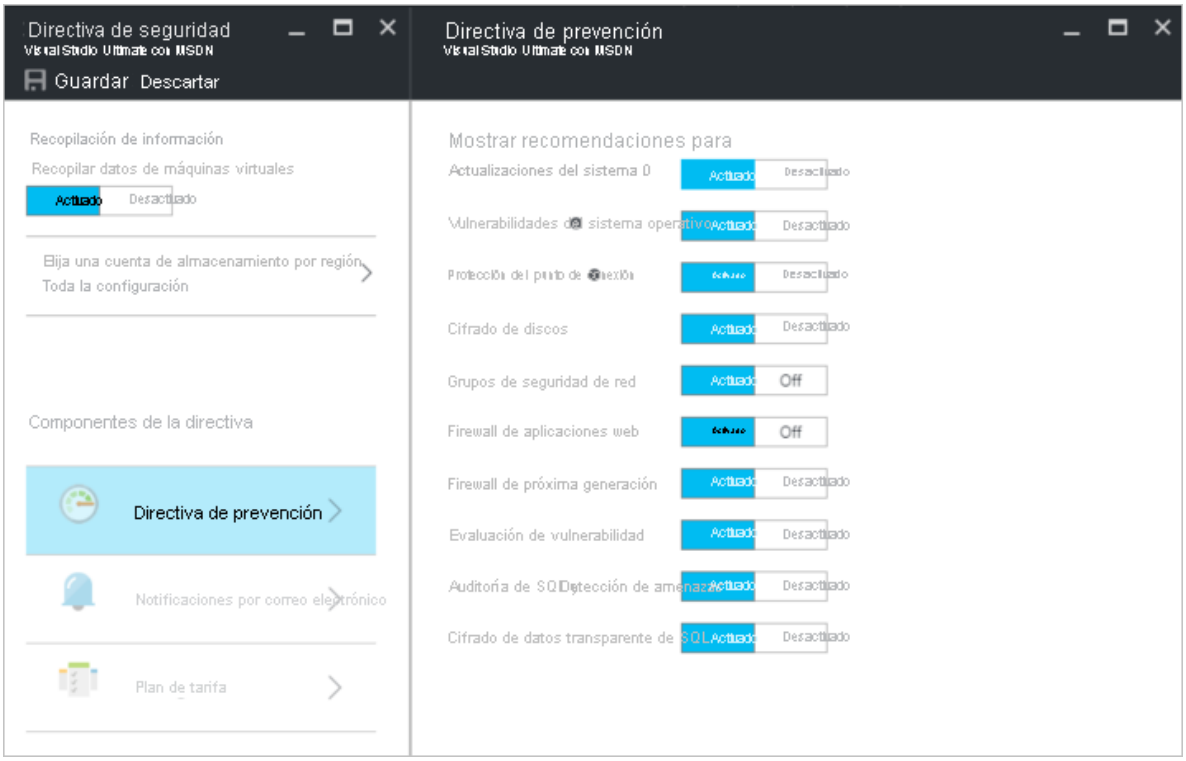
**Exploración de recomendaciones de Microsoft Defender for Cloud**

Microsoft Defender for Cloud ayuda a evitar amenazas y a detectarlas y responder a ellas con más visibilidad y control sobre la seguridad de los recursos de Azure. Security Center le ayuda a proteger los datos de las máquinas virtuales en Azure al proporcionar visibilidad sobre la configuración de seguridad de las máquinas virtuales. Cuando Security Center ayuda a proteger las máquinas virtuales, están disponibles las siguientes funcionalidades:

- Configuración de seguridad del sistema operativo con las reglas de configuración recomendadas.
- Actualizaciones de seguridad del sistema y críticas que faltan.
- Recomendaciones de Endpoint Protection.
- Validación de cifrado de disco.
- Evaluación y corrección de vulnerabilidades
- Detección de amenazas.

**Establecimiento de directivas de seguridad para administrar vulnerabilidades de máquinas virtuales**

Debe habilitar la recopilación de datos para que Microsoft Defender for Cloud pueda recopilar la información que necesita para proporcionar recomendaciones y alertas basadas en la directiva de seguridad que configure. En la ilustración siguiente, se ha activado la recopilación de datos.

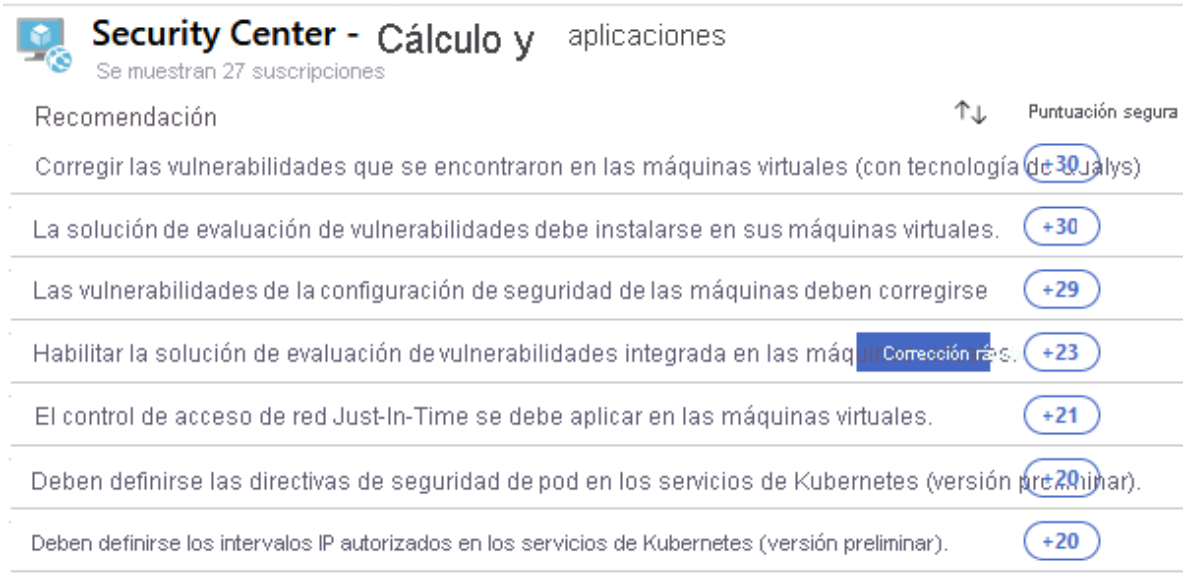


Una directiva de seguridad define el conjunto de controles recomendados para los recursos dentro de la suscripción o el grupo de recursos especificados. Antes de habilitar una directiva de seguridad, debe habilitar la recopilación de datos. Security Center recopila datos de las máquinas virtuales para evaluar su estado de seguridad, proporcionar recomendaciones de seguridad y alertar sobre amenazas. En Security Center, el usuario define directivas para las suscripciones o grupos de recursos de Azure de acuerdo con las necesidades de seguridad de la empresa y los tipos de aplicaciones o la confidencialidad de los datos de cada suscripción.

Security Center analiza el estado de seguridad de los recursos de Azure. Cuando el Centro de seguridad identifica vulnerabilidades de seguridad potenciales, crea recomendaciones. Las recomendaciones le guían en el proceso de configuración de los controles necesarios.

Después de establecer una directiva de seguridad, el Centro de seguridad analiza el estado de seguridad de los recursos, con el fin de identificar vulnerabilidades potenciales. Muestra recomendaciones en un formato de tabla, donde cada línea representa una recomendación. En la tabla siguiente se incluyen ejemplos de recomendaciones para máquinas virtuales de Azure y qué hará cada una de ellas si la aplica. Al seleccionar una recomendación, Security Center proporciona información sobre cómo puede implementar esa recomendación.

Security Center supervisa y analiza las directivas de seguridad habilitadas para identificar posibles vulnerabilidades. En la hoja **Estado de seguridad del recurso**, puede comprobar el estado de seguridad de los recursos junto con cualquier problema. Al seleccionar **Máquinas virtuales** en **Estado de seguridad del recurso**, se abre la hoja **Máquinas virtuales** con recomendaciones para las máquinas virtuales, como se muestra en la ilustración siguiente.




La detección de amenazas de Security Center recopila automáticamente información de seguridad de sus recursos de Azure, de la red y de soluciones de asociados relacionadas. Después, analiza estos datos (a menudo, relacionando la información de diferentes orígenes) para identificar las amenazas. Security Center prioriza las alertas junto con recomendaciones sobre cómo corregir las amenazas.

Security Center emplea análisis de seguridad avanzados que van mucho más allá de los enfoques basados en firmas. Security Center aprovecha los avances en las tecnologías de aprendizaje automático y de macrodatos para evaluar los eventos en toda la estructura de la nube, detectando amenazas que serían imposibles de identificar a través de enfoques manuales y prediciendo la evolución de los ataques. Estas técnicas de análisis son:

- Inteligencia sobre amenazas integrada. Busca a los hackers malintencionados conocidos aprovechando la inteligencia global sobre amenazas de los productos y servicios de Microsoft, la unidad de delitos digitales de Microsoft, el Centro de respuestas de seguridad de Microsoft y fuentes externas.
- Análisis del comportamiento. aplica patrones conocidos para identificar comportamientos malintencionados.
- Detección de anomalías. usa la generación de perfiles estadísticos para crear una base de referencia histórica. Envía alertas sobre desviaciones de las líneas de base establecidas que se ajustan a posibles vectores de ataque.

Con estos análisis, Security Center puede ayudar a interrumpir la cadena de eliminación agregando la detección en distintas fases de la cadena de eliminación, como se muestra en la ilustración siguiente.

En la ilustración anterior se muestran algunas alertas comunes para cada fase, y existen varios tipos más de alertas. Security Center también correlaciona las alertas y crea un incidente de seguridad. Los incidentes de seguridad le dan una mejor vista de qué alertas pertenecen a la misma campaña de ataque.

---

# Protección de cargas de trabajo de Azure con pruebas comparativas de seguridad de Azure

La prueba comparativa de seguridad de Azure incluye una colección de recomendaciones de seguridad de alto impacto que puede usar para ayudar a proteger los servicios que usa en Azure: **Controles de seguridad**: estas recomendaciones suelen aplicarse en el inquilino de Azure y en los servicios de Azure. Cada recomendación señala una lista de partes interesadas que suelen estar implicadas en el planeamiento, la aprobación o la implementación de la prueba comparativa. **Líneas de base del servicio**: Estos controles se aplican a los servicios individuales de Azure para ofrecer recomendaciones sobre la configuración de seguridad de dicho servicio.

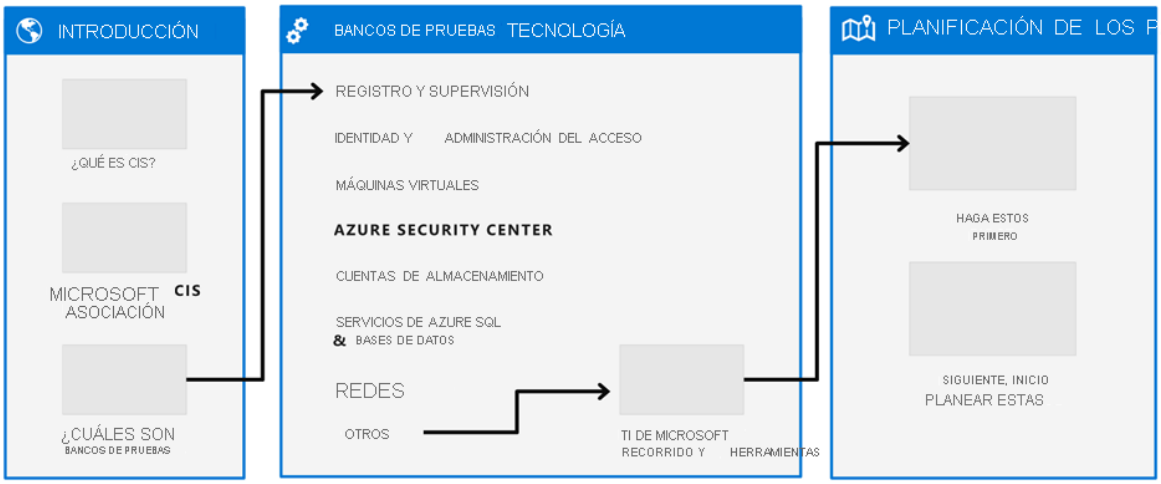
El grupo de ciberseguridad de Microsoft, junto con el Centro para la seguridad de Internet (CIS) ha desarrollado procedimientos recomendados para ayudarle a establecer líneas de base de seguridad para la plataforma Azure. Una línea de base de seguridad es:

- Conjunto de objetivos de seguridad básicos que debe cumplir cualquier servicio o sistema determinado.
- Establece lo que hay que hacer y no cómo hacerlo.

La guía CIS Microsoft Azure Foundations Security Benchmark (Banco de pruebas de CIS de seguridad de la base de Microsoft Azure) proporciona instrucciones prescriptivas para establecer una configuración de línea de base segura para Azure. Esta guía se ha probado en los servicios de Azure mostrados a partir de marzo de 2018. El ámbito de este banco de pruebas es establecer el nivel fundamental de seguridad para cualquier persona que adopte Azure.

**Creación de una línea base de seguridad de la plataforma**

Una gama de estándares de seguridad puede ayudar a los clientes de servicios en la nube a alcanzar la seguridad de la carga de trabajo al usar servicios en la nube. Debajo se indican los grupos tecnológicos recomendados para ayudar a crear cargas de trabajo seguras habilitadas para la nube. Estas recomendaciones no deben considerarse una lista exhaustiva de todas las configuraciones de seguridad y arquitecturas posibles, sino simplemente como un punto de partida.




CIS tiene dos niveles de implementación y varias categorías de recomendaciones.

**Nivel 1**: configuración de seguridad mínima recomendada

- Debe configurarse en todos los sistemas.
- Esto no debería producir ninguna interrupción de los servicios, o muy poca, ni una funcionalidad reducida.

**Nivel 2**: recomendaciones para entornos de alta seguridad

- Esto podría dar lugar a una funcionalidad reducida.

En la tabla siguiente se proporcionan las categorías y el número de recomendaciones realizadas para cada uno.

**Grupo de tecnología**

**Descripción**

**Número de recomendaciones**

**Administración de identidad y acceso (IAM)**

Recomendaciones relacionadas con las directivas IAM

23

**Microsoft Defender for Cloud**

Recomendaciones relacionadas con la configuración y el uso de Microsoft Defender for Cloud

19

**Cuentas de almacenamiento**

Recomendaciones para establecer las directivas de la cuenta de almacenamiento

7

**Azure SQL Database**

Recomendaciones para ayudar a proteger las bases de datos de Azure SQL

8

**Registro y supervisión**

Recomendaciones a fin de establecer directivas de registro y supervisión para las suscripciones de Azure

13

**Redes**

Recomendaciones para ayudar a configurar de forma segura las directivas y la configuración de redes de Azure

5

**Máquinas virtuales**

Recomendaciones para establecer directivas de seguridad para los servicios de proceso de Azure: en particular, máquinas virtuales

6

**Otros**

Recomendaciones relacionadas con la seguridad general y los controles operativos, incluidos los relacionados con Azure Key Vault y los bloqueos de recursos

3

**Total recomendado**

84