

Introducción a Azure Security Benchmark

Diariamente se publican nuevos servicios y características en Azure; los desarrolladores publican rápidamente nuevas aplicaciones en la nube basadas en estos servicios y los atacantes buscan siempre nuevas formas de aprovechar los recursos configurados incorrectamente. La nube se mueve rápidamente, los desarrolladores también y los atacantes siempre están en movimiento. ¿Cómo puede mantenerse al día y asegurarse de que sus implementaciones en la nube están seguras? ¿En qué se diferencian los procedimientos de seguridad para sistemas en la nube de los sistemas en el entorno local? ¿Cómo puede supervisar la coherencia en muchos equipos de desarrollo independientes?

Microsoft ha descubierto que el uso de *pruebas comparativas de seguridad* puede ayudarle a proteger rápidamente las implementaciones en la nube. Las recomendaciones para las pruebas comparativas del proveedor de servicios en la nube ofrecen un punto de partida para seleccionar opciones de configuración de seguridad específicas en su entorno y le permiten reducir rápidamente los riesgos para su organización.

Azure Security Benchmark incluye una recopilación de recomendaciones de seguridad de gran impacto que puede usar para ayudar a proteger los servicios que usa en Azure:

- **Controles de seguridad:** Estas recomendaciones se suelen aplicar tanto en el inquilino de Azure como 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.

Implementación de Azure Security Benchmark

- **Planee** la implementación de Azure Security Benchmark revisando la [documentación](#) de los controles empresariales y las líneas de base específicas del servicio para planear el marco de control y cómo se asigna a instrucciones como [Center for Internet Security \(CIS\) Controls](#), [National Institute of Standards and Technology \(NIST\)](#) y el marco [Payment Card Industry Data Security Standard \(PCI-DSS\)](#).
- **Supervise** el cumplimiento con el estado de Azure Security Benchmark (y otros conjuntos de controles) mediante el [panel de cumplimiento normativo](#) de Microsoft Defender for Cloud.
- **Establezca** límites de protección para automatizar las configuraciones seguras y exigir el cumplimiento de Azure Security Benchmark (y otros requisitos de su organización) con Azure Blueprints y Azure Policy.

Casos de uso comunes

Azure Security Benchmark se usa con frecuencia para abordar estos desafíos comunes para clientes o socios de servicio que:

- Es nuevo en Azure y busca procedimientos recomendados de seguridad para garantizar la implementación segura de los servicios de Azure y su propia carga de trabajo de aplicación.
- Busca mejorar la postura de seguridad de sus implementaciones existentes de Azure para clasificar por orden de prioridad los principales riesgos y mitigaciones.
- Evalúa las características y funcionalidades de seguridad de los servicios de Azure antes de incorporar o aprobar un servicio de Azure en el catálogo de servicios en la nube.
- Debe cumplir los requisitos de cumplimiento en sectores altamente regulados, como el Estado, las finanzas y la atención sanitaria. Estos clientes deben asegurarse de que sus configuraciones de servicio de Azure cumplen la especificación de seguridad definida en el marco como CIS, NIST o PCI. Azure Security Benchmark proporciona un enfoque eficaz con los controles ya asignados previamente a estas pruebas comparativas del sector.

Terminología

Término	Descripción	Ejemplo
Control	Un control es una descripción de alto nivel de una característica o actividad que debe abordarse y no es específico de una tecnología o implementación.	La protección de datos es una de las familias de control de seguridad. La protección de datos contiene acciones específicas que deben abordarse para ayudar a garantizarla.
Línea base	Una línea base es la implementación del control en el servicio individual de Azure. Cada organización decide cuáles recomendaciones de prueba comparativa y configuraciones correspondientes son necesarias en el ámbito de implementación de Azure.	La empresa Contoso busca habilitar las características de seguridad de Azure SQL según la configuración recomendada en la línea de base de seguridad de Azure SQL.

[Azure Security Benchmark](#) es el conjunto de directrices específico de Azure y de creación de Microsoft para los procedimientos recomendados de seguridad y cumplimiento basados en marcos de cumplimiento comunes. Este punto de referencia, que cuenta con un 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. Los clientes usan ASB como marco de control completo para poder cumplir todos sus requisitos de seguridad. Benchmark se implementa como una iniciativa de Azure Policy que implementa la supervisión de todas estas directrices.

Azure Security Benchmark es la base de las recomendaciones de Security Center y se ha integrado completamente como la iniciativa de directiva predeterminada. Esto significa que todos los clientes de ASC obtienen automáticamente ASB como directiva de seguridad predeterminada, y ASB se posiciona como conjunto singular de procedimientos recomendados de seguridad en Azure, alineado con la Puntuación de seguridad.

Trabajar con directivas de seguridad en Microsoft Defender para la nube

De forma predeterminada, todas las directivas de prevención están activadas. Las directivas de prevención y las recomendaciones están asociadas entre ellas. Es decir, si habilita una directiva de prevención, como vulnerabilidades del sistema operativo, se habilitarán recomendaciones para esa directiva. En la mayoría de las situaciones, querrá habilitar todas las directivas, aunque algunas puedan ser más importantes que otras en su caso, en función del recurso de Azure que haya implementado.

Security Center crea automáticamente una directiva de seguridad predeterminada para cada una de las suscripciones de Azure. Puede editar las directivas de Azure:

- Crear nuevas definiciones de directiva.
- Asignar directivas entre grupos de administración y suscripciones, que pueden representar una organización entera o una unidad de negocio dentro de la organización.
- Supervisar el cumplimiento de las directivas.

Una directiva de Azure consta de los siguientes componentes:

- Una **directiva** es una regla.
- Una **iniciativa** es una colección de directivas.
- Una **asignación** es la aplicación de una iniciativa o una directiva para un ámbito concreto (grupo de administración, suscripción o grupo de recursos).



A continuación, se muestra una lista generada de los tipos de recomendaciones. Las recomendaciones ayudan a proporcionar visibilidad completa sobre el estado de seguridad de su entorno.

Directiva de seguridad

DEMOSTRACIÓN DE ASC

Directiva de seguridad en: DEMOSTRACIÓN DE ASC

Directivas asignadas en esta suscripción





Directiva predeterminada del centro de seguridad

Azure Security Benchmark (2 asignaciones)

Esta es la directiva predeterminada para recomendaciones de Azure Security Center que está habilitada de forma predeterminada en su suscripción.

[Ver directiva efectiva](#)





Estándares normativos y del sector

Directivas de cumplimiento que puede ver en el panel de cumplimiento. Para agregar más estándares de cumplimiento, haga clic en **Agregar más estándares**.

Azure Security Benchmark	Realice un seguimiento de los controles de Azure Security Benchmark en el Panel de cumplimiento a partir de un conjunto recomendado de directivas y evaluaciones.	De serie	Deshabilitar ⓘ
PCI DSS 3.2.1	Realice un seguimiento de los controles de PCI-DSS v3.2.1:2018 en el Panel de cumplimiento, según un conjunto recomendado de directivas y evaluaciones.	De serie	Deshabilitar ⓘ
ISO 27001	Realice un seguimiento de los controles de la ISO 27001:2013 en el Panel de cumplimiento, según un conjunto recomendado de directivas y evaluaciones.	De serie	Habilitación ⓘ
SOC TSP	Realice un seguimiento de los controles de SOC TSP en el Panel de cumplimiento, según un conjunto recomendado de directivas y evaluaciones.	De serie	Habilitación ⓘ
SWIFT CSP CSCF v2020	Permite realizar un seguimiento de los controles de SWIFT CSP CSCF v2020 en el Panel de cumplimiento según un conjunto recomendado de directivas y evaluaciones.	Agregado manualmente	Eliminar
NIST SP 800-53 R4	Seguimiento de los controles NIST SP 8020-53 R4 en el Panel de cumplimiento, basado en un conjunto recomendado de directivas y evaluaciones.	Agregado manualmente	Eliminar
Azure CIS 1.1.0 (Nuevo)	Seguimiento de los controles de Azure CIS 1.1.0 (nuevo) en el Panel de cumplimiento, basado en un conjunto recomendado de directivas y evaluaciones.	Agregado manualmente	Eliminar

[Agregar más estándares](#) ⓘ



Sus iniciativas personalizadas

Las directivas de iniciativas personalizadas que ha creado y que están disponibles en la página de **Recomendaciones**. Para agregar otra directiva de iniciativa personalizada, haga clic en **Agregar una iniciativa personalizada**.

MyOrgDemoCustomPolicy	Esta es una iniciativa personalizada que representa la directiva de seguridad personalizada de mi organización.	Eliminar
CustomPolicyDemo		Eliminar

[Agregar una iniciativa personalizada](#) ⓘ

- **Actualizaciones del sistema.** Recupera una lista diaria de actualizaciones de seguridad disponibles y actualizaciones críticas de Windows Update o Windows Server Update Services (WSUS).
- **Vulnerabilidades del sistema operativo.** Analiza diariamente las configuraciones del sistema operativo para determinar los problemas que pueden hacer que la máquina virtual sea vulnerable a ataques.

- **Protección de puntos de conexión.** Recomienda el aprovisionamiento de la protección de puntos de conexión para todas las máquinas virtuales de Windows con el fin de ayudar a identificar y eliminar virus, spyware y otro software malintencionado.
- **Cifrado de discos.** Recomienda habilitar el cifrado de discos en todas las máquinas virtuales para mejorar la protección de datos en reposo.
- **Grupos de seguridad de red.** Recomienda configurar los NSG para controlar el tráfico entrante y saliente de las máquinas virtuales que tienen puntos de conexión públicos. Además de comprobar que se haya configurado un NSG, esta directiva evaluará las reglas de seguridad de entrada.
- **Firewall de aplicaciones web.** Extiende las protecciones de red más allá de los grupos de seguridad de red, que están integrados en Azure. Security Center detectará las implementaciones para las que se recomienda un firewall de última generación y le permitirá aprovisionar una aplicación virtual.
- **Firewall de última generación.** Microsoft Defender para la nube puede recomendarle agregar el firewall de última generación (NGFW) de un asociado de Microsoft para aumentar las protecciones de seguridad.
- **Evaluación de vulnerabilidades.** Se recomienda instalar una solución de evaluación de vulnerabilidades en la máquina virtual.
- **Detección de amenazas y auditoría de SQL.** Recomienda habilitar la auditoría del acceso a Azure SQL Database para el cumplimiento y la detección avanzada de amenazas, con fines de investigación.
- **Cifrado de SQL.** Recomienda habilitar el cifrado en reposo para la base de datos de Azure SQL, las copias de seguridad asociadas y los archivos de registro de transacciones. Esto ayuda a evitar que los datos sean legibles incluso aunque se produzca una vulneración de seguridad.

¿Quién puede editar directivas de seguridad?

Security Center usa el control de acceso basado en rol (RBAC), que proporciona roles integrados que se pueden asignar a usuarios, grupos y servicios en Azure. Cuando los usuarios abran Security Center, solo podrán ver información relacionada con los recursos a los que tienen acceso. Esto significa que a los usuarios se les asigna el rol de propietario, colaborador o lector para la suscripción o el grupo de recursos a los que pertenece un recurso. Además de estos roles, hay dos roles específicos de Security Center:

- **Lector de seguridad:** el usuario tiene derecho a visualizar el contenido de Security Center (recomendaciones, alertas, directivas y estados) pero no puede realizar cambios.
- **Administrador de seguridad:** tiene los mismos derechos que el lector de seguridad, pero también puede actualizar la directiva de seguridad o descartar recomendaciones y alertas.