas de actividades sospechosas.

El panel de navegación de Microsoft 365 Defender incluye estas opciones y más:

https://www.youtube.com/watch?v=1rewKCKZ9kc

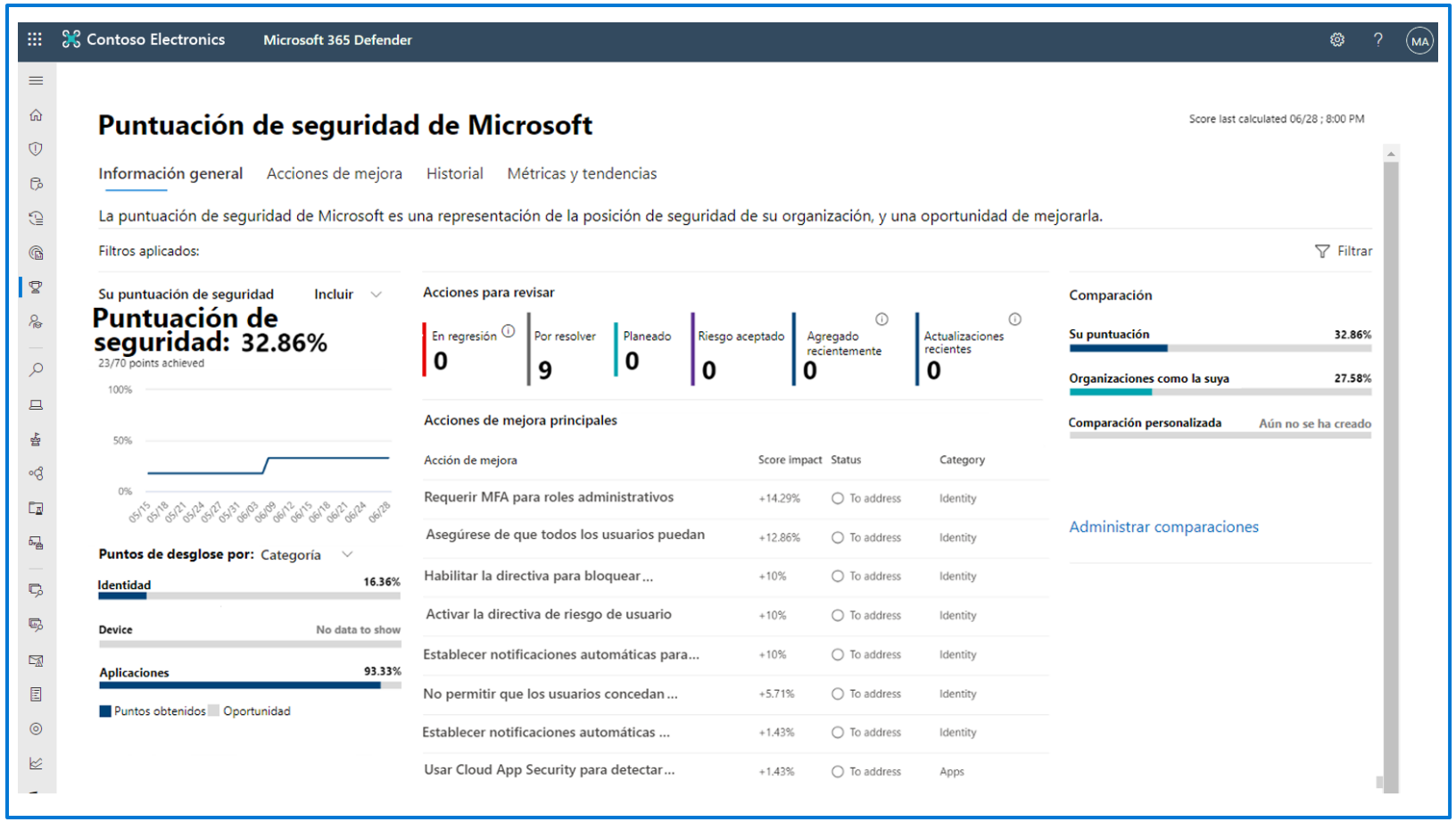
Puntuación de seguridad de Microsoft

La Puntuación de seguridad de Microsoft es la representación de la seguridad de una organización.

Indicará todas las mejoras posibles para el producto, sea cual sea la edición de la licencia, la suscripción o el plan.

Incluye recomendaciones para:

- Microsoft 365
- Azure Active Directory
- Microsoft Defender para punto de conexión
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps



Microsoft Security