**Introducción**

Este módulo se centra en equipar a los administradores con los conocimientos y aptitudes necesarios para administrar y mejorar la posición de seguridad de su entorno de nube mediante Microsoft Defender for Cloud, lo que garantiza la identificación proactiva y la corrección de los riesgos de seguridad.

**Escenario**

Imagine que es un especialista en seguridad en la nube responsable de proteger los recursos en la nube de la organización. La organización se basa en varios proveedores y servicios en la nube, y necesita mantener una posición de seguridad sólida en todo el entorno, mediante la identificación y solución de forma proactiva de los riesgos de seguridad.

**Objetivos de aprendizaje**

Al final de este módulo, los participantes podrán:

* Identifique y corrija riesgos de seguridad mediante el inventario y la puntuación de seguridad de Microsoft Defender for Cloud para evaluar y mejorar la posición de seguridad.
* Evalúe el cumplimiento con los marcos de seguridad y Microsoft Defender for Cloud para garantizar la alineación con los estándares de seguridad y los procedimientos recomendados.
* Agregue estándares normativos y del sector a Microsoft Defender for Cloud para mantener el cumplimiento de requisitos específicos.
* Agregue iniciativas personalizadas a Microsoft Defender for Cloud para satisfacer las necesidades de seguridad específicas de la organización.
* Conectar entornos de nube híbrida y multinube a Microsoft Defender for Cloud para centralizar la supervisión y administración de la seguridad.
* Identificar y supervisar recursos externos con la Administración de superficie expuesta a ataques externos de Microsoft Defender para protegerse de amenazas externas.

**Objetivos**

El módulo tiene como objetivo proporcionar a los participantes el conocimiento y la experiencia necesarios para administrar y mejorar de forma eficaz la posición de seguridad de su entorno de nube mediante Microsoft Defender for Cloud. Los participantes podrán identificar y corregir los riesgos de seguridad, mantener el cumplimiento y protegerse frente a amenazas externas, para, en última instancia, garantizar la seguridad y la resistencia de los recursos en la nube de su organización.

**Implementar Microsoft Defender para la nube**

Microsoft Defender for **Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP)** con un conjunto de medidas y procedimientos de seguridad diseñado para proteger las aplicaciones basadas en la nube frente a diversas ciberamenazas y vulnerabilidades.

Para obtener información general interactiva sobre cómo administrar la posición de seguridad en la nube con Microsoft Defender for Cloud, **haga clic en la imagen siguiente**.

[](https://mslearn.cloudguides.com/guides/Manage%20your%20cloud%20security%20posture%20with%20Microsoft%20Defender%20for%20Cloud)

<https://mslearn.cloudguides.com/guides/Manage%20your%20cloud%20security%20posture%20with%20Microsoft%20Defender%20for%20Cloud>

Defender for Cloud combina las funcionalidades de:

* Una solución de operaciones de seguridad de desarrollo (DevSecOps) que unifica la administración de seguridad en el nivel de código en entornos multinube y varias canalizaciones
* Una solución de administración de posturas de seguridad en la nube (CSPM) que muestra las acciones que puede realizar para evitar infracciones
* Una plataforma de protección de cargas de trabajo en la nube (CWPP) con protecciones específicas para servidores, contenedores, almacenamiento, bases de datos y otras cargas de trabajo

**Identificación y corrección de riesgos de seguridad mediante el inventario y la puntuación de seguridad de Microsoft Defender for Cloud**

**Información general de la puntuación segura**

Microsoft Defender for Cloud tiene **dos** objetivos principales:

* Ayudarlo a **comprender** la posición de seguridad actual
* Ayudarlo a mejorar la seguridad de forma **eficiente** y **eficaz**

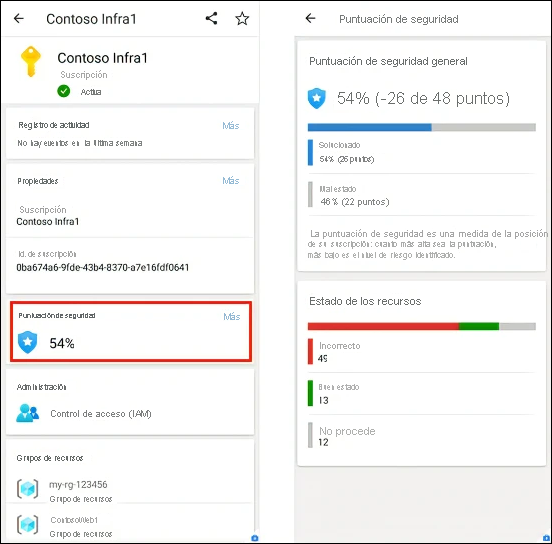
La característica principal de Defender for Cloud que le ayudará a conseguir estos objetivos es la puntuación de seguridad.

Defender for Cloud evalúa continuamente los recursos en distintas nubes en busca de problemas de seguridad. A continuación, **agrega todos los resultados en una sola puntuación** para que pueda saber de un vistazo su posición de seguridad actual: **cuanto mayor sea la puntuación**, **menor será el nivel de riesgo identificado**.

* En las páginas de Azure Portal, la puntuación de seguridad se muestra como un **valor porcentual** y los valores subyacentes también se presentan claramente:

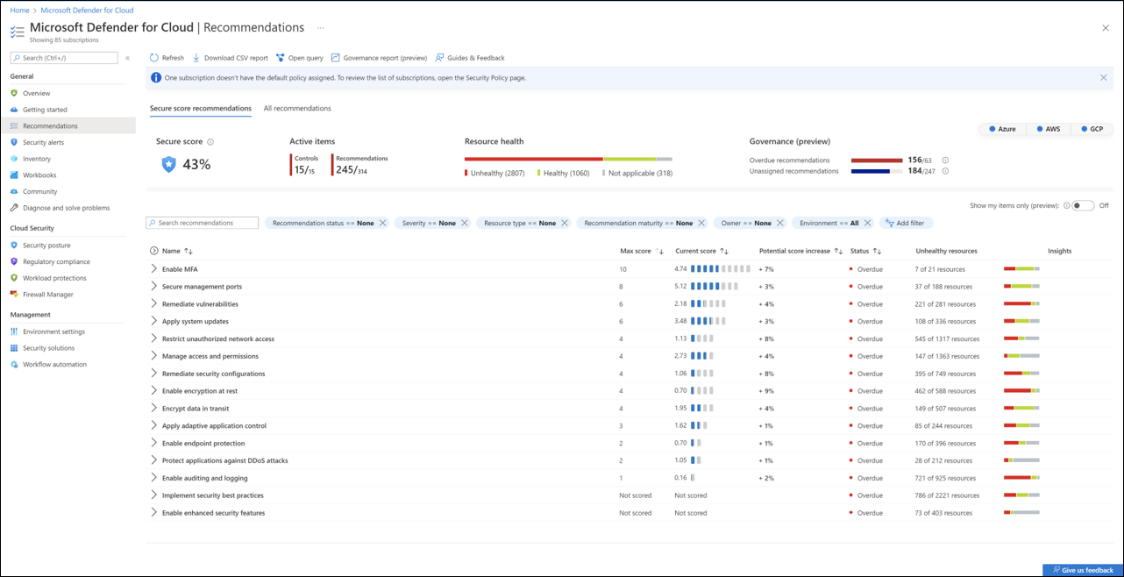


* En Azure Mobile App, la puntuación de seguridad se muestra como un valor porcentual. Púlsela para ver los detalles que la explican:



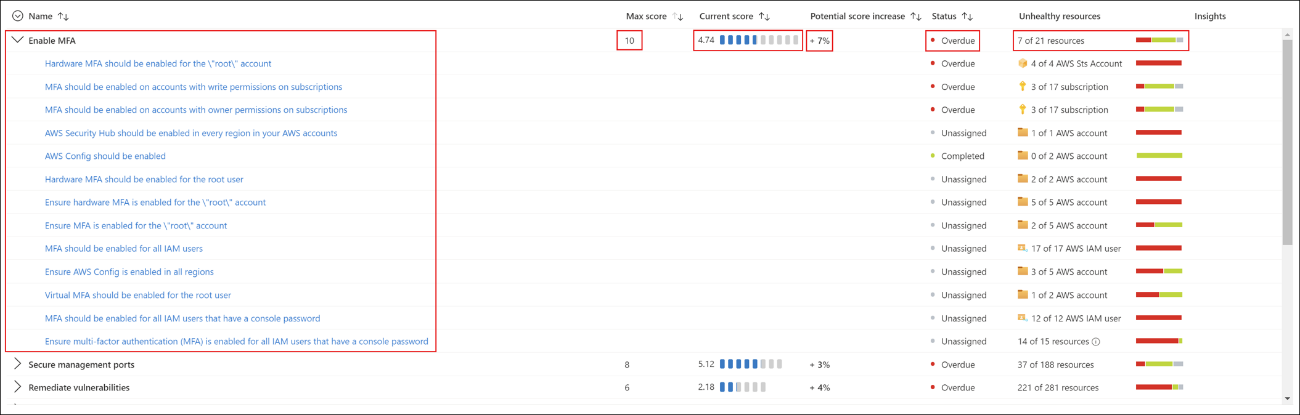
Para aumentar la seguridad, revise la **página de recomendaciones** de Defender for Cloud e implemente las instrucciones para corregir cada problema hasta que la recomendación desparezca. **Las recomendaciones se agrupan en controles de seguridad**. Cada control es un **grupo lógico de recomendaciones de seguridad relacionadas** y **refleja las superficies de ataque vulnerables**. La puntuación solo mejora cuando ***corrige todas*** las recomendaciones para un ***solo recurso de un control***. Para ver cómo protege su organización cada todas y cada una de las superficies expuesta a ataques, revise las puntuaciones de cada control de seguridad.

**Cálculo de la puntuación de seguridad**



Para obtener todos los puntos posibles de un control de seguridad, todos los **recursos deben cumplir todas las recomendaciones de seguridad para ese control**. **Por ejemplo**, Defender for Cloud tiene varias recomendaciones sobre cómo proteger los puertos de administración. Deberá corregirlas todas para que la puntuación de seguridad mejore.

**Puntuaciones de ejemplo para un control**



**En este ejemplo:**

* Control de seguridad Corregir vulnerabilidades: este control agrupa varias recomendaciones relacionadas con la detección y resolución de vulnerabilidades conocidas.
* Puntuación máxima: el número máximo de puntos que puede obtener al completar todas las recomendaciones de un control. La puntuación máxima de un control indica la importancia relativa de ese control y es fija para cada entorno. Use los valores de puntuación máxima para evaluar la prioridad de los problemas.
* Puntuación actual: la puntuación actual de este control.

Puntuación actual = [**Puntuación por recurso**] \* [**Número de recursos con un estado correcto**]

Cada control contribuye a la puntuación total. En este ejemplo, el control contribuye con **2,00 puntos** a la puntuación total de seguridad actual.

* Posible aumento de puntuación: los demás puntos disponibles están bajo su control. Si corrige todas las recomendaciones de este control, la puntuación aumentará en un 9 %.

Posible aumento de puntuación = [**Puntuación por recurso**] \* [**Número de recursos incorrectos**]

* Información: proporciona detalles adicionales de cada recomendación, como:
  + Screenshot of the preview recommendation icon that provides extra detail.**Recomendación de versión preliminar**: esta recomendación no afectará a la puntuación de seguridad hasta que esté **disponible con carácter general (GA)**.
  + Screenshot of the fix icon that enables you to resolve issues.**Corregir**: en la página de detalles de la recomendación, use "**Corregir**" para resolver este problema.
  + Screenshot of the enforce icon that enables you to automatically deploy a policy to fix an issue.**Aplicar**: en la página de detalles de la recomendación, puede implementar automáticamente una directiva para corregir este problema cada vez que alguien crea un recurso no conforme.
  + Screenshot of the deny icon that enables you to prevent new resources from being created with identified issues.**Denegar**: en la página de detalles de la recomendación, puede evitar la creación de recursos con este problema.

**¿Qué recomendaciones se incluyen en los cálculos de la puntuación de seguridad?**

* Solo las recomendaciones integradas afectan a la puntuación de seguridad.
* Las recomendaciones marcadas como Versión preliminar no se incluyen en los cálculos de la puntuación de seguridad. Aun así, deben corregirse siempre que sea posible para que, cuando finalice el período de versión preliminar, contribuyan a aumentar la puntuación.
* Las recomendaciones en versión preliminar están marcadas con: Screenshot of the preview recommendations icon for secure score options after General Availability.

**Mejora de su puntuación de seguridad**

Para mejorar la puntuación de seguridad, corrija las recomendaciones de seguridad de la lista de recomendaciones. Puede corregir manualmente cada recomendación de cada recurso, o bien usar la **opción Corregir** (**cuando esté disponible**) para resolver un problema en varios recursos rápidamente.

También puede configurar las opciones "Forzar" y "Denegar" en las recomendaciones pertinentes para mejorar la puntuación y asegurarse de que los usuarios no creen recursos que afecten negativamente a la puntuación.

**Preguntas más frecuentes (P+F) sobre la puntuación de seguridad**

**Si solo corrijo tres de cuatro recomendaciones de un control de seguridad, ¿cambia mi puntuación de seguridad?**

No. No cambiará hasta que corrija todas las recomendaciones para un único recurso. Para obtener la puntuación máxima de un control, deberá corregir todas las recomendaciones de los recursos.

**Si una recomendación no es aplicable a mí y la deshabilito en la directiva, ¿se cumplirá mi control de seguridad y se actualizará mi puntuación de seguridad?**

Sí. Se recomienda deshabilitar las recomendaciones cuando no son aplicables a su entorno.

**Si un control de seguridad ofrece cero puntos para mi puntuación de seguridad, ¿debería ignorarlo?**

En algunos casos verá una puntuación máxima del control mayor que cero, pero el impacto es nulo. Cuando la puntuación incremental para corregir recursos es insignificante, se redondea a cero. Aun así, no ignore estas recomendaciones, ya que todavía pueden aportar mejoras de seguridad. La única excepción es el control "**Procedimiento recomendado adicional**". La corrección de estas recomendaciones no aumentará la puntuación, pero mejorará la seguridad en general.

**Evaluación del cumplimiento con marcos de seguridad y Microsoft Defender for Cloud**

Microsoft Defender for Cloud resulta de gran ayuda para simplificar el proceso necesario para cumplir los requisitos de cumplimiento normativo, para lo que se usa el panel de cumplimiento normativo. Defender for Cloud evalúa continuamente el entorno de nube híbrida para analizar los factores de riesgo con arreglo a los controles y los procedimientos recomendados establecidos en los estándares que haya aplicado a las suscripciones. El panel refleja el estado de cumplimiento con respecto a estos estándares.

Cuando habilite Defender for Cloud en una suscripción de Azure, se asignará automáticamente Microsoft Cloud Security Benchmark a esta suscripción. Este punto de referencia, que cuenta con un amplísimo respaldo, se basa en los controles del Center for Internet Security (CIS), del PCI-DSS y del Instituto Nacional de Normas y Tecnología (NIST), con un enfoque en seguridad centrada en la nube.

En el panel de cumplimiento normativo se indica el estado de todas estas valoraciones realizadas en el entorno conforme a las normativas y los estándares elegidos. Al actuar sobre las recomendaciones y reducir los factores de riesgo en su entorno, su estado de cumplimiento normativo mejora.

**Sugerencia**

*Los datos de cumplimiento de Defender for Cloud ahora se integran perfectamente con el Administrador de cumplimiento de Microsoft Purview, lo que le permite evaluar y administrar de manera centralizada el cumplimiento en todo el patrimonio digital de la organización. Al agregar cualquier estándar al panel de cumplimiento (incluidos los estándares de cumplimiento que supervisan otras nubes como AWS y GCP), los datos de cumplimiento de nivel de recurso se exponen automáticamente en el Administrador de cumplimiento para el mismo estándar. Por lo tanto, el Administrador de cumplimiento proporciona acciones y estado de mejora en la infraestructura en la nube y en todos los demás recursos digitales de esta herramienta central.*

**Mejora del cumplimiento de reglamentaciones**

El panel de cumplimiento normativo muestra los estándares normativos seleccionados, con todos sus requisitos. Los requisitos compatibles se asignarán a las evaluaciones de seguridad correspondientes. El estado de estas evaluaciones refleja el estado de cumplimiento con respecto a los estándares.

Utilice el panel de cumplimiento normativo para centrarse en las deficiencias relativas al cumplimiento de las normativas y estándares elegidos. Esta vista focalizada también le permite supervisar continuamente su puntuación de cumplimiento a lo largo del tiempo para entornos híbrido y de nube dinámicos.

1. Inicie sesión en Azure Portal.
2. Vaya a **Defender for Cloud**, **Cumplimiento normativo**.

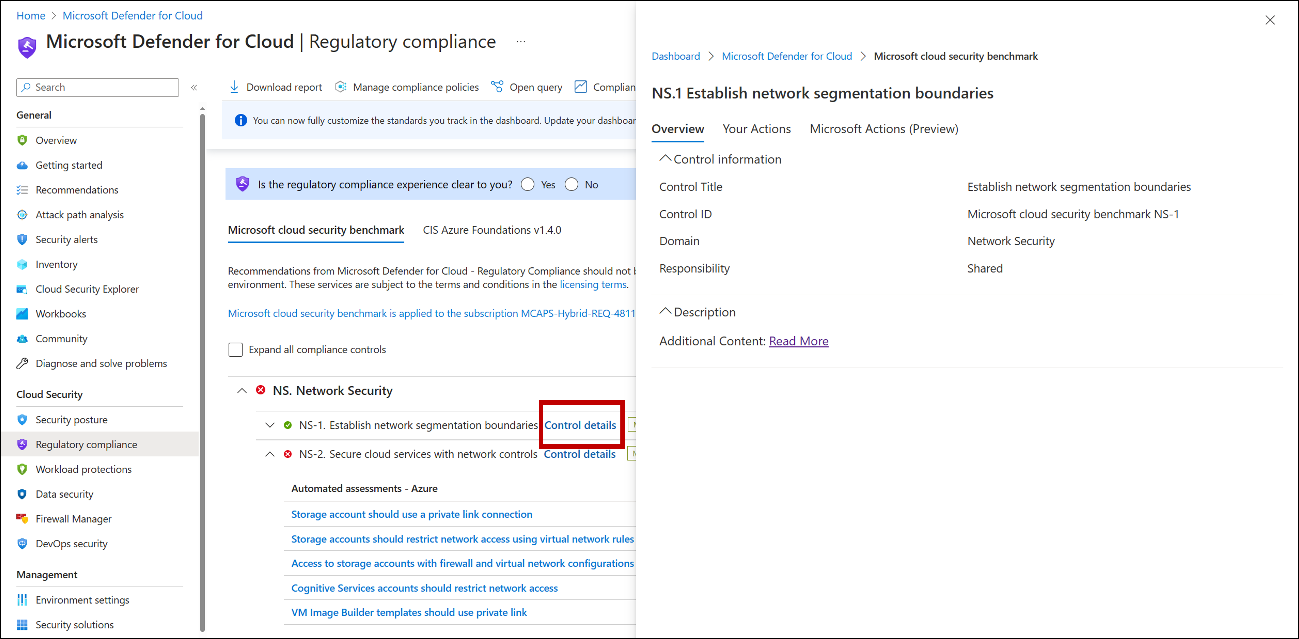
El panel proporciona información general sobre el estado de cumplimiento y el conjunto de normativas de cumplimiento admitidas. Allí se indica la puntuación global de cumplimiento y el número de valoraciones aprobadas y suspendidas asociadas a cada estándar.

**Investigación de los problemas de cumplimiento normativo**

Se puede usar la información del panel de cumplimiento normativo para investigar cualquier incidencia que pudiera afectar a su posición de cumplimiento.

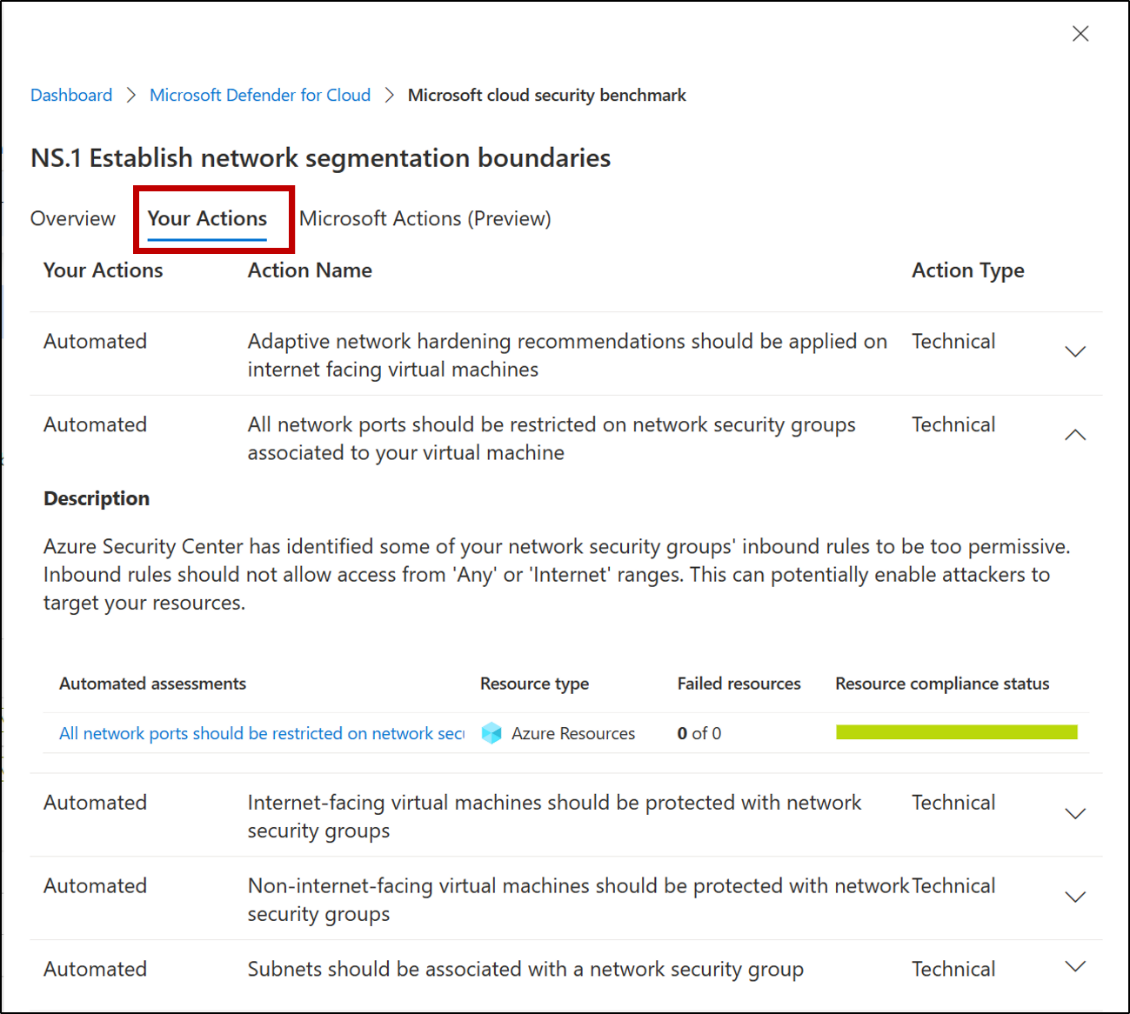
**Para investigar los problemas de cumplimiento, haga lo siguiente:**

1. Inicie sesión en Azure Portal.
2. Vaya a **Defender for Cloud**, **Cumplimiento normativo**.
3. Seleccione un estándar de cumplimiento normativo.
4. Seleccione un control de cumplimiento para expandirlo.
5. Seleccione **Detalles del control**.



* Seleccione Información general para ver la información específica sobre el control seleccionado.
* Seleccione Sus acciones para ver una vista detallada de las acciones automatizadas y manuales que debe realizar para mejorar su posición de cumplimiento.
* Seleccione Acciones de Microsoft para ver todas las acciones que Microsoft ha realizado para garantizar el cumplimiento del estándar seleccionado.

1. En **Sus acciones**, puede seleccionar una flecha abajo para ver más detalles y resolver la recomendación de ese recurso.



**Nota**

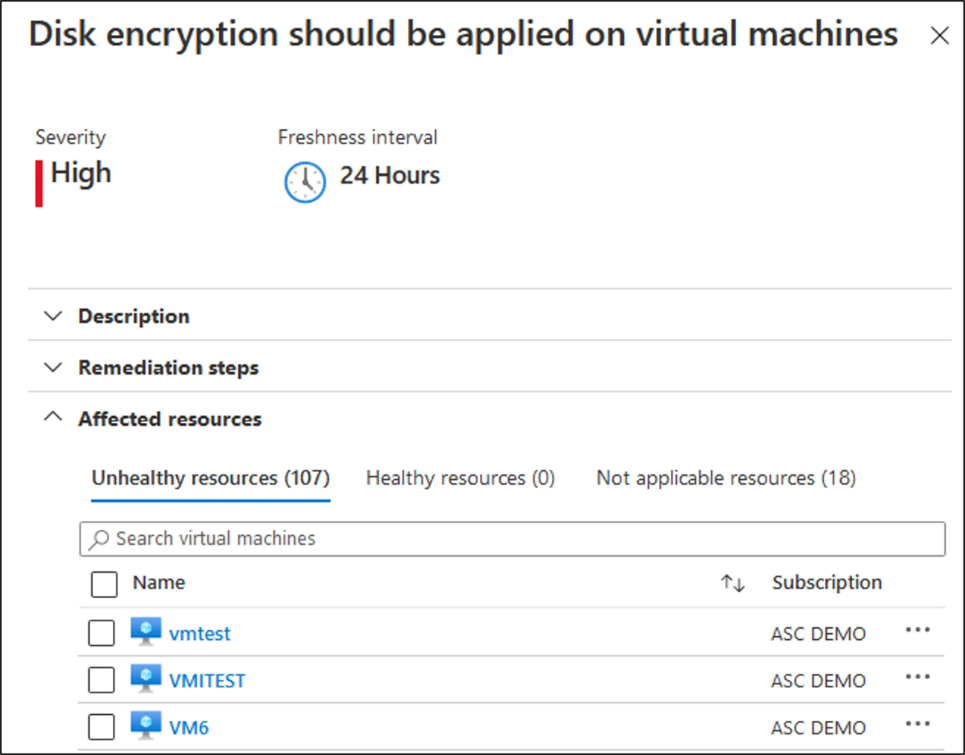
*Las valoraciones se ejecutan aproximadamente cada 12 horas, por lo que el efecto sobre los datos de cumplimiento solo se constatará tras la ejecución siguiente de la valoración en cuestión.*

**Corrección de una evaluación automatizada**

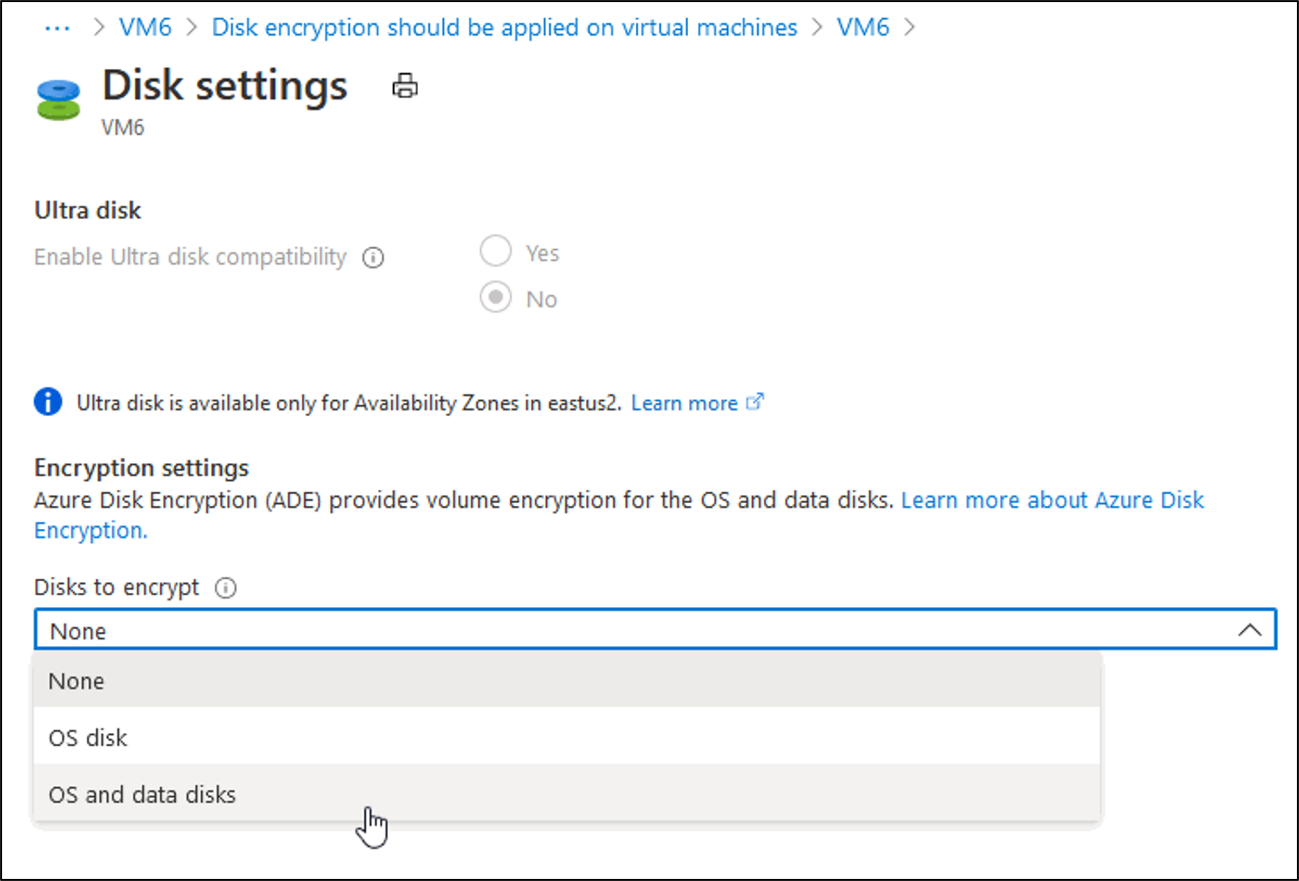
El cumplimiento normativo tiene evaluaciones automatizadas y manuales que quizá se tengan que corregir. El panel contiene información que le ayudará a mejorar el cumplimiento normativo y le permitirá resolver las recomendaciones directamente en él.

**Para corregir una evaluación automatizada, haga lo siguiente:**

1. Inicie sesión en Azure Portal.
2. Vaya a **Defender for Cloud**, **Cumplimiento normativo**.
3. Seleccione un estándar de cumplimiento normativo.
4. Seleccione un control de cumplimiento para expandirlo.
5. Seleccione cualquiera de las evaluaciones no superadas que aparecen en el panel para ver los detalles de dicha recomendación. Cada recomendación incluye un conjunto de pasos de corrección para resolver el problema.
6. Seleccione un recurso concreto para ver más detalles y resolver la recomendación relacionada.



1. En este ejemplo, si selecciona **Realizar acción** en la página de detalles de la recomendación, accederá Azure Portal, a las páginas de la máquina virtual de Azure, donde podrá abrir la pestaña **Seguridad** y habilitar el cifrado:



1. Una vez realizadas las acciones necesarias para resolver las recomendaciones, podrá ver el resultado en el informe del panel de cumplimiento, ya que la puntuación de cumplimiento mejora.

**Corregir una evaluación manual**

El cumplimiento normativo tiene evaluaciones automatizadas y manuales que quizá se tengan que corregir. Las evaluaciones manuales son evaluaciones que requieren la intervención del cliente para corregirlas.

**Para corregir una evaluación manual, haga lo siguiente:**

1. Inicie sesión en Azure Portal.
2. Vaya a **Defender for Cloud**, **Cumplimiento normativo**.
3. Seleccione un estándar de cumplimiento normativo.
4. Seleccione un control de cumplimiento para expandirlo.
5. En la sección Atestación y evidencia manual, seleccione una evaluación.
6. Seleccione la suscripción correspondiente.
7. Seleccione **Atestar**.
8. Escriba la información pertinente y adjunte pruebas para el cumplimiento.
9. Seleccione **Guardar**.

**Agregar estándares regulatorios y del sector a Microsoft Defender for Cloud**

La **prueba comparativa de seguridad en la nube de Microsoft (MCSB)** proporciona **procedimientos recomendados prescriptivos** y **recomendaciones** para ayudar a mejorar la seguridad de las cargas de trabajo, los datos y los servicios en Azure y su entorno multinube. Se centra en las áreas de control orientadas a la nube con entrada desde un conjunto de instrucciones holísticas de seguridad de Microsoft y del sector que incluyen:

* **Cloud Adoption Framework**: guía de **seguridad** que incluye indicaciones sobre **estrategias**, **roles** y **responsabilidades**, los **10 principales procedimientos recomendados de seguridad de Azure** y una **implementación de referencia**.
* **Marco de buena arquitectura de Azure**: instrucciones sobre protección de las cargas de trabajo en Azure.
* **Taller para directores de seguridad de la información (CISO)**: instrucciones del programa y estrategias de referencia para acelerar la modernización de la seguridad usando principios de Confianza cero.
* **Otros marcos y estándares de procedimientos recomendados de seguridad del sector y de proveedores de servicios en la nube**; por ejemplo, Amazon Web Services (**AWS**), Marco de buena arquitectura, controles del Center for Internet Security (**CIS**), Instituto Nacional de Estándares y Tecnología (**NIST**) y Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (**PCI-DSS**).

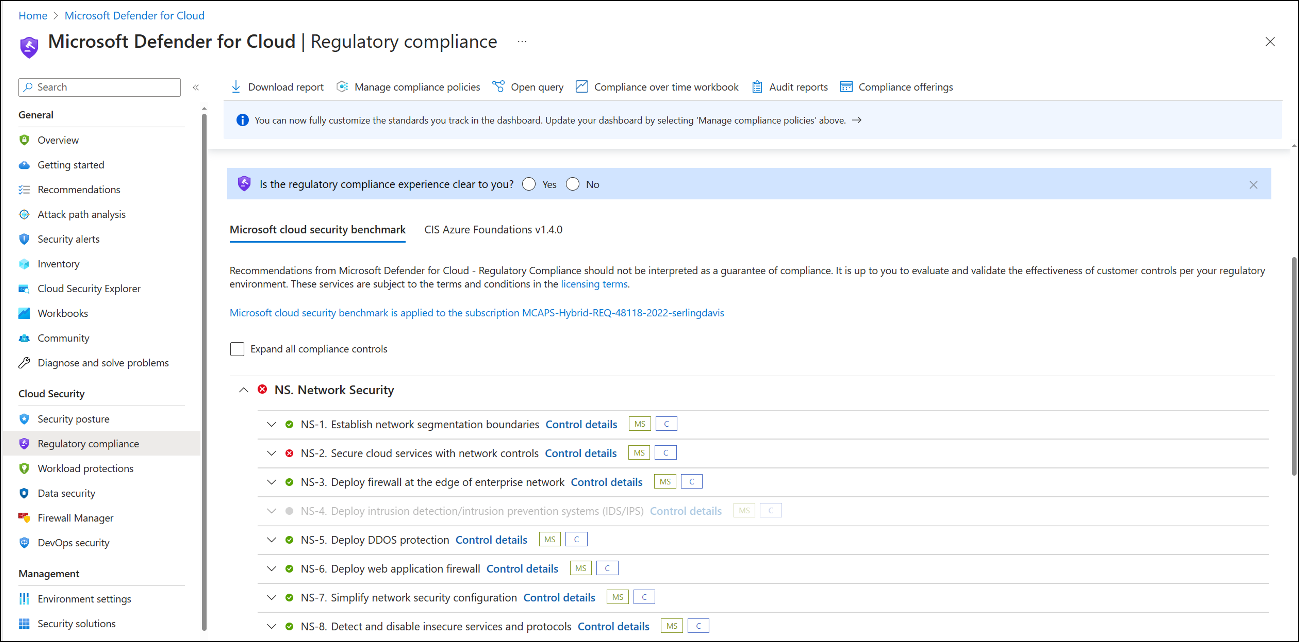
**Características de Microsoft Cloud Security Benchmark**

**Marco de seguridad multinube integral**: con frecuencia, las organizaciones tienen que crear un estándar de seguridad interno para conciliar los controles de seguridad en varias plataformas en la nube, a fin de cumplir los requisitos de seguridad y cumplimiento en cada una de ellas. Esto suele requerir que los equipos de seguridad repitan las mismas tareas de implementación, supervisión y evaluación en los diferentes entornos de nube (**a menudo con diferentes estándares de cumplimiento normativo**). Esto supone una sobrecarga, un coste y un esfuerzo innecesarios. Para solucionar este problema, hemos mejorado **Azure Security Benchmark (ASB)**, que ahora es **Microsoft Cloud Security Benchmark (MCSB)**. Este marco le ayuda a trabajar rápidamente con diferentes nubes porque:

* Proporcionando un único marco de control para satisfacer fácilmente los controles de seguridad de todas las nubes
* Proporcionando una experiencia de usuario uniforme para supervisar y aplicar el punto de referencia de seguridad multinube en Defender for Cloud
* Se mantiene alineado con los estándares del sector (por ejemplo, Center for Internet Security, Instituto Nacional de Estándares y Tecnología, e Industria de Tarjetas de Pago).

**Supervisión de controles automatizada para AWS en Microsoft Defender for Cloud**: puede usar el **panel de cumplimiento normativo de Microsoft Defender for Cloud** para supervisar su entorno de AWS respecto a **Microsoft Cloud Security Benchmark (MCSB)**, de igual forma que supervisa su entorno de Azure. Hemos desarrollado alrededor de **180 comprobaciones de AWS** para la nueva guía de seguridad de AWS en MCSB, lo que le permite supervisar su entorno y sus recursos de AWS en Microsoft Defender for Cloud.

**Ejemplo**: Microsoft Defender for Cloud: panel de cumplimiento normativo



**Guía y principios de seguridad de Azure**: guía, principios, características y funcionalidad de seguridad de Azure.

**Controles**

| **Dominios de control** | **Descripción** |
| --- | --- |
| Seguridad de red (NS) | **Seguridad de red** cubre controles que protegen las redes, incluida la protección de redes virtuales, el establecimiento de conexiones privadas, la prevención y la mitigación de ataques externos, y la protección de DNS (sistema de nombres de dominio). |
| Administración de identidades (IM) | **Administración de identidades** cubre controles que establecen una identidad segura y controles de acceso mediante sistemas de administración de identidad y acceso, incluido el uso del inicio de sesión único, la autenticación segura, las identidades administradas (y las entidades de servicio) para las aplicaciones, el acceso condicional y la supervisión de anomalías en las cuentas. |
| Acceso con privilegios (PA) | **Acceso con privilegios** cubre controles que protegen el acceso con privilegios a su inquilino a los recursos. Incluye una serie de controles para proteger el modelo administrativo, las cuentas administrativas y las estaciones de trabajo de acceso con privilegios frente a riesgos deliberados e involuntarios. |
| Protección de datos (DP) | **Protección de datos** cubre el control de la protección de datos en reposo, en tránsito y a través de mecanismos de acceso autorizados, incluidas la detección, la clasificación, la protección y la supervisión de los recursos de datos confidenciales mediante el control de acceso, el cifrado y la administración de claves y certificados. |
| Administración de recursos (AM) | **Administración de recursos** cubre controles que garantizan la visibilidad y la gobernanza de seguridad de los recursos, incluyendo recomendaciones sobre permisos para el personal de seguridad, el acceso de seguridad al inventario de recursos y la administración de las aprobaciones de servicios y recursos (**inventario**, **seguimiento** y **corrección**). |
| Registro y detección de amenazas (LT) | **Registro y detección de amenazas** cubre controles que detectan amenazas en la nube y habilitan, recopilan y almacenan registros de auditoría de servicios en la nube, incluida la habilitación de procesos de detección, investigación y corrección con controles para generar alertas de alta calidad con detección de amenazas nativa en los servicios en la nube. También incluye la recopilación de registros con un servicio de supervisión en la nube, la centralización de los análisis de seguridad con un sistema de **administración de eventos de seguridad (SEM)**, la sincronización de la hora y la retención de registros. |
| Respuesta a los incidentes (IR) | **Respuesta a incidentes** cubre controles del ciclo de vida de respuesta a incidentes: preparación, detección y análisis, contención y actividades posteriores a los incidentes, incluido el uso de servicios de Azure (**como Microsoft Defender for Cloud y Sentinel**) y otros servicios en la nube para automatizar el proceso de respuesta a incidentes. |
| Administración de posiciones y vulnerabilidades (PV) | **Administración de la posición y la vulnerabilidad** se centra en controles que evalúan y mejoran la posición de seguridad en la nube, incluyendo el examen de vulnerabilidades, las pruebas de penetración y la corrección, así como el seguimiento de la configuración de seguridad, informes y la corrección en los recursos en la nube. |
| Seguridad del punto de conexión (ES) | **Seguridad de los puntos de conexión** cubre controles de detección y respuesta de puntos de conexión, incluyendo el uso de detección y respuesta de puntos de conexión (EDR) y el servicio antimalware para puntos de conexión en entornos en la nube. |
| Copia de seguridad y recuperación (BR) | **Copia de seguridad y recuperación** cubre controles que garantizan que se realizan, validan y protegen las copias de seguridad de los datos y la configuración en los distintos niveles de servicio. |
| Seguridad de DevOps (DS) | **Seguridad de DevOps** cubre controles relacionados con la ingeniería de seguridad y las operaciones en los procesos de DevOps, incluida la implementación de comprobaciones de seguridad críticas (como las pruebas de seguridad de aplicaciones estáticas y la administración de vulnerabilidades) antes de la fase de implementación para garantizar la seguridad a lo largo del proceso de DevOps. También incluye temas comunes como el modelado de amenazas y la seguridad del suministro de software. |
| Gobernanza y estrategia (GS) | **Gobernanza y estrategia** proporciona una guía para garantizar una estrategia de seguridad coherente y un enfoque de gobernanza documentado para guiar y mantener el control de la seguridad, incluyendo el establecimiento de roles y responsabilidades para las diferentes funciones de seguridad en la nube, una estrategia técnica unificada y directivas y estándares de apoyo. |

**Incorporación de iniciativas personalizadas a Microsoft Defender for Cloud**

**¿Qué son las políticas e iniciativas de seguridad?**

Microsoft Defender for Cloud aplica iniciativas de seguridad a las suscripciones. Estas **iniciativas contienen una o varias directivas de seguridad**. Cada una de esas directivas da como resultado una recomendación de seguridad para mejorar la posición de seguridad.

**¿Qué es una iniciativa de seguridad?**

Una iniciativa de seguridad es una **colección de definiciones de Azure Policy** o **reglas agrupadas para satisfacer un objetivo o propósito concreto**. Las iniciativas de seguridad simplifican la administración de las directivas al **agrupar conjuntos de directivas**, **de manera lógica**, como un **elemento único**.

Una iniciativa de seguridad define la configuración deseada de las cargas de trabajo y ayuda a garantizar el cumplimiento de los requisitos de seguridad normativos o corporativos.

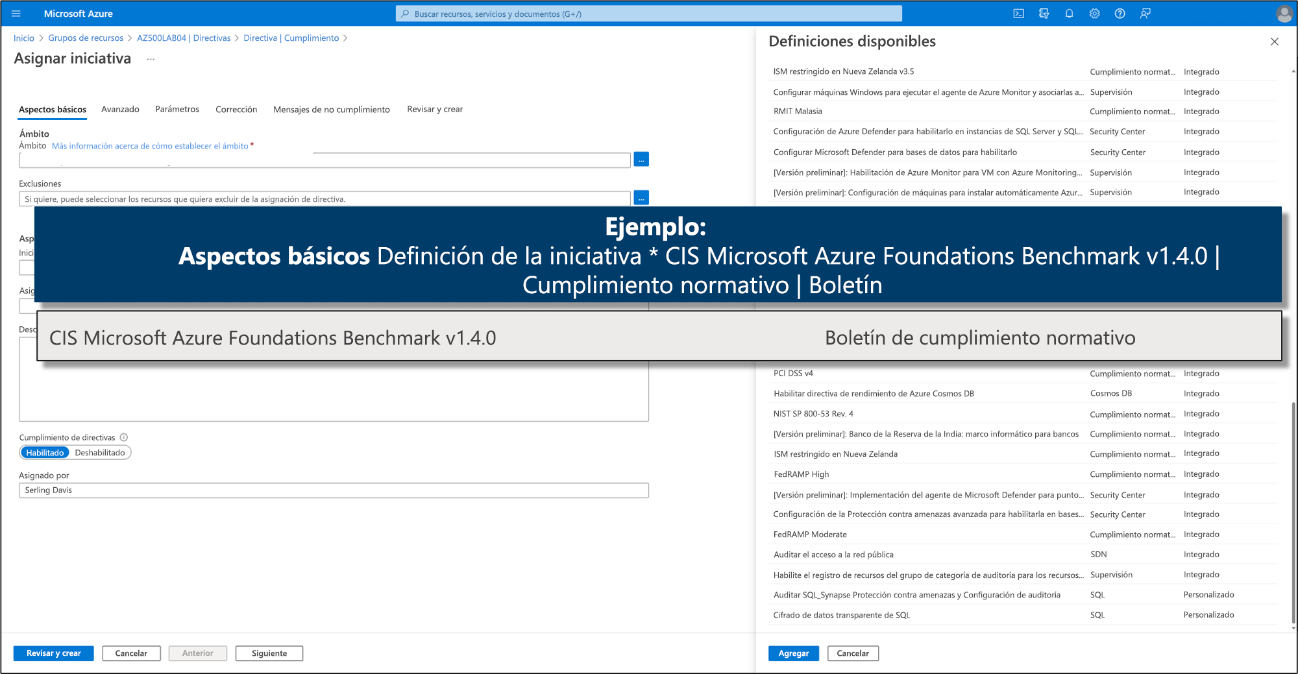
Al igual que las directivas de seguridad, las iniciativas de Defender for Cloud también se crean en Azure Policy. Puede usar **Azure Policy** para administrar las directivas y crear iniciativas y asignarlas a varias suscripciones o a grupos de administración completos.

La iniciativa predeterminada asignada automáticamente a todas las suscripciones en Microsoft Defender for Cloud son las pruebas comparativas de seguridad de Microsoft Cloud. Este punto de referencia es el conjunto de directrices creado por Microsoft relativo a los procedimientos recomendados de seguridad y cumplimiento basados en marcos de cumplimiento comunes. Esta prueba comparativa, que cuenta con amplísimo respaldo, se basa en los controles del **Centro de seguridad de Internet (CIS)** y del **Instituto Nacional de Normas y Tecnología (NIST)**, con un enfoque en seguridad centrada en la nube.

Defender for Cloud le ofrece las siguientes opciones para trabajar con iniciativas y directivas de seguridad:

* **Ver y editar la iniciativa predeterminada integrada**: al habilitar Defender for Cloud, la iniciativa denominada "Microsoft Cloud Security Benchmark" se asigna automáticamente a todas las suscripciones registradas de Defender for Cloud. Para personalizar esta iniciativa, puede habilitar o deshabilitar directivas individuales en ella mediante la edición de los parámetros de una directiva.
* **Agregar sus propias directivas personalizadas**: si quiere personalizar las iniciativas de seguridad que se aplican a su suscripción, puede hacerlo en Defender for Cloud. A continuación, recibirá recomendaciones si las máquinas no siguen las directivas que creó.
* **Incorporación de estándares de cumplimiento normativo como iniciativas**: el panel de cumplimiento normativo de Defender for Cloud muestra el estado de todas las evaluaciones dentro de su entorno en el contexto de un estándar o reglamento determinado (como **Azure Center for Internet Security (CIS)**, **Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST) SP 800-53 Rev.4**, **Call Session Control Function (CSCF) v2020 del programa de seguridad del cliente de Swift)**.

**Ejemplo:** Iniciativa de seguridad integrada



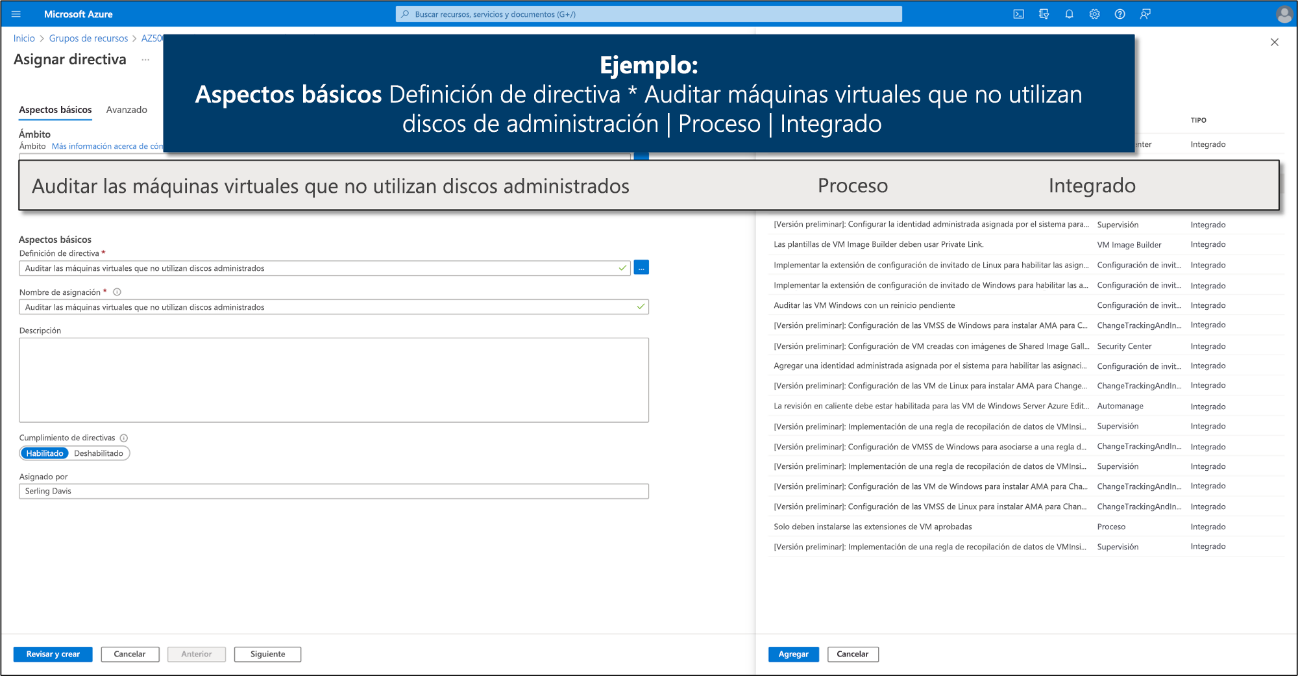
**¿Qué es una directiva de seguridad?**

Una definición de Azure Policy, creada en Azure Policy, es una **regla sobre condiciones de seguridad específicas que quiere controlar**. Las definiciones integradas incluyen elementos como el **control del tipo de recursos que se pueden implementar** o la **aplicación del uso de etiquetas en todos los recursos**. También puede crear su propia definición de directiva personalizada.

Para implementar estas definiciones de directiva (**tanto integradas** como **personalizadas**), será preciso asignarlas. Puede asignar cualquiera de estas directivas a través de **Azure Portal**, **PowerShell** o la **CLI de Azure**. Las directivas se pueden habilitar o deshabilitar desde Azure Policy.

Hay diferentes tipos de directivas en Azure Policy. Defender for Cloud utiliza principalmente directivas de "**auditoría**" que **comprueban condiciones** y **configuraciones** específicas y, **a continuación, notifican el cumplimiento**. También hay directivas de **aplicación** que se pueden usar para **aplicar una configuración segura**.

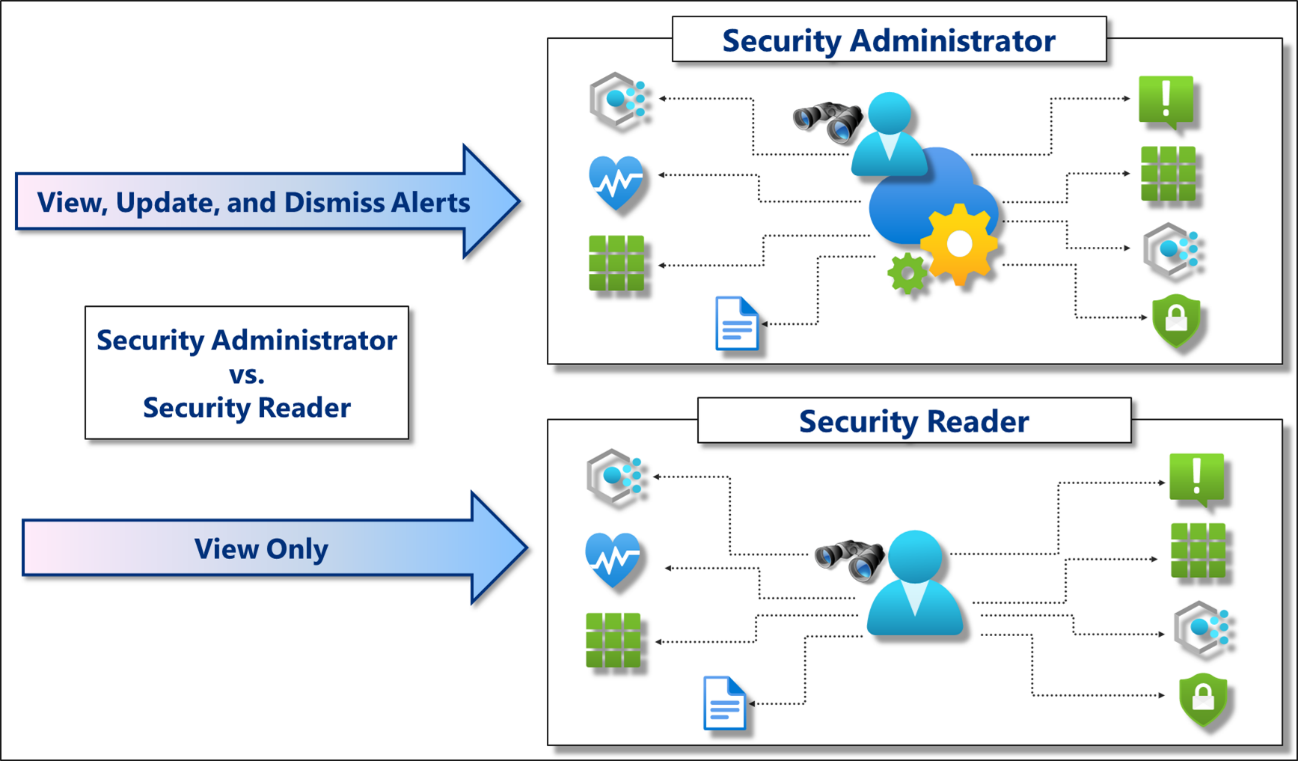
**Ejemplo:** Directiva de seguridad integrada



Defender for Cloud usa el **control de acceso basado en rol de Azure (Azure RBAC)**, que proporciona roles integrados que puede asignar a **usuarios**, **grupos** y **servicios** de Azure. Cuando un usuario abre Defender for Cloud, solo ve la información relacionada con los recursos a los que puede tener acceso. A los usuarios se les asigna el rol de propietario, colaborador o lector para la suscripción del recurso.

Hay dos roles específicos para Defender for Cloud:

* **Administrador de seguridad**: tiene los mismos derechos de visualización que el lector de seguridad. También se puede actualizar la directiva de seguridad y descartar alertas.
* **Lector de seguridad**: tiene derechos para ver elementos de Defender for Cloud como recomendaciones, alertas, directiva y estado. No se pueden realizar cambios.



Puede editar las directivas de seguridad en el **portal de Azure Policy** mediante la **interfaz de programación de aplicaciones de transferencia de estado representacional (API REST)** o con **Windows PowerShell**.

La pantalla "Directiva de seguridad" refleja la acción realizada por las directivas asignadas a la suscripción o al grupo de administración que ha seleccionado.

* Use los vínculos de la parte superior para abrir cada asignación de directiva que se aplique a la suscripción o al grupo de administración. Puede usar esos vínculos para obtener acceso a la asignación y editar o deshabilitar la directiva. **Por ejemplo**, si ve que una asignación de directiva determinada está denegando la protección de puntos de conexión, puede usar el vínculo para editar o deshabilitar la directiva.
* En la lista de directivas, puede ver la aplicación efectiva de la directiva en su suscripción o grupo de administración. Esto significa que se tiene en cuenta la configuración de cada directiva que se aplica al ámbito y se proporciona el resultado acumulado de la acción que realiza esa directiva. **Por ejemplo**, si en una asignación la directiva está deshabilitada, pero en otra está definida en **AuditIfNotExist**, el efecto acumulado aplica **AuditIfNotExist**. El efecto más activo siempre tiene prioridad.
* El efecto de las directivas puede ser: **Append**, **Audit**, **AuditIfNotExists**, **Deny**, **DeployIfNotExists** o **Disabled**.

**Conectar entornos de nube híbrida y multinube a Microsoft Defender for Cloud**

Conectar la nube híbrida y los entornos multinube a Microsoft Defender for Cloud es fundamental para mantener una posición de seguridad unificada en diversos entornos de TI. Con servidores habilitados de Azure Arc para máquinas que no son de Azure, Naive Cloud Connector y Classic Connector, puede ampliar las capacidades de Microsoft Defender para la nube a recursos que no son de Azure. Esta integración le permite supervisar, detectar y responder a amenazas de seguridad de forma completa. Aquí se proporciona información general sobre el proceso, junto con requisitos detallados para una conexión correcta.

**Conexión de máquinas que no son de Azure a Microsoft Defender for Cloud**

Microsoft Defender for Cloud puede supervisar la posición de seguridad de las máquinas que no son de Azure, pero, para ello, debe conectarlas primero a Azure.

Puede conectar equipos que no son de Azure de alguna de las maneras siguientes:

* Incorporación con Azure Arc:
  + Mediante servidores habilitados para Azure Arc (recomendado)
  + Mediante Azure Portal.
* Incorporación directa con Defender para punto de conexión

**Conexión de máquinas locales mediante Azure Arc**

Una máquina que tiene servidores habilitados para Azure Arc se convierte en un recurso de Azure. Cuando instala el agente de Log Analytics, aparece en Defender for Cloud con recomendaciones, como con los demás recursos de Azure.

Los servidores habilitados para Azure Arc proporcionan funcionalidades mejoradas, como la habilitación de directivas de configuración de invitados en la máquina y la simplificación de la implementación con otros servicios de Azure. Para obtener información general sobre las ventajas de los servidores habilitados para Azure Arc, consulte Operaciones en la nube admitidas.

Para implementar Azure Arc en una máquina, siga las instrucciones de Inicio rápido: Conexión de máquinas híbridas con servidores habilitados para Azure Arc.

Para implementar Azure Arc en varias máquinas a escala, siga las instrucciones de Conexión de máquinas híbridas a Azure a escala.

Las herramientas de Defender for Cloud para la implementación automática del agente de Log Analytics funcionan con máquinas que ejecutan Azure Arc. Sin embargo, esta capacidad se encuentra en versión preliminar. Cuando haya conectado las máquinas mediante Azure Arc, use la recomendación pertinente de Defender for Cloud para implementar el agente y aprovechar las ventajas del conjunto de protecciones que ofrece Defender for Cloud:

* El agente de Log Analytics se debe instalar en las máquinas de Azure Arc basadas en Linux
* El agente de Log Analytics se debe instalar en las máquinas de Azure Arc basadas en Windows

**Conexión de una cuenta de AWS a Microsoft Defender for Cloud**

Las cargas de trabajo suelen abarcar varias plataformas en la nube. Los servicios de seguridad en la nube deben hacer lo mismo. Microsoft Defender for Cloud ayuda a proteger las cargas de trabajo en Amazon Web Services (AWS), pero debe configurar la conexión entre ellas y Defender for Cloud.

Si está conectando una cuenta de AWS que conectó anteriormente mediante el conector clásico, debe eliminarla primero. Utilizar una cuenta de AWS que esté conectada tanto por el conector clásico como por el nativo puede producir recomendaciones duplicadas.

**Requisitos previos**

Para completar los procedimientos de este artículo, necesita:

* Una suscripción de Microsoft Azure. Si no tienes una suscripción de Azure, puedes registrarte para obtener una gratuita.
* Microsoft Defender for Cloud instalado en su suscripción Azure.
* Acceso a una cuenta de AWS.
* Permiso de colaborador para la suscripción a Azure correspondiente, y Permiso de administrador en la cuenta de AWS.

**Defender para contenedores**

Si elige el plan Microsoft Defender para contenedores, necesita:

* Al menos un clúster de Amazon EKS con permiso para acceder al servidor API de EKS Kubernetes. Si necesita crear un nuevo clúster de EKS, siga las instrucciones de Introducción a Amazon EKS: eksctl.
* La capacidad de recursos para crear una nueva cola de Amazon SQS, un flujo de entrega de Kinesis Data Firehose y un bucket de Amazon S3 en la región del clúster.

**Defender para SQL**

Si elige el plan Microsoft Defender para SQL, necesitará:

* Microsoft Defender para SQL habilitado en la suscripción. Aprenda a proteger su base de datos.
* Una cuenta de AWS activa, con instancias EC2 que ejecuten SQL Server o RDS Custom para SQL Server.
* Azure Arc para servidores instalados en sus instancias EC2 o RDS Custom para SQL Server.

Se recomienda usar el proceso de aprovisionamiento automático para instalar Azure Arc en todas las instancias de EC2 existentes y futuras. Para habilitar el aprovisionamiento automático de Azure Arc, necesita el permiso Propietario en la suscripción de Azure correspondiente.

AWS Systems Manager (SSM) administra el aprovisionamiento automático mediante el agente de SSM. Algunas imágenes de máquina de Amazon ya tienen el agente SSM preinstalado. Si sus instancias EC2 no tienen el Agente SSM, instálelo siguiendo estas instrucciones de Amazon: Instalar Agente SSM para un entorno híbrido y multicloud (Windows).

Asegúrese de que su Agente SSM tiene la directiva administrada AmazonSSMManagedInstanceCore. Habilita la funcionalidad principal para el servicio AWS Systems Manager.

Habilite estas otras extensiones en los equipos conectados a Azure Arc:

* Microsoft Defender para punto de conexión
* Una solución de evaluación de vulnerabilidades (TVM o Qualys)
* El agente de Log Analytics en máquinas conectadas a Azure Arc o el agente de Azure Monitor.

Asegúrese de que el área de trabajo de Log Analytics seleccionada tiene instalada una solución de seguridad. El agente de Log Analytics y el agente de Azure Monitor están configurados actualmente en el nivel subscription. Todas sus cuentas de AWS y proyectos de Google Cloud Platform (GCP) bajo la misma suscripción heredan la configuración de suscripción para el agente de Log Analytics y el agente de Azure Monitor.

**Defender para servidores**

Si elige el plan Microsoft Defender para servidores necesitará:

* Microsoft Defender para servidores está habilitado en la suscripción. Obtenga información sobre cómo habilitar planes en Habilitación de las características de seguridad mejoradas.
* Una cuenta de AWS activa, con instancias de EC2.
* Azure Arc para servidores instalado en las instancias de EC2.

Se recomienda usar el proceso de aprovisionamiento automático para instalar Azure Arc en todas las instancias de EC2 existentes y futuras. Para habilitar el aprovisionamiento automático de Azure Arc, necesita el permiso Propietario en la suscripción de Azure correspondiente.

AWS Systems Manager administra el aprovisionamiento automático mediante el agente de SSM. Algunas imágenes de máquina de Amazon ya tienen el agente SSM preinstalado. Si sus instancias EC2 no tienen el Agente SSM, instálelo utilizando cualquiera de las siguientes instrucciones de Amazon:

* Instalación del Agente SSM para un entorno híbrido y multinube (Windows)
* Instalación del Agente SSM para un entorno híbrido y multinube (Linux)

Asegúrese de que su Agente SSM tiene la directiva administrada AmazonSSMManagedInstanceCore, que habilita la funcionalidad principal para el servicio AWS Systems Manager.

Si quiere instalar manualmente Azure Arc en las instancias de EC2 existentes y futuras, use la recomendación de Las instancias de EC2 deben estar conectadas a Azure Arc para identificar las instancias que no tienen instalado Azure Arc.

Habilite estas otras extensiones en los equipos conectados a Azure Arc:

* Microsoft Defender para punto de conexión
* Una solución de evaluación de vulnerabilidades (TVM o Qualys)
* El agente de Log Analytics en máquinas conectadas a Azure Arc o el agente de Azure Monitor.

Asegúrese de que el área de trabajo de Log Analytics seleccionada tiene instalada una solución de seguridad. El agente de Log Analytics y el agente de Azure Monitor están configurados actualmente en el nivel subscription. Todas sus cuentas de AWS y proyectos de GCP bajo la misma suscripción heredan la configuración de suscripción para el agente de Log Analytics y el agente de Azure Monitor.

Defender para servidores asigna etiquetas a los recursos de AWS para administrar el proceso de aprovisionamiento automático. Debe tener estas etiquetas correctamente asignadas a sus recursos para que Defender for Cloud pueda administrarlos: AccountId, Cloud, InstanceId y MDFCSecurityConnector.

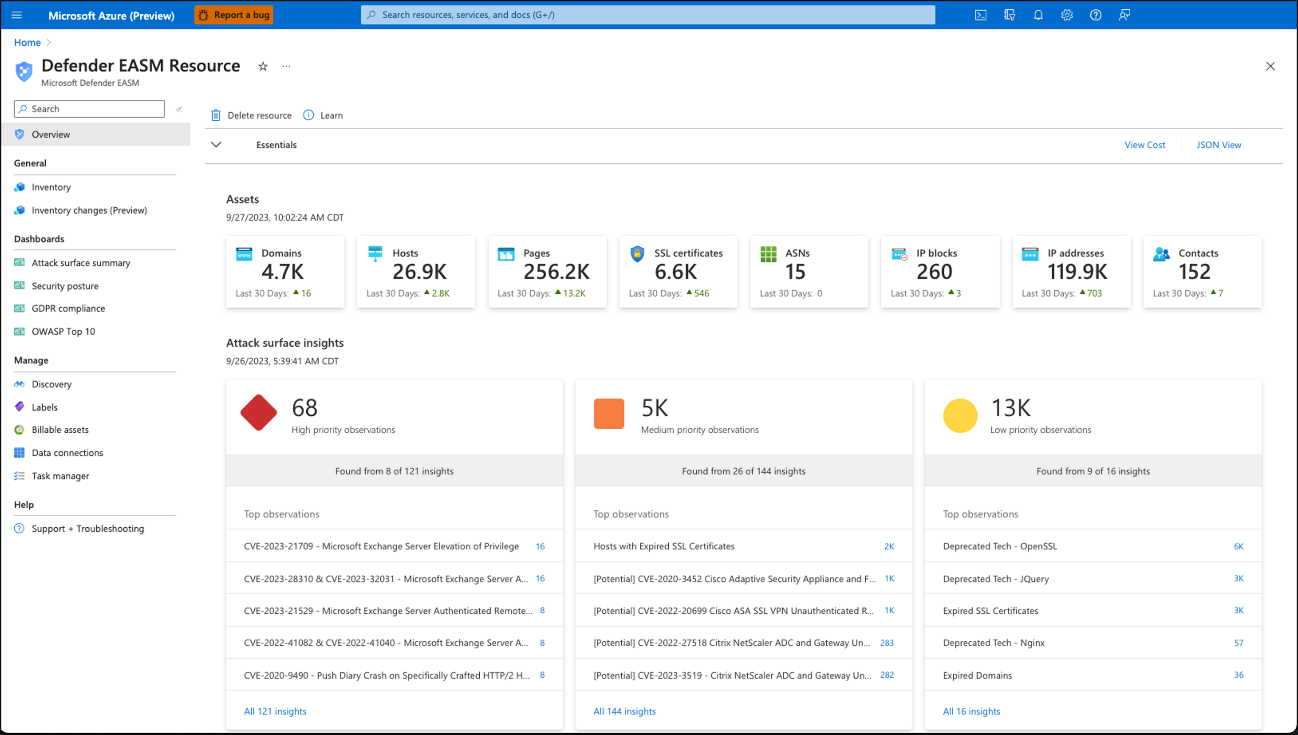
**Administración de la posición de seguridad en la nube de Defender**

Si elige el plan CSPM de Microsoft Defender, necesitará:

* una suscripción de Microsoft Azure. Si no tiene una suscripción de Azure, puede registrarse para una evaluación gratuita.
* Debe haber habilitado Defender for Cloud en la suscripción de Azure.
* Conecte sus máquinas que no son de Azure, sus cuentas de AWS.
* Para obtener acceso a todas las características disponibles en el plan de CSPM, el **propietario de la suscripción** debe habilitar el plan.

**Identificar y supervisar recursos externos con la Administración de superficie expuesta a ataques externos de Microsoft Defender**

Microsoft Defender External Attack Surface Management (Defender EASM) detecta y asigna continuamente la superficie expuesta a ataques digitales para proporcionar una visión externa de la infraestructura en línea. Esta visibilidad permite a los equipos de seguridad y TI identificar elementos desconocidos, priorizar el riesgo, eliminar amenazas y ampliar el control de vulnerabilidades y exposición además que con el firewall. Se genera información sobre las superficies expuestas a ataques aprovechando los datos de vulnerabilidad y la infraestructura para mostrar las áreas clave de interés para la organización.

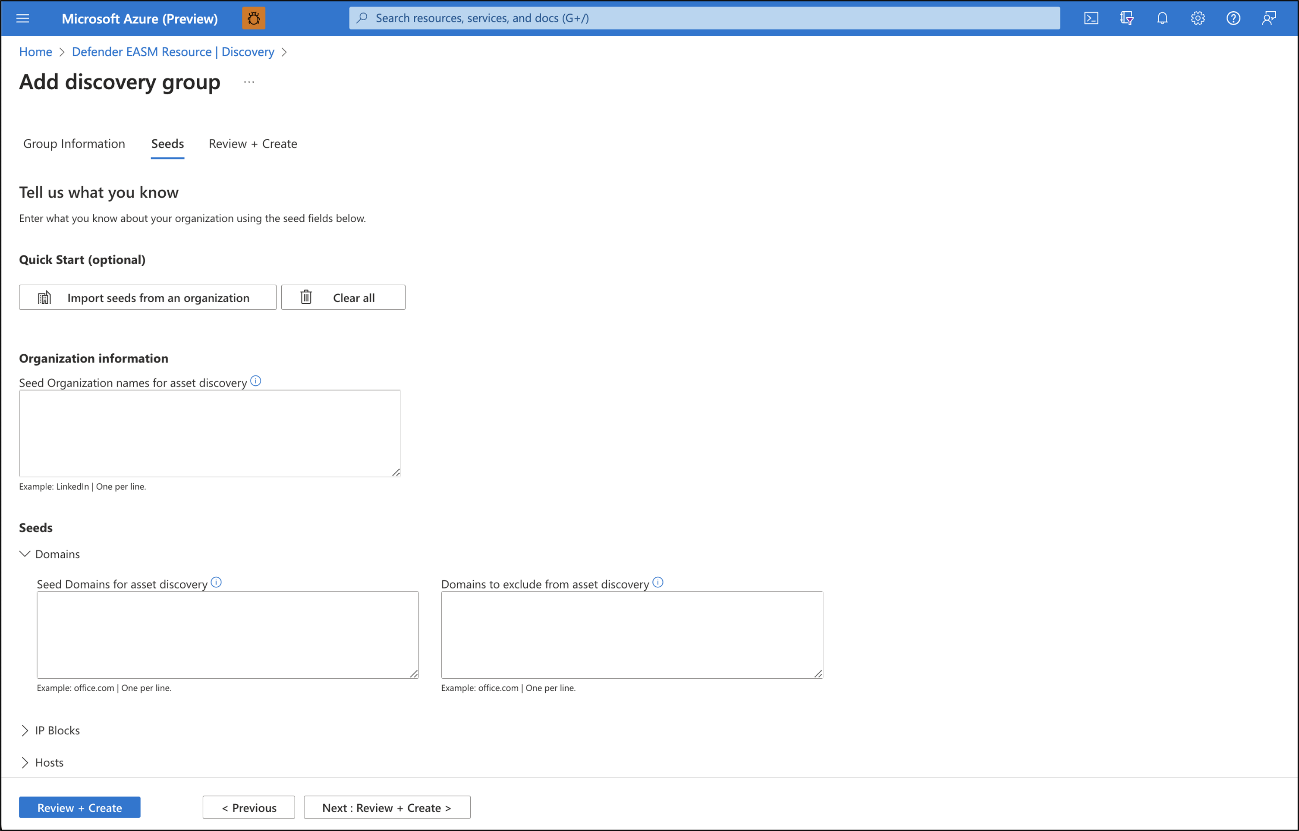


**Detección e inventario**

La tecnología de detección propiedad de Microsoft busca de forma recurrente infraestructura con conexiones observadas a recursos legítimos conocidos para hacer inferencias sobre la relación de esa infraestructura con la organización y descubrir propiedades que antes ni se conocían ni se supervisaban. Estos recursos legítimos conocidos se denominan "inicializaciones" de detección; Defender EASM detecta primero las conexiones sólidas con estas entidades seleccionadas y repite para revelar más conexiones y, en última instancia, compilar la superficie expuesta a ataques.

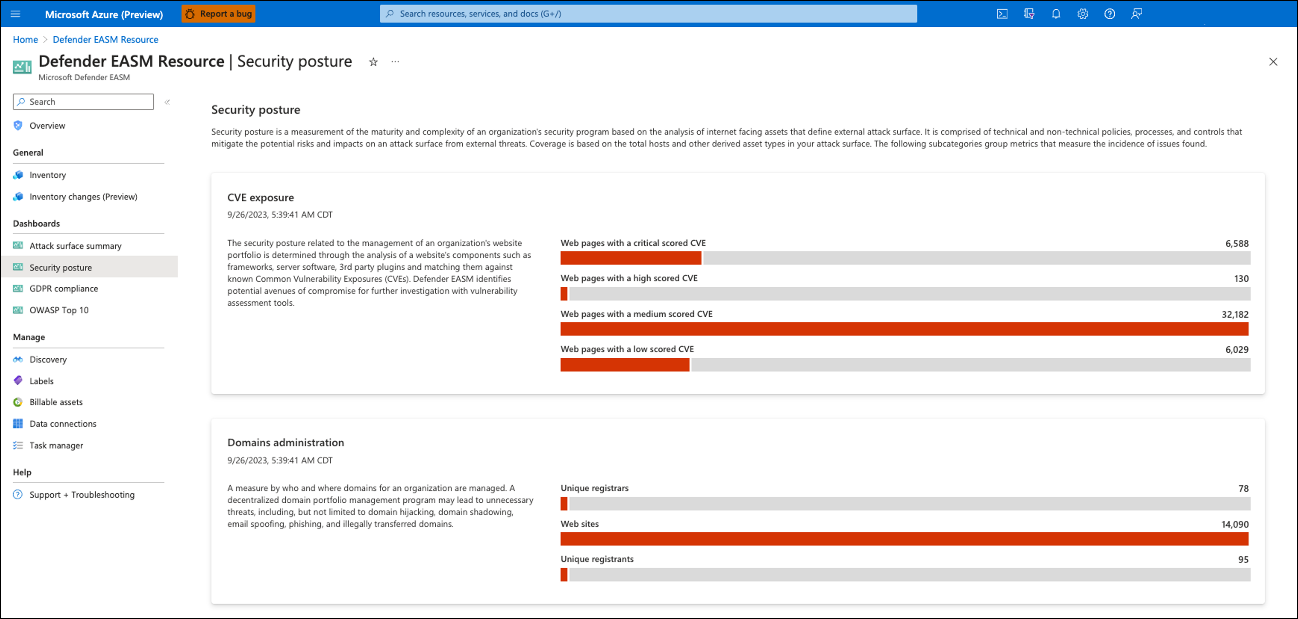
Defender EASM incluye la detección de los siguientes tipos de recursos:

* Dominios
* Nombres de host
* Páginas web
* Bloqueos de IP
* Direcciones IP
* ASN
* Certificados SSL
* Contactos de WHOIS



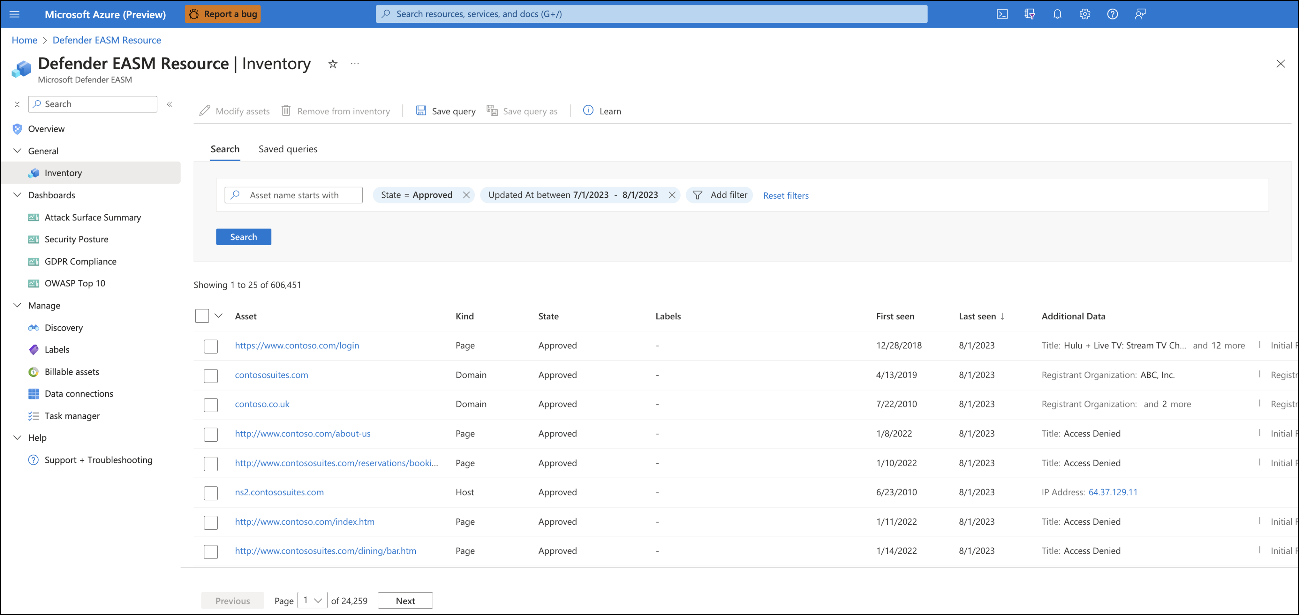
**Paneles**

Defender EASM proporciona una serie de paneles que ayudan a los usuarios a comprender rápidamente su infraestructura en línea y cualquier riesgo clave para su organización. Estos paneles están diseñados para proporcionar información sobre áreas específicas de riesgo, incluidas las vulnerabilidades, el cumplimiento y la higiene de la seguridad. Esta información ayuda a los clientes a abordar rápidamente los componentes de su superficie expuesta a ataques que suponen el mayor riesgo para la organización.



**Administración de recursos**

Los clientes pueden filtrar su inventario para exponer la información específica que más les interesa. El filtrado ofrece un nivel de flexibilidad y personalización que permite a los usuarios acceder a un subconjunto específico de recursos. Esto permite aprovechar los datos de Defender EASM según su caso de uso específico, ya sea para buscar recursos que se conectan a infraestructura en desuso o para identificar nuevos recursos en la nube.



**Permisos de usuario**

Los usuarios a los que se han asignado roles de propietario o colaborador pueden crear, eliminar y editar recursos de la EASM de Defender y los recursos de inventario que contiene. Estos roles pueden usar toda la funcionalidad disponible en la plataforma. Los usuarios a los que se ha asignado el rol Lector pueden ver los datos de la EASM de Defender, pero no pueden crear, eliminar ni editar recursos de inventario o el propio recurso.

**Residencia de los datos, disponibilidad y privacidad**

Microsoft Defender External Attack Surface Management contiene datos globales y datos específicos del cliente. Los datos subyacentes de Internet son datos globales de Microsoft; las etiquetas aplicadas por los clientes se consideran datos de cliente. Todos los datos de cliente se almacenan en la región que este prefiera.

Con fines de seguridad, Microsoft recopila las direcciones IP de los usuarios cuando inician sesión. Estos datos se almacenan durante un máximo de 30 días, pero pueden almacenarse más tiempo si es necesario para investigar posibles usos fraudulentos o malintencionados del producto.

En el caso de un escenario de región fuera de servicio, solo los clientes de la región afectada experimentarán el tiempo de inactividad.

El marco de cumplimiento de Microsoft requiere que todos los datos del cliente se eliminen en un plazo de 180 días a partir de que esa organización deje de ser cliente de Microsoft. Esto también incluye el almacenamiento de datos del cliente en ubicaciones sin conexión, como copias de seguridad de bases de datos. Una vez eliminado un recurso, nuestros equipos no pueden restaurarlo. Los datos del cliente se conservarán en nuestros almacenes de datos durante 75 días, pero no se puede restaurar el recurso real. Después del período de 75 días, los datos del cliente se eliminarán permanentemente.

**Prueba de conocimientos**

Elija la mejor respuesta para cada una de las preguntas. Después, seleccione **Comprobar las respuestas**.

**Comprobación de conocimientos**

Principio del formulario

**1. Un administrador de seguridad quiere aplicar directivas que se pueden usar para aplicar la configuración de seguridad. ¿Cuál de las siguientes directivas de seguridad integradas en Defender for Cloud usa el control de acceso basado en rol de Azure (Azure RBAC)?**

1. Defender for Cloud no tiene ninguna directiva de seguridad integrada.
2. Defender for Cloud usa una herramienta de terceros para directivas de seguridad integradas.
3. Defender for Cloud usa el control de acceso basado en rol de Azure (Azure RBAC), que proporciona roles integrados que puede asignar a usuarios, grupos y servicios de Azure.

**2. Una empresa quiere mejorar su posición de cumplimiento mediante la resolución de evaluaciones no superadas directamente dentro del panel. ¿Cuáles son los pasos que deben seguir para corregir una evaluación automatizada?**

1. Seleccione un recurso concreto para ver más detalles y resolver la recomendación relacionada.
2. Seleccione una evaluación manual para expandirla y ver los detalles de esa recomendación.
3. Seleccione un estándar de cumplimiento normativo, seleccione un control de cumplimiento para expandirlo, seleccione cualquiera de las evaluaciones no superadas que aparecen en el panel para ver los detalles de esa recomendación, seleccione un recurso determinado para ver más detalles y resolver la recomendación de ese recurso.

**3. Un analista de seguridad debe priorizar el riesgo y eliminar las amenazas más allá del firewall. ¿Qué característica de administración de superficie expuesta a ataques externos de Microsoft Defender proporciona visibilidad de la infraestructura en línea de la organización?**

1. Antivirus de Microsoft Defender
2. Firewall de Microsoft Defender
3. Administración de superficie expuesta a ataques externos de Microsoft Defender

**4. Una organización quiere conciliar los controles de seguridad en varias plataformas en la nube para cumplir los requisitos de seguridad y cumplimiento en cada uno de ellos. ¿Cuál es la mejor solución para este problema?**

1. Creación de un estándar de seguridad interno para cada plataforma en la nube
2. Uso de marcos de control diferentes para cada plataforma en la nube
3. Usando un único marco de control para satisfacer fácilmente los controles de seguridad de todas las nubes

**5. Una empresa quiere asegurarse de que los datos de sus clientes se almacenan de forma segura y se pueden restaurar en caso de desastre. Quieren saber cuánto tiempo se conservarán sus datos de cliente en los almacenes de datos y si se pueden restaurar después de ese período. ¿Cuál de las siguientes opciones describe correctamente el período de retención y la funcionalidad de restauración de los datos de los clientes?**

1. Los datos del cliente se conservarán en almacenes de datos durante un período indefinido y se pueden restaurar en cualquier momento.
2. Los datos del cliente se conservarán en almacenes de datos durante 30 días y se pueden restaurar después de ese período.
3. Los datos del cliente se conservarán en nuestros almacenes de datos durante 75 días, pero el recurso real no se puede restaurar. Después del período de 75 días, los datos del cliente se eliminarán permanentemente.
4. C
5. C
6. C
7. C
8. C

Final del formulario

**Resumen**

En este módulo, ha aprendido a administrar y mejorar de forma eficaz la posición de seguridad de su organización mediante Microsoft Defender for Cloud, incluida la identificación y el direccionamiento de los riesgos de seguridad a través de puntuación de seguridad e inventario, la evaluación del cumplimiento con marcos de seguridad, la personalización de estándares de seguridad, la conexión de entornos híbridos y multinube y la supervisión de recursos externos para una protección contra amenazas completa.